Vidyawarta

Peer-Reviewed International Research Journal

July To Sept. 2021, Special Issue

"Education Through Self-help is Our Motto"

Rayat Shikshan Sanstha's

Shripatrao Kadam Mahavidyalaya Shirwal, Tal.Khandala, Dist. Satara

(Dr.PatangraoKadam Educational Complex)

(Shivaji University, Kolhapur)

INTERNAL QUALITY ASSURANCE CELL

AND

DEPARTMENT OF COMMERCE

ORGANISE

AONE DAY ONLINE

INTERDISCIPLINARYINTERNATIONALCONFERENCE

ON

The Role of Cyber Security in the Global Context

Saturday,5thJune,2021

PRINCIPAL

DR.MANJUSHRI VILASRAO BOBADE

CONVENOR

DR.BALASAHEB KALHAPURE

CO-ORDINATORS

PROF. TULSHIDAS APHALE DR.VILAS SADAPHAL

ORGANIZING COMMITTEE MEMBERS

DR.PRATAP SINHMANE RROF.RAJENDRA TAMBILE PROF. SANTOS HGHANGALE

Reg.No.U74120 MH2013 PTC 251205

Harshwardhan Publication Pvt.Ltd.

At.Post.Limbaganesh,Tq.Dist.Beed
Pin-431126 (Maharashtra) Cell:07588057695,09850203295
harshwardhanpubli@gmail.com, vidyawarta@gmail.com

All Types Educational & Reference Book Publisher & Distributors / www.vidyawarta.com

Date of Publication
01 July 2021

Vidyawarta™
International Multilingual Research Journal

www. विद्यावार्ता .कॉम ®
YouTube Channel

Vidyawarta is peer reviewed research journal. The review committee & editorial board formed/appointed by Harshwardhan Publication scrutinizes the received research papers and articles. Then the recommended papers and articles are published. The editor or publisher doesn't claim that this is UGC CARE approved journal or recommended by any university. We publish this journal for creating awareness and aptitude regarding educational research and literary criticism.

The Views expressed in the published articles,Research Papers etc. are their writers own. This Journal dose not take any libility regarding appoval/disapproval by any university, institute, academic body and others. The agreement of the Editor, Editorial Board or Publicaton is not necessary. *Editors and publishers have the right to convert all texts published in Vidyavarta (e.g. CD / DVD / Video / Audio / Edited book / Abstract Etc. and other formats).*

If any judicial matter occurs, the jurisdiction is limited up to Beed (Maharashtra) court only.

Indexed Indexed

IMPACT 7.940 iijif FACTOR

TM
Govt. of India,
Trade Marks Registry
Regd. No. 2611690

http://www.printingarea.blogspot.com

OUR PATRONS

Hon. Shri. Sharadchandra Pawar
(President, Rayat Shikshan Sanstha, Satara)

Hon. Dr. Anil Patil
(Chairman, Rayat Shikshan Sanstha, Satara)

Hon. Adv. Bhagirath Shinde
(Vice- Chairman, Rayat Shikshan Sanstha, Satara)

Hon. Prin. Dr. Vitthal Shivankar
(Secretary, Rayat Shikshan Sanstha, Satara)

Hon. Prin. Dr. Pratibha Gaikwad
(Joint Secretary, Rayat Shikshan Sanstha, Satara)

Hon. Prin. Dr. Shivling Menkudale
(Auditor, Rayat Shikshan Sanstha, Satara)

ADVISORY COMMITTEE

Hon. Dr. Vishwajeet Kadam
(Chairman, College Development Committee)

Hon. Appasaheb Deshmukh
(Member, College Development Committee)

Hon. Uday (Dada) Kabule
(President, Satara Jilha Parishad, Satara)

Hon. Rajendra (Anna) Tambe
(Sabhapati, Panchayat Samiti, Khandala Tahsil)

Hon. Mrs. Neha Paranjape
(Director, Paranjape Autocast Pvt. Ltd.)

Hon. Mrs. Laxmitai Pansare
(Sarpanch, Grampanchayat Shirwal)

RESOURCEPERSONS

Mr. Mahesh Ghule
Senior Cyber Security Consultant CGI UK IT Ltd., London, U.K.
Topic : Cyber Security

Mr. Swapnil Ranadive
Chief Revenue Officer, Intellect Select Ltd., Canterbury, U.K.
Topic: AI, ML & RPA use cases

Mr. Suhas Patil
Global New Business Development UNIFRAX ILLC, New York, U.S.A.
Topic: Economic Impact of Weak Cyber Security on Society

Mr. Rakesh Churi
SAP Business Solutions Specialist UNIFRAX ILLC, New York, U.S.A.
Topic: Economic Impact of Weak Cyber Security on Society

ABOUT THE SANSTHA:

Rayat Shikshan Sanstha was founded by Late Padmabhushan Dr. Karmaveer Bhaurao Patil in 1919, for imparting education to the down-trodden masses in the rural areas of Maharashtra and Karnataka State. It is well known for its contribution to education system in Maharashtra by providing education to deprived class of the society. At present the Sanstha is managing 42 degree colleges of Arts, Science and Commerce streams, 01 Research Institute, 02 B. Ed. Colleges, 01 Law, 01 Engineering college, 08 D. Ed. colleges, 182 Junior colleges, 438 High Schools, 84 Primary and Pre-primary schools, 02 Industrial Training Institutes, 08 Ashram Shalas, 91 hostels and 57 other institutes. It is the biggest educational institute in Asia. The mission laid down by Late Padmabhushan Dr. Karmaveer Bhaurao Patil is the guiding principle for all the branches of Rayat Shikshan Sanstha. The motto of the institution is “Education through self-help” and symbol of the Banyan tree reflects the growth of the institution.

ABOUT THE COLLEGE:

Shripatrao Kadam Mahavidyalaya, Shirwal, established in 1983, is one of the branches of Rayat Shikshan Sanstha, Satara which is situated in the rural and hilly area of Shirwal, Tal. Khandala, Dist. Satara (Maharashtra, INDIA). The college is recognized by U.G.C. with 2f and12B status. It is affiliated to Shivaji University, Kolhapur. It has been reaccredited by N.A.A.C. with ‘B’ Grade (C.G.P.A. 2.73). The institution follows all the norms and regulations of U.G.C., Government of Maharashtra and Shivaji University, Kolhapur.

The vision of the college is in tune with the parent institute Rayat Shikshan Sanstha, Satara which provides value based quality education to generate skilled human resource for building the nation. Besides two under graduate aided degree Programmes i.e. Arts and Commerce, the college has also introduced Bachelor of Computer Application and two Post- Graduate Programmes i.e. M.Com. in Advanced Accountancy and M.A. in English on self- financed basis. The college also offers 12 skill based add-on-courses and 04 career oriented courses.

ABOUT THE CONFERENCE:

The digital age has brought a complete change in the way we view and experience the world. The world functions have become smaller and, it has certainly brought its share of problems. As connectivity increases, the risk of security also crops up inevitably. In the present scenario, sensitive data is continuously at risk and different types of technologies and processes are designed to protect it. The data here can refer to one saved on devices, programs, software networks and more. Any sort of unauthorized access to such information is a security breach and hence strong measures are taken to prevent it.

500 million users were breached and personal information was extracted from them. This brings down the reputation of the enterprise and its credibility in the eyes of the consumer. It also puts the customers at risk as their valuable information is out in the open and can be misused for any purpose. The conference therefore opens the wide platform to all of us to discuss and share the invaluable ideas to nurture the better humanity at large.

Principal's Message

It gives me great pleasure to extend to you all a very warm welcome on behalf of all those who have accepted our invitation to convene this A One Day Online Multidisciplinary International Conference on 'The Role of Cyber Security in the Global Context' . First and foremost, I would like to thank our Resource person **Hon'ble Suhas Patil, Mr. Rakesh Churi, Mr.Mahesh Ghule and Mr. Swapnil Ranadive**, for their valuable guidance and encouraging us to take up these global issues of vital interests. also My sincere thanks also owe to **Hon'ble Chairman, Dr. Anil Patil, Vice-Chairman Adv. Bhagirath Shinde, Secretary Prin. Dr. Vitthal Shivankar, Joint Secretary, Prin. Dr. Pratibha Gaikwad and Auditor, Hon. Prin. Dr. Shivling Menkudale** for giving us an opportunity to organize this international event and providing their valuable guidance regarding the Conference.

Moving further, I would like to appreciate kindness and sincere cooperation of our resource persons Mr. Mahesh Ghule, Mr. Swapnil Ranadive, Mr. Suhas Patil and Mr. Rakesh Churi for sparing time for us on this occasion.

My team would like to be indebted to all the scholars who have submitted their research papers for the publication and showed their heartfelt interest for the success of this conference. Your genuine feeling is also highly appreciated by our Management . I wish every success to this conference.

I really appreciate the efforts of Dr. Kalhapure Sir, and Dr. Vilas Sadaphal Sir who Prof. Tulshidas Aphale Sir, Coordinator, IQAC and Vice- Principal of this college have taken painstaking efforts to plan this joint venture. I also owe due recognition to everyone who is directly or indirectly associated with the organization of this conference in this pandemic.
Be Healthy! Be Safe!!
JAY KARMAVEER!

Thank you very much.

Prin. (Dr.) Manjushri Bobade

From the Convener and Editor's Desk

Welcome to A One-Day Online Multidisciplinary International Conference on 'The Role of Cyber Security in the Global Context'. The purpose of the conference is to provide a forum for teachers, researcher, students and citizens in the field of digital technologies and social media, for this conference we received a great number of papers and from them editors have selected the quality papers those which are published.

I am grateful to our Principal for extending support to make this conference fruitful. I am also thankful to our entire team to make this conference successful. We hope that the proceedings will serve the purpose of generating awareness among the researchers and students.

Thank you.

Dr. Balasaheb Kalhapure
Assistant Professor and Head,
Department of Commerce

INDEX

01

CRITICAL ANALYSIS OF HOW INDIA IS BECOMING HOTSPOT OF CYBERCRIME AMID COVID-19 PANDEMIC

Prin. Dr.Manjushri Bobade
Rayat Shikshan Sanstha's, Shripatrao Kadam Mahavidyalaya, Shirwal

****

Abstract— As the whole world is been impacted by the COVID- 19 pandemic, there is no aspect remained untouched without the impact of this virus.This virus has restricted all humans from going out from our houses to our works, social meetings,shopping,educational institutes and all.So with this quarantine lifestyle emerged the dependency of human life on computers, laptops and smart phones. However, these gadgets help make life easy but come the threats of cyber security too. In the year 2020, we saw one of the biggest statistics of data breaches and the figures give the notion of being as if to be only rising.According to a study in February, 2021 almost one year from the beginning of the pandemic—there were 30 Crore 77 Lakh brute-force attacks a far cry from the 9 Crore 31 Lakh witnessed at the start of 2020. This research paper focuses on impact on cyber security in Covid-19 pandemic.This analysis shows the aspects of threats caused due to higher use of internet facilities and cyber attack.

Keywords: COVID-19,Pandemic,Cyber security, Cyber Crime, Malware, Analysis

I. INTRODUCTION

In the midst of pandemic troublesome businesses and with isolated functioning appropriate reality, cyber criminals have been seen busy exploiting vulnerabilities. In the year 2020, we saw one of the major figures of data breaches and the figures seems to be rising. As the whole world is been impacted by the COVID-19 pandemic, there is no aspect remaining without the impact of this virus. As this virus has restricted all us humans from going out from our houses to our work, social meetings, shopping, education institutes and all. So with this quarantine lifestyle came the dependency of human life on computers, laptops and smart phones. However these gadgets help make life easy but come the threats of cyber security too. In the year 2020, we saw one of the biggest statistics of data breaches and the figures give the notion of being as if to be only rising.According to a study in February 2021 almost one year from the start of the pandemic there were 30 Crore 77 Lakh brute-force attacks a far cry from the 9 Crore 31 Lakh witnessed at the start of 2020. This research paper focuses on impact on cyber security in Covid- 19 pandemic.This analysis shows the aspects of threats caused due to higher use of internet facilities and cyber attack.

II. OBJECTIVES

This analysis shows the current scenario of COVID-19 impact on cyber security and emphasis of the following objectives.

In this article we have focused on three main aspects of cyber crime

1. Level one has the analysis of country wise impact of cyber crime.

2. Level two shows us the analysis of state wise impact of cyber crime.

3. Level three focuses on the analysis of city wise impact of cyber crime.

III. METHODOLOGY

In this research analysis resources were studied and accordingly analysis study was been carried out. Major findings were been studied and the representation of the paper were been recorded.

A solitary cause for the tall figure of data breaches is that as India is flourishing its startups and powerhouses are a highly striking promotes Cybercrime. As well as Indian companies are economically doing well, they have a brand to worry about separately from the enormous amount of private, economic and user behavioral data that they hold. In a recent study by Infosys-Interbrand, the probable risk in brand name and value of data breach to the world's 100 most expensive brands could total to as much as $223 billion.According to study last year 52% of firms in India reported cyber attack.

According to the survey by global cyber security firm Sophos, among all these successful breaches, 71% of firms said that it was a severe or very severe hit, and 65 % said it took longer than seven days to remediate.

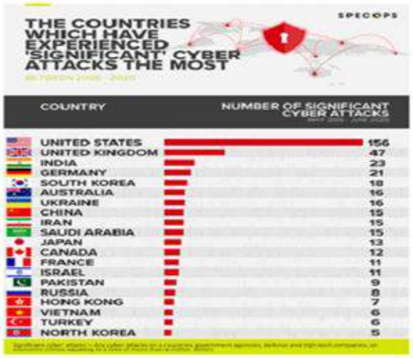


Fig. 1(Source Google)

Above given image describes India's Cyber attacks significance worldwide. We rank at three number in globe according to study.

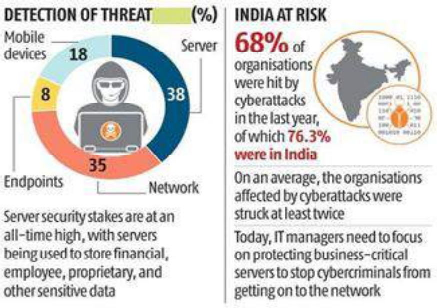
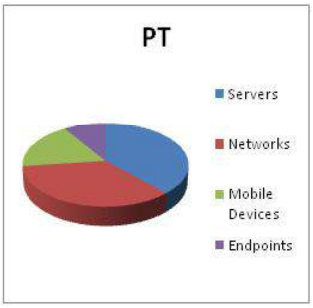


Fig. 2(Source Google)

Another survey detected the percentage of threat caused by various scenarios of cyber attack.

1. 38% are caused by Servers.
2. 35% are caused by Network.
3. 18% are caused by Mobile device
4. 9% are caused by Endpoints.



State wise ranking	
Rank	States
1	Maharashtra
2	Delhi
3	West Bengal
4	Gujarat
5	Uttar Pradesh
6	Karnataka
7	Rajasthan
8	Tamil Nadu
9	Madhya Pradesh
10	Telangana
11	Haryana
12	Odisha

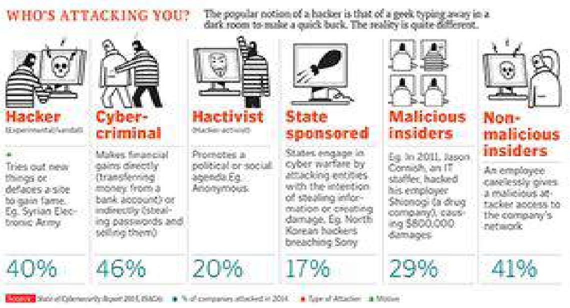
(Source Google)

An important aspect study stated the most vulnerable states in India. The statistics gives us the brief idea of state wise representation of ranking. The above given is the important figure of states mostly impacted by Cyber Attacks in India.

The below given table represents the cities in India which are at the higher risk of Cyber Attack. According to survey 3 out of every 10 Indian cyber users is encountered many cyber attacks, meanwhile in metropolitan cities have experienced a comparable figure when compared to the earlier quarter. Among the metropolitan cities, Delhi has seen the highest.

City wise ranking	
RANK	CITIES
1	Mumbai
2	Delhi
3	Bangalore
4	Kolkata
5	Pune
6	Hyderabad
7	Nagpur

IV. SUGGESTIONS



The popular notion of a hacker is that of a geek typing away in a dark room to make a quick buck. The reality is quite different.

Tries out new things or defaces a site to gain fame. Eg. Syrian Electronic Army

Makes financial gains directly (transferring money from a bank account) or indirectly (stealing passwords and selling them)

Promotes a political or social agenda Eg. Anonymous

States engage in cyber warfare by attacking entities with the intention of stealing information or creating damage. Eg. North Korean hackers breaching Sony

Eg. In 2011, Jason Cornish, an IT staffer, hacked his employer Shionogi (a drug company), causing $800,000 damages

An employee carelessly gives a malicious attacker access to the company's network

The most common attacks which take place are noted below. The main suggestions are to be aware from the below given aspects.

1. Hackers 40% of attacks are been done by the hackers.

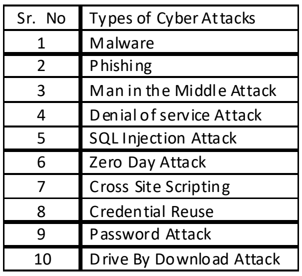
2. 46% attacks are been done by the Cyber Criminals.

3. 20% are been attacked by Hactivist.

4. 29% is the count of malicious insiders.

5. 41% are attacked by Non Malicious insiders.

The Top ten main types of Cyber Attacks which takes place are-



Sr. No	Types of Cyber Attacks
1	Malware
2	Phishing
3	Man in the Middle Attack
4	Denial of service Attack
5	SQL Injection Attack
6	Zero Day Attack
7	Cross Site Scripting
8	Credential Reuse
9	Password Attack
10	Drive By Download Attack

The main aspect is to safeguard ourselves from the above given cyber attacks. We have to find out the ways to save ourselves.

V. CONCLUSION

The basic conclusion from this research is

1) Government should focus on more cyber security provision of each and every aspects of the country; more budgets should be allocated for the security of IT firms, government offices and other institutes.

2) Proper use of a service internet security suite should be done.

3) Always set strong passwords on your devices to avoid further problems.

4) Software updating should be done time to time

5) Social media settings should be managed by self always.

6) Home network should be always strengthened.

7) Children should be aware about the uses and misusesof internet

8) Updates of the security breaches should be taken.

ACKNOWLEDGMENT

I would like to thank all the people who directly and in directly helped supported and guided me during this research article. I owe my gratitude to all these supporters

REFERENCES

[1] From retrieved on https://www.business-standard.com/

[2] From Wikipedia. India's Covid-19 Pandemic. Retrieved on https://en.wikipedia.org/wiki/in-India education

[3] Reference from https://www.tcs.com/perspectives/articles/how-covid-19-is-dramatically-changing-cybersecurity

[4] Reference from https://cio.economictimes.indiatimes.com/news/digital-security/the-importance-of-cybersecurity-in-the-post-covid-19-world/77516894

❑❑❑

02

An Importance of Cyber Security in Indian Banking System

Dr.Balasaheb Kalhapure
Assistant Professor in Commerce,
SKM College Shirwal, Tal-Khandala, Dist.Satara

****

Abstract:

Indian banks have seen a gradual rise in cyber threats as they need been exploring or clutch complicated technologies (such as mobile and net banking), rising worker computer network, and a lot of recently, adopting hybrid cloud technology. As a result, they need been selective in adopting digitization within the past. Before the COVID-19 crisis, a majority of the Indian banks targeted on strategic digitization of their client services and experiences "one amongst the four pillars of the banking system. The speedily ever-changing behavior and preferences amongst rising urban customers, millennia's, and also the middle-income population (demanding quicker solutions and higher made-to-order products) drove digitization in services to customers. On the opposite hand, usages of digital technologies amongst the opposite 3 stakeholders—employees, business alliances, and vendors—were measured and gradual. this can be partially thanks to the quality of operations and also the associated degree of cyber risks. within the future, this trend of selective digitization can amendment thanks to the evolving trends within the post COVID-19 era.

1. Introduction

The banking sector has been under fire for many years. First, it had been the physical larceny of monies. Then it had been laptop fraud. Today, it's not solely cyber fraud however hacks into servers to get a customer's in person specifiable info (PII). Hence, the explanation why cyber security in banking is of utmost importance. As people and firms perform most transactions on-line, ATM, RTGS, NEFT, ECS, EFT, Retail Banking, Debit and Credit cards and plenty of additional the chance of a knowledge breach will increase daily. this can be why there's a larger stress to look at the importance of cyber security in banking sector processes.

Since the pandemic has set foot worldwide in 2020,cyber-attacks in banks have broken-backed headlines across the globe. Moody warned banks globally of "increased risks of cyber-attacks throughout the continued COVID-19 pandemic". in line with a VMware C report, cyber-attacks against banks and money establishments globally exaggerated 238 % amidst the COVID-19 crisis between Feb 2020 and Apr 2020.

Increase operational resilience

Banking is Associate in nursing employee-intensive business and maintains a high bit customer-service model (as disclosed from the quantity of bank branches that remained open throughout the nationwide lockdown). Therefore, once Asian country went into an entire internment once the onset of the pandemic, quality restrictions for workers, vendors, and partners affected business operations, resources convenience, and productivity.

The onset of COVID-19 and also the government's response to contain the unfold reveal one placing vulnerability of banks "business operations will be noncontiguous anytime, and most unexpectedly. Banks could need to still subsume disruptions in their operations because of social distancing norms, and intermittent regional and native lockdowns, going forward.

They will need to build resilience within the info Technology (IT) design to confirm continued access to business applications from anyplace any time to workers, vendors, and partners. Therefore, fast digital transformation is instance for banks to confirm watertight business continuity set up and uphold productivity throughout tough times, whereas comprehending ensuing info security risks against these edges.

Improve client stretch

In India, banks subsume a myriad of shoppers with completely different digital preferences. Their preferences vary with their data of and inclination to use digital platforms, the perception of risks related to digital processes, and also the nature of knowledge and repair necessities. Therefore, banks have had to manage a hybrid of client interaction channels.

Since the pandemic, business disruptions have caused inconvenience to multiple client segments World Health Organization earlier trusted branches for essential money transactions or recommendation on complicated money merchandise. Banks have seen a pointy decline within the use of ancient ways in which of communication amongst a majority of their customers. within the future, social distancing norms (to combat the COVID-19 crisis) can probably amendment behavior within the Indian society for good. Exaggerated demand for contactless transactions and virtual services, that square measure secure and convenient to use and navigate, would force banks to modify apace.

Save cost

Every business strives to form its operations price effective and banking isn't any exception. Banks need to offer comprehensive and essential services with efficiency despite disruption, whereas remaining price effective. With COVID-19, one among the largest challenges that banks square measure probably to face is that of rising Non-Performing Assets (NPA). in line with the RBI's latest money stability report, macro stress tests for credit risk indicate that the gross terrorist group magnitude relation of regular industrial Banks (SCBs) could increase from eight.5 % in March 2020 to twelve.5 % by March 2021 beneath their baseline situation. The magnitude relation could step up to fourteen.7 % beneath a severely stressed situation. Rising NPAs can probably raise money stress and credit prices. conversion are going to be key for banks to run operations with efficiency, improve productivity, scale back prices, and stay competitive throughout and once the pandemic. As a result, there's a pressing ought to portion adequate resources towards conversion.

2. Objectives of the Study

1. Examine how the banking industry is responding to the changing operating environment

2. Analyze the rising cyber security risks in banks afterCOVID-19 in the wake of rapid digitization.

3. Advocate the possible cyber security solutions for banks to cope with the challenges.

3. Methodology:

The present review paper is based on the Secondary data. It analyses the available literature on Banking technology and various existing and upcoming innovative products offered by banks in India. The Secondary data pertaining to the study was obtained from the various journals, books, Magazines, Newspapers and websites of the concerned Banks

4. The importance of cyber security

The plain cause for the importance of cyber security in banking sector transactions is to guard purchaser belongings. As more humans go cashless, sports are achieved via online checkout pages and physical credit score scanners. In both conditions, PII may be redirected to other locations and used for malicious activities

Now not best does this have an effect on the purchaser. It additionally greatly harms the bank whilst they try to recover the information. while it's taken hostage, the financial institution would possibly want to pay loads of lots of dollars to launch the records. In flip, they lose the agree with in their customers and other financial institutions.

That's now not the best aspect that takes place when steps for cyber safety banking aren't implemented. The customer needs to cancel all their cards and begin new accounts – probable at some other bank. And though their budget are protected by way of the FDIC, it doesn't stop criminals from seeking to use their PII.

A few dangers presently associated with banking at the web

The above examples account for a small percent of capability issues with cyber security in banking. a number of the other objects to be worried approximately encompass:

Associated some crucial content

Cyber protection & Fraud Taking treasury through the cyber safety undertaking

Cyber protection & Fraud BoE, FCA, and MAS to collaboration on cyber security

a. More risks from cellular apps —

More individuals access their bank money owed on mobile apps. Many of these people generally tend to have minimum or no security, and this makes the capacity of assault a great deal more. Hence, banking software answers are required at the endpoint to prevent malicious activity.

b. Breaches at third-party agencies —

As banks have upgraded their cyber security, hackers have grew to become to shared banking systems and 1/3-birthday party networks to advantage get admission to. If those aren't as protected as the financial institution, the attackers can get thru effortlessly.

c. Improved danger of crypto forex hacks —

In addition to conventional price range, hacks have improved within the growing global of cryptocurrency. For the reason that area is unsure how to enforce cyber safety software for banking on this ever-converting marketplace, the capability for attackers to grab massive amounts of this forex is greater. Specifically when it quick jumps in valuefive.Protect towards attacks with secured software programwhile you observe the on-going kingdom of safety on the net, you must do not forget enhancement or entire replacement of your present day safety packages. here are a few matters to examine in the global of banking software program improvement.

a. Safety audit —

An intensive audit is imperative earlier than any new cyber protection software is carried out. The evaluate famous the strengths and weaknesses of the existing setup. Moreover, it affords recommendations that may assist shop money while additionally taking into account the right investments.

b. Firewalls —

Cyber protection banking configuration does not only consist of packages. It also calls for the right hardware to dam attacks. With an updated firewall, banks can block malicious interest earlier than they attain other parts of the network.

c. Anti-virus and anti-malware applications —

Even as a firewall upgrade will increase protection, it gained stop assaults except antivirus and anti-malware applications are updated. Older software won't include the modern day guidelines and virus signatures. In flip, it could omit a potentially disastrous assault to your machine.

d. Multi-component authentication —

This safety, additionally referred to as MFA, is extremely important to defend customers who utilize cell or online apps to do their banking. Many customers by no means trade their passwords. Or, if they do, they make small changes. applying MFA stops attackers from reaching the network because it asks for every other degree of safety. for example, a six-digit code dispatched to a consumer's cellular phone.

e. Biometrics —

That is any other version of MFA even more at ease than a texted code. This shape of authentication is predicated on retina scans, thumbprints, or facial popularity to verify a consumer's identification. though hackers have accessed this type of authentication inside the beyond, it's far greater hard to accomplish.

f. Automatic logout —

Many websites and apps permit a person to live logged in in the event that they permit it. therefore, they can access their information at any time without coming into their login credentials. but, this also lets in attackers to without difficulty obtain your records. computerized logout minimizes this by way of final a consumer's get right of entry to after a couple of minutes of inactiveness.

g. Schooling —

All the above measures can growth cyber protection inside the banking quarter. Although, they are able to' assist if customers continue to access their facts from unprotected locations or improperly defend their login credentials. that is why training is crucial. When banks notify their clients of effects related to these vulnerabilities it could pass them to change their behavior for worry of dropping their investments.

6. Suggestions

1. Prioritizing cyber safety evaluation

A non-stop hazard assessment using a risk-based technique. The Cyber protection maturity evaluation, Bridging the gaps. An Integrating cyber chance evaluation with fraud chance and monetary crime reporting.

2. Tightening access to third-party services

A Prioritizing get admission to to and availability of offerings for alliance companions and companies, The limiting or controlling their get right of entry to to core infrastructure.A exploring the possibility of modifying contractual agreements to monitor third-party.

3. Get entry to banking infrastructure

Adopting superior era solutions and equipment. The growing many strains of protection at different stages in the security ecosystem. An Adopting defense alternatives for hazard intelligence and response competencies, along with: zero-believe structure, advanced endpoint security structures, increase cyber safety with AI, Develops

4.Securing remote get right of entry to manipulate

To permitting server-primarily based computing and virtual workspaces. A Deploying zero customers and thin clients, Reviewing remote connectivity answers and protection governance., A Deploying an advanced and sturdy authentication and authorization, choosing the scope of offerings that want secured get entry to

5. Contracting or outsourcing cyber protection skills

Coping with shortages of cyber protection specialists the usage of leading-area offerings of third-birthday party safety companies, considering outsourcing a myriad of cyber protection functions, inclusive of protection operations and insider chance detection (consisting of risk searching and risk intelligence)

6. Raising recognition via education

Introducing formal education programmes on cyber threats and cyber protection practices for employees, involving special methods to educate employees, growing cyber security subculture at every level and viewing it as a non-stop manner,

7. Bolstering security through hazard identification and response competencies

Integrating a present day and evolving security infrastructure while digitization, embedding protection, confidentiality, and coverage tests into their Develops choices and actions

7. Conclusion

Banks will in all likelihood undertake technologies including cellular, cloud, far off get right of entry to, and IoT, no longer out of desire however out of the want to preserve business all through the pandemic and thrive thereafter. Such transformative digitization may even result in an increased attack surface. For bank executives, the focal point might be on accomplishing business desires at the same time as they recalibrate strategies to address the ever-evolving cyber dangers.

Banks will need to priorities and put money into cyber protection to create an agile and resilient infrastructure of the destiny. Such an infrastructure will address the modern cyber protection dangers and put together itself for cyber challenges of the destiny. but, for that to take place, the initiative has to come back from financial institution executives and board individuals who set desires and allocate price range. Accelerating cyber skills to suit the speed of virtual transformation would require govt attention, prioritization, price range, resources, and governance. only the leadership can force such a change. Banks' leaders will decide the degree of agility, tempo of trade in infrastructure, and collaborative efforts required toward constructing cyber safety of the future

Reference:

1. Aditi Mittal and Sumit Gupta "Emerging role ofinformation technology in banking sector's developmentof India" Acme International Journal ofMultidisciplinary, Volume – I, Issue – IV April – 2013ISSN: 2320 – 236X

2.BhosaleSatishTanaji, SawantB.S, "Technological Developments in Indian Banking Sector."

3.Kiran Kumar T.V.U., Karthik B., Improvingnetwork life time using static cluster routing for wirelesssensor networks, Indian Journal of Science andTechnology, v-6, i-SUPPL5, pp-4642-4647, 2013.

4. Arul Selvi S., Sundararajan M., SVM based twolevel authentications for primary user emulation attackdetection, Indian Journal of Science and Technology, v-9,i-29, pp—, 2016.

5. Kanniga E., Selvaramarathnam K., SundararajanM., Embedded control using mems sensor with voicecommand and CCTV camera, Indian Journal of Scienceand Technology, v-6, i-SUPPL.6, pp-4794-4796, 2013.

6. KPMG, "Technology enabled transformation in Banking", The Economic Times Banking Technology, Conclave 201.

7. Lakshmi C., Sundararajan M., Manikandan P.,Hierarchical approach of discriminative common vectorsfor bio metric security, 2010 The 2nd InternationalConference on Computer and Automation Engineering,ICCAE 2010, v-2, i-, pp-784-790, 2010.

8. Nair G.K. and Prasad P.N., 2002. Development through Information Technology in Developing countries: Experiences from an Indian State, The Electronic Journal of Information System in Developing Countries.

9. Venkataganesan K.A., Mohan Kumar R., BrindaG., The impact of the determinant factors in the career satisfaction of banking professionals, InternationalJournal of Pharmacy andTechnology, v-8, i-3, pp-17431-17436, 2016.

10.Sambantham M.C., Venkatramaraju D., Humanresources management (HRM) practices in multinationalcompanies with reference to knowledge transfer,International Journal of Pharmacy and Technology, v-8,i-3, pp-18565-18571, 2016.

11. Alper Kerman, Oliver Borchert, Scott Rose, Eileen Division, and Allen Tan "Zero Trust Architecture", NIST-NCCOE, 2020, https://www.nccoe.nist.gov/projects/building-blocks/zero-trust-architecture

12. Mangnale V.S, ChavanJ.V ,Randive A.D, " E –CRM in Indian Banking Sector, Golden Research Thoughts.

13. Brindha G., Emerging trends and issues inhuman resource management, Middle -East Journal ofScientific Research, v-14, i-12, pp-1727-1730, 2013.

14. Payment Systems in India-Vision 2012-2015. • Report on Trends and Progress of Banking in India-2009-2013,RBI

15.Uppal R.K., ¯Customer Perception of E ▪ %/h-#/▪Banking Services of Indian Banks: Some Survey Evidence, The ICFAI Journal of Bank Management, Vol. VII No.10.

16. Reserve Bank of India, RBI releases the financial stability report, July 2020, July 24, 2020, https://www.rbi.org.in/Scripts/BS_Press

ReleaseDisplay.aspx?prid=50122 Cybersecurity in the Indian banking industry - Part 1

17 "Cyber resilience assessment framework", Hong Kong Monetary Authority, May 2016, https://docplayer.net/85773113-Cyber-resilienceassessment-framework-consultation-draft.html

18. Deborah Golden, "AI-augmented cyber security", Deloitte, June 08, 2017, https://www2.deloitte.com/us/en/insights/industry/public-sector/addressing-cybersecurity-talent-shortage.html

19. Note: A few of such security solutions are security information and event management (SIEM) and security orchestration, automation and response (SOAR).

20. Deborah Golden and IrfanSaif, "The future of cyber survey 2019", Deloitte, 2019, https://www2.deloitte.com/us/en/pages/advisory/articles/future-of-cyber-survey.html

21 Deborah Golden, Jason Frame, Kelly Miller Smith, "COVID-19: Cyber Preparedness & Response", Deloitte, https://www2.deloitte.com/content/am/Deloitte/za/Documents/risk/COVID-19%20Cyber%20Preparedness %20and%20Response.pdf;

Note: A few of such security solutions are security information and event management (SIEM) and security orchestration, automation and response.

❑❑❑

03

Farmers at the crossroads: Human-Nature Relationship in Sadanand Deshmukh's *Baromaas*

Rajendra Tambile
Assistant Professor, Department of English
Shripatrao Kadam Mahavidyalaya, Shirwal
(Shivaji University, Kolhapur)

****

Sahitya Academy awardee writer Sadanand Deshmukh's *Baromaas* throws lights on the various aspects of agrarian life of India. Majority rural population of India engaged in farming. Agriculture is the profession which not only includes the farming but customs and tradition, overall cultural lifestyle related to it. The author of the novel, Sadanand Deshmukh himself was born in such an agrarian family. His father was a farmer belonged Marathwada region of Maharashtra. This part of Maharashtra always remained under drought-prone. *Baromaas* is his second novel published in 2002, which means '*twelve enduring months*'. The farmer community is always under threat either of nature or the money lenders. These money lenders illegally lend money to the farmers and give very inhuman treatments to them when they are not able to pay the debt in time. The farmers are humiliated by such people on one side and there is no minimum support price to the agricultural produce on the other side. The only way remains for the farmers is to commit suicide. Farmers from Maharashtra are among the most hardworking, adoption of scientific inputs is high, basic support infrastructure have much improving over the years and still high levels of stress. This is one side of the picture. The other side of the picture is not so encouraging. The number of farmers' suicide is very high in the state.

Everyone should consciously mind that nobody commits suicide happily. The farmer community is very much conscious about its respect and honour, hence if they get humiliated, they cannot bear it and embrace death. The farmers are considered as the *Annadata,* but the same people are suffering a lot. After Independence our country was insufficient in the food grains, the government of India used to export from other countries like the U.S. and European Countries. Our farmers made India excess in food. Farming is considered the main occupation of the country. Today, the condition of the farmers is not so good. Farmers produce the food and give everything to India but they have nothing. Indian agriculture is under great depression. The changing technological developments and changing government policies changed the attitude of the people and the generation born after 1991. The people are forgetting the fact that man can live without modern technology but cannot survive without food.

The story of the novel moves around a young man named Eknath. He spent his childhood in a small village with his parents and other relatives. His family occupation is farming from his forefathers. His grandfather was a farmer, so his father was. But there is a generation gap of thinking. Eknath's grandfather was strongly against the modern techniques of farming. He believed in the traditional way of farming and was against the use of chemical fertilizers and advanced BT seeds. He even refused to consume food grown in the farm where chemical fertilizers are used. But on the other hand, Eknath and his father thought of a modern way of agriculture. The farmers do hard work in their farms but natural calamity like famine is always there. It does not leave farmers aside and let them suffer. The natural conditions by and large are against the farmers. Hence there is news in daily newspapers about the killing of self by the farmers. Eknath is post graduate in Marathi literature. His family took great efforts for his education. Though he secured good marks, he could not get the job. Being a member of farmer's family Eknath did not have money to fulfil the donation of the employer. His younger brother Madhu wanted to sell some piece of land in order to fulfil the demand for donation but everybody was against this idea. Sometimes Eknath thought the same idea. But some part the land was sold when Madhu got the chance of job of gramsevak. The savkar –money lender cheated Madhu's family by adding extra conditions on the paper. Madhu gave money to the middle man Sathe for his job, but unfortunately died in an accident and the P.A. of the MLA took the money and refused to give any assurance of job to Madhu. His family thus gets badly affected by this betrayal. Madhu made a gang of such unemployed boys and they used to dig for the secret wealth buried by their forefathers. One of the boys his gang Dilip went crazy due to unemployment and his craziness lingered in the novel till the end. Madhu's gang did not get any wealth and became robbers in the end. On the other hand, Eknath wanted to have money in order to fulfil the donation; he did new experiments on the farm. This has created many familial problems in Eknath's life. There was always quarrel between his mother and his wife. His wife Alka left Eknatha and went to live with her parents. The misery became worst when Subhanrao Eknath's father commits suicide due failure of the crops and by accepting the responsibility of the failure of the family. Moreover, Eknath's brother-in-law embraced death as he could not repay the money he took from the money lender. Actually, the money lender imposed illegal and unnatural interest which made him impossible pay and he committed suicide.

Every government always says that the crop loan system for the farmers is eased and they will not have to suffer for getting the fresh crop loans. The govt. advertises for such schemes as a part of their political agenda. It just makes a show that the govt. is working for the welfare of the farmer community by offering various schemes. The govt. increases the minimum support price of crops every year, but the middlemen don't allow the farmers to share their profit. In the end, the farmers don't get the direct benefit of any of the govt, schemes. The banks say that they are willing to give all kinds of loans to the farmer with minimum documents. But the ground reality always remains something different. The banks many times demand unnecessary documents and put such conditions before the farmers which they cannot fulfil. In Baromaas also the writer throws light on this issue. Here Balimama, Eknath's maternal uncle wanted a fresh crop loan by renewing the old loan. The bank demands the papers of the farm for the sanction of the loan. The talathi (the lowest rank revenue officer of the system) is avoiding giving the papers by giving unnecessary reasons. Balimama abuses the system. On the one side government says that farmers will get their papers related to farm at their home as and when the demand. But the talathi wants a bribe from the farmers. Until Balimama gives the talathi fifty rupees he will not give the papers. This is nothing but the insult into the injury of the farmers. Though Balimama gets the papers still it not easy to get his loan renewed. The bank officer rejects his proposal by showing him the waiting list of the farmers who are in the line of getting loans. Thus renewal of the crop loan becomes the difficult work for Balimama. Eknath started working in the farmer's movement. He tells the farmers about the advanced farming and crop techniques in the farm. He tries to convince the farmers about the ways of modern farming. Eknath feels that try new crops and especially fruit farming. He is in favour of globalization and he says that the government should not impose on exports. He advocates the problems of farmers, loans, debts, loss of production value at APMC. He strongly feels that nature, money lenders and government policies are enemies of farmers and they are responsible for the destruction of farmers.

Agriculture is an unorganized activity; moreover, the most farmers are small and economically unfeasible. Middlemen and exploitation of farmers and Government programmes do not reach the farmers. High indebtedness and exorbitant interest rates of the illegal money lenders are other problems. The farming and farmers are hit badly due to climate change. The increase in global temperature with increased concentrations of anthropogenic greenhouse gases is negligible so also the impact of this on sea level rise, ice melts, etc are also negligible. This affects the crops. A large number of populations of our country are engaged in agriculture and allied activities. It fulfills the fundamental needs of the people. When our country got freedom from the long pertained British rule by that time we were deficient in food and other edible items. The challenge was accepted by the farmers and made India excess in food production. The whole credit should be given to the farmers. They have achieved the green revolution and made our nation proud by making it independent in food grains. But today this sector is undergoing many problems and these are very serious. The number of farmers' suicide is increasing day by day. This is not a proud picture of the country whose main occupation is farming. They face many natural and manmade as well as policy made problems though they do hard work on the farm. This leads them to the great depression and suicide in the end. The pro-capitalist policies of the government have created much chaos among the farming community. Illegal acquisition of land either by the government or by the capitalists is another major issue. No government today is looking at farmers' problem seriously. The required infrastructure for the industry is made ready quite easily but the infrastructure needed to agriculture is not developed. The irrigation projects take a longer time to complete and farmers do suffer a lot due to such negligence. The farmers' movements are trying to educate farmers regarding the problems faced by them. Though such movements are successful in creating awareness among the farmers, still the success is limited. Those who lead the movements, later on, do the tie-up with some political party and gain a seat either in assembly or parliament and ignore the welfare of the farmers.

Works Cited:

1. Deshmukh, Sadanand Baromaas
2. The Punjab State Co-op. Apex Bank Ltd Department of Co-Operation, Government of Punjab. *Suicides in Rural Punjab.* 1998. Print

3 . Hawton K, Fagg J, Simkin S, Harris L, Aslog M. *Methods used for Suicide by Farmers in England and Wales*. 1998;173:320-4.

4. http:// ww.VidarbhaJanAandolanSamiti.com.

5. Behere P.B., Rathod M. *Report on farmers' suicide in Vidarbha. Wardha*: Report submitted to Collectorate. 2006. Print

6. Gururaj G, Isaac MK. *In Mental Health: An Indian perspective 1946-2003*. Pub Ministry of Family Welfare and Health, Government of India; 2004. *Psychiatric epidemiology in India: Moving beyond numbers*; pp. 37–61.

7. National Crime Records Bureau [NCRB] Ministry of Home Affairs. New Delhi: Government of India; 1999. Accidental Deaths and Suicides in India.

8. Desai P.T. *India Today, Farmers suicide*. Delhi: Living Media India Ltd; 2006. Feb 27,

9. Deshpande S.H. *Hitwada Farmers of Vidarbha at crossroads*. Guest Column. Thursday, June 7, 2007.

04

A Study of Cyber security management in India

Dr. Rani Somnath Shitole
Shri Shahu Mandir Mahavidyalaya, Pune

****

Abstract

Cyber security is a very significant because it protects data of all categories from theft and damage. Cyber security is become essential for the entire organizer all over the world. It covers all aspects of transactions and activities on and involving the Internet, World Wide Web and Cyberspace. Now days more and more business and social users are online. Not only big but small companies also face threat of cyber attack, if they don't keep their security strong. The Indian Cyber laws are governed by the Information Technology Act, 2000. It is passed by the parliament of India.

Keywords: Introduction, Cyber Threats, Classification of Cyber Crimes.

INTRODUCTION:

Cyber security is a very significant because it protects data of all categories from theft and damage. Cyber attack can happen at global level, so proper protection is required to face the problems of cyber attacks. Now days more and more business and social users are online. Not only big but small companies also face threat of cyber attack, if they don't keep their security strong. Almost large organization uses cloud storage service to store their data. If proper measures are taken to protect the data then this data can be subjugated by cyber criminals. Cyber security is become essential for the entire organizer all over the world. It covers all aspects of transactions and activities on and involving the Internet, World Wide Web and Cyberspace.

The Indian Cyber laws are governed by the Information Technology Act, 2000. It is passed by the parliament of India. It focuses on the serious punishments and penalties safeguarding the e-governance, e-banking and e-commerce sectors. Important sections of this act are as follows:

Section 43:

It is applicable to people who damage the computer systems without permission from the owner. In this case owner can fully claim for compensation for the entire damage.

Section 66:

This section is applicable in case of a person is found dishonestly committing any act referred to in section 43. In this case the imprisonment term is upto three years and fine of Rs. 5 lakh

Section 66 B:

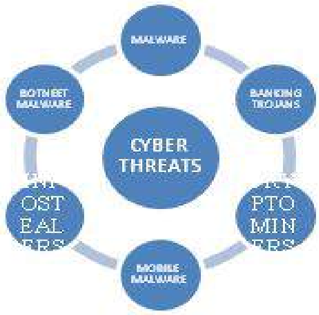
Dishonestly receiving stolen computer source or communication device with punishment upto there years or 1 lakh rupees as fine or both.

Section 66C:

Electronic signature or other identity theft like using other passwords or electronic signature etc. Punishment is three year imprisonment or fine of 1 lakh rupees or both.

Cyber Threats:

A cyber security threats refers to any possible spiteful attack that seeks to unlawfully access data, disturb digital operations or damage information. Cyber attackers can use on individual's or company's sensitive data.



Ransomware:

This is malware designed to use encryption to fore the target of the attack to pay a ransom demand. It has became one of the most visible and creative type of malware.

Malware:

Malware comes in a variety of different forms and can be used achieve a number of different objectives. In 2020 these types of common forms of malware included. Malware can install on computer manually by attackers.

Cryptominers:

It is online threat that hides on a computer or mobile device.

Mobile Malware:

It is targeting mobile devices. It specifically targets the operating systems on mobile phones.

Botnet Malware

This type of malware is infects a system and add to a botnet. The risks associated with botnets are exactly the same as the risk associated with malicious software in general.

Infostealers:

This malware collect very sensitive information from an infected computer and send it to the malware operator.

Banking Trojans:

This type of malware specifically target financial information.

Classification of Cyber Crimes:

- CRIMES AGAINST INDIVIDUAL
- CRIME AGAINST ORGANIZATION
- CRIMES AGAINST SOCIETY

Crime against individual:

These types of crimes committed against individuals or their properties. E.g. e-mail harassment, cyber stalking, unauthorized control over computer etc.

Crime against organization:

These types of crimes committed against organizations such as possessing of unauthorized information, cyber terrorism against government organization etc.

Crime against Society:

These types of crimes committed against society such as trafficking, financial crimes, online gambling etc.

Online Gambling: It is generally means the use of internet to place bets and earns money on internet. In India millions of people are connected online to each other daily. Online gambling is similar to playing in casino but the difference is that it is held in a virtual environment.

E-mail Bombing: In e-mail bombing is often done from a single system in which one user sends 100 or 1000 messages to another user. The main purpose of it to overflow the user inbox.

Web Jacking: This method is mostly used in social media where the attacker create a fake website and when the website is open it will redirect it to on another website and harm the user system.

Cyber Warfare: It is the use of cyber attacks against a nation-state causing it significant harm. It damage network system of another nation by this attack.

CYBER CRIME STATEWISE (2016-2018)

S.NO.	STATE	2016	2017	2018
1	Andhra Pradesh	616	931	1207
2	Arunachal Pradesh	4	1	7
3	Assam	696	1120	2022
4	Bihar	309	433	374
5	Chhattisgarh	90	171	139
6	Goa	31	13	29
7	Gujarat	362	458	702
8	Haryana	401	504	418
9	Himachal Pradesh	31	56	69
10	Jammu & Kashmir	28	63	73
11	Jharkhand	259	720	930
12	Karnataka	1101	3174	5839
13	Kerala	283	320	340
14	Madhya Pradesh	258	490	740
15	Maharashtra	2380	3604	3511
16	Manipur	11	74	29
17	Meghalaya	39	39	74
18	Mizoram	1	10	6
19	Nagaland	2	0	2
20	Odisha	317	824	843
21	Punjab	102	176	239
22	Rajasthan	941	1304	1104
23	Sikkim	1	1	1
24	Tamil Nadu	144	228	295
25	Telangana	593	1209	1205
26	Tripura	8	7	20
27	Uttar Pradesh	2639	4971	6280
28	Uttarakhand	62	124	171
29	West Bengal	478	568	335

(https://ncrb.gov.in/sites/default/files/Crime%20in%20India%202018%20-%20Volume%202_1_0.pdf)

AS per the data shown in above table, shows that in 2018 cyber crime cases are increased as compared to 2016 and 2017. In state of Uttar Pradesh, Maharashtra, Telangana, Rajasthan, Karnataka, Assam and Andhra Pradesh cyber crime cases are rapidly increased. In the state of Mizoram, Nagalan, Skkim and Arunachal Pradesh there are very less number of cyber crimes cases are shown in the above table.

Avoid cyber crime by using strong password, secure mobile data, protect computer with security software etc. There is need to create awareness among the people regarding cyber crime. In education institutions workshops, seminars and conferences should be organized on the cyber crime and security subject.

References:

1. https://www.latestlaws.com/wp-content/uploads/2015/05/Cyber-laws-in-India.pdf

2. https://taxguru.in/wp-content/uploads/2012/10/cyber-laws-overview.pdf

3. https://onlinedegrees.und.edu/blog/types-of-cyber-security-threats/

4. https://www.toppr.com/guides/business-laws-cs/cyber-laws/classification-of-cyber-crimes/

5.https://www.cybercrimechambers.com/blog-web-jacking-117.php

6. https://ncrb.gov.in/sites/default/files/Crime%20in%20India%202018%20-%20Volume%202_1_0.pdf)

❑❑❑

05

Cyber Security: issues and Challenges for E-Commerce in Modern Era

Prof. Velekar Laxmikant Chandrakant
Mudhoji College, Phaltan

****

Abstract:

E-Commerce sites will always be a hot target for cyber attacks for would be thieves, they are treasure troves of personal and financial data. An for businesses of all sizes, the cost of a breach both in loss of data and in customer trust can be hugely damaging for businesses of all sizes.

E-Commerce business owners are all too aware of these issues and are increasing their security measures. The VM ware carbon black 2020 cyber security outlook Report found that 78% of businesses surveyed had purchased new security products in the last year and 70% had increased security staff.

In this constant game of cat and mouse, as online retailers add increasingly innovative technologies to their sites to stay competitive, cyber attackers are equally honing their skills and finding new vulnerabilities to exploit. The best way to stay ahead is to be aware of e-commerce security best practices and the types of attacks to be on the lookout for.

In this research paper researched mentioned Need of cyber security E-commerce in present scenario, cyber security, issues and challenges for E-commerce in modern era. This paper provides directions for e-commerce security to improve customer confidence in e-commerce shopping.

Key Words: Cyber Security, Malware, Software Vulnerabilities, E-commerce, Challenges and issues.

Introduction:

The development of digital era in every aspect of life that is not excluding to the trade sector with the emergence of e-commerce features that offer convenience in shopping make the community seem powerless to contain it. Such developments of course in addition to bringing positive impact also brings negative impact of the cyber crime potentials in electronic transactions on e-commerce such as theft of personal data and fraud is rife through e-commerce today criminal law in this case provides both penal and non-penal bidders to cope them.

The rapid expansion of computer connectivity has provided opportunities for criminals to exploit security vulnerabilities is the online environment. Most detrimental are malicious and exploit code that interrupt computer operations on a global scale and along with other cyber crimes threaten e-commerce. In response to the threat of cyber crime there is an urgent need to reform methods of mutual legal assistance and to develop transactional policing capability. So in this paper I have mentioned cyber security some issues & challenges in e-commerce & high lighten some major solutions on it, which is useful to business sector & consumer in present scenario.

Objectives of the Study:

1) To study need of cyber security in e-commerce.

2) To know cyber security issues in e-commerce in present scenario.

3) To study various cyber security challenges for e-commerce in modern era.

Research Methodology:

The descriptive methodology has been used to collect data. Secondary data has been collected from various published sources, reference books, journals, periodicals, newspaper, internet websites.

Need of Cyber Security in E-commerce:

Cyber-security represents may be the most important e-commerce feature. Without the existence and implementation of proper protocols, online store owners put themselves and also their customers at risk for payment fraud more than financial consequences, data breaches harm an e-commerce websites reputation.

E-commerce site security is critical for a number of reasons, specifically when it comes to protecting the privacy and sensitive data of customers on a website, safeguarding the finances scams and defending the reputation of an online store as a safe place to conduct.

The foundation of success in the digital world is having the proper cyber security measures in place to protect consumers, employees, and the business itself from constant security threats cyber security is woven into the very fabric of business operations and has special impacts on the e-commerce sector.

The importance of cyber security cannot be emphasized enough many brands are often wondering what steps can be taken to improve practices, customer satisfaction, and ultimately increase revenue streams security should not be overlooked because it often provides the solution to the challenges many e-commerce brands are facing security has wide reaching effects that can truly help lead to positive changes in e-commerce venture.

Cyber Security issues in e-commerce in present scenario:

Online retailers use a wealth of innovative new technology to give their business a boost machine learning technology that improves conversion rates or site-search analytics that provide deep insight into shopper behavior.

However, as online stores become more advanced, it’s important to keep up with the significant security risks that come with it. In this blog we’ll explore the different that you should be aware of and the best methods to avoid them in 2020.

Cyber security issues in e-commerce in

present scenario as under.

1) Malware:

Malware is any piece of software that's been designed by cyber criminals with the intention of gaining access or causing damage to a computer network. Inserted into web pages through techniques like SQL injection, malware files can allow hacker to:

i) Fake (Spoof) their identity

ii) Take control of your computers and networks.

iii) Tamper with your databases

iv) Send malicious emails on your behalf

Because malware strategies are constant evolving so too must your anti-virus protocols, to protect your site against security threats to e-business.

2) Account acquisition:

The theft and selling on of login details is a major industry in the darker corners of the web once a hacker has these credentials, they can send out bots to try username and password combinations on many different retail sites until they're successful. Once in, the hacker has free – rain to place orders, steal card details and more.

3) E-skimming:

E-skimming refers to hacker methods of stealing personal data, such as credit card information, from payment card processes pages on e-commerce sites its' as significant security risk in e-commerce, as shoppers can be misguided by misleading external links and portals to payment pages or cyber – criminals gain access to your site via a third – party, a successful phishing attempt, or cross – site scripting.

4) Price Scraping:

Price Scraping bots can be sent by competitors to monitor your pricing strategy, inventory levels, marketing plans and more allowing them to undercut your prices or outrank you in search engine results.

5) Distributed Denial of Service (DDOS) Attack

Cyber Security challenges for E-commerce in Modern Era.

Cyber security is becoming a severe issue for individuals, enterprise and governments alike. In a world where everything is on the internet, from cute kitten videos and our travel diaries to our credit card information, ensuring that our data remains safe is one of the biggest challenges of cyber security. Cyber security challenges come in many forms such as ranosmware, phishing attacks malware attacks and more. India ranks 11th globally in terms of local Cyber attacks and has witnessed 2, 299, 682 incidents in Q- 1 of 2020 already.

Cyber Security challenges for E-commerce in modern era as under.

Ransomware attack

1) IOT attacks
2) Cloud attacks
3) Phising attacks
4) Blockchain and cryptocurrency attack
5) Software vulnerabilities
6) Machine learning and AI Attacks
7) BYOD Policies
8) Insider Attacks
9) Outdated Hardware

Challenges of E-Commerce:

Now days due to rapid growth of E-commerce challenges will work as a hindrance for customer satisfaction challenges are as under.

1) Snooping the shopper's Computer:
2) Personal Firewall:
3) Cross-site Script (XSS):
4) Ethical hackers:

Conclusion:

E-commerce security is a piece of the information security framework and is specifically applied to the component that affects e-commerce including of Data security and other wider realms of the Information security framework. E-commerce security is the protection of e-commerce assets from unauthorized access. Use alteration or destruction. E-commerce offers the managing an account industry great chance, yet additionally creates a set of new dangers and vulnerability.

E-commerce is one of the way through which many things can be streamlined and flexibility with convenience can be provided to users. So that cyber security aspects must be considered while making all the transactions digital. E-commerce security is the protection of e-commerce assets from unauthorized access.

References:

1) A Bhattacherjee Individual trust in online firms: scale development and initial test Journal of management information system, volume 19, issue 1, P. 211-242.

2) Adam Jolly The secure online business; Great Britain and the united states, P. 93-118

3) Biswajit Tripathy, Jibitesh Mishra "Protective measures in e-commerce to deal with security threats arising out of social issues a frame work – ISSN 976-6375 (online) volume 4.

4) Cyber Warfare – techniques tactics and tool for security practitioners.

5) Exbal Hamirani, RK University The challenges for Cyber Security in E-commerce, International conference on Digital culture – changing global Landscape at Mumbai.

6) Jason Andress a Steve Winterfeld The Best E-commerce security practices – https://www.getastra.com

7) Nikmah Rosidah, Chaidir Ali –Construction of Non-penal effects to prevent cyber crime on E-commerce.

8) Review of e-commerce security challenges by Jarnail Singh in International Journal of Innovative Research in Computer and Communication, Engineering.

9) Ross Anderson Why cryptosystems fail communications of the ACM, volume 37, issue 11, P. 32-40

10) www.google.com

❑❑❑

06

LAWS TO PROTECT WOMEN AGAINST CYBER CRIMES – A STUDY

Dr. Caesar Roy
Assistant Professor of Law,
Surendranath Law College, Kolkata, West Bengal

****

Abstract

India stepped toward digitalization which brought technological power. People explore using internet and made life easy and comfortable. They explore the unknowns and communicate with virtually anyone, anytime, anywhere across the world. Digital space has opened doors to criminals in cyber space and mostly woman is their target. Computer and internet has positive impact in our society. But with use of such science and technology particularly internet, crimes against women are increasing day by day and at the same time this technology becomes a curse. These types of crimes are called cyber crimes though there is no fixed definition of cyber crime. After passing of time, women are victimized sometimes by the use of internet technology. The cyber crimes against the women through the use of internet include sexual crimes and sexual abuses. Today these types of crimes are the fastest growing crimes in the world. In this paper, various kinds of cyber crimes against women and also the relevant provisions of law are mentioned. The reasons are also made out for such crimes in this paper. Lastly some suggestions are made to make this more effective.

Keywords – cyber crime, women, science and technology, internet

Introduction

In India women are placed with very high regards. They are worshipped as Goddess in India. The crime against women in the era of science and technology is increasing day by day not only in India but throughout the world. These types of crimes against women cause great damage to the victims through the use of computers and internet technology. The unknown and transnational natures of the internet make it an easy weapon in the hands of the miscreants in the society and women owing to their vulnerability are most often victimized. Actually internet was created to make our life easier which mainly started to use it as an important tool for learning, evolving and entertaining oneself. By the use of internet technology, women throughout the world are getting enriched. But after passing of time, women are victimized sometimes by the use of internet technology. The crimes against the women through the use of internet include sexual crimes and sexual abuses in the internet. Presently, the privacy, dignity and security of a woman are in danger. Trolling, threatening, stalking, revenge porn, defaming, voyeurism, abusing, body-shaming, surveillance and other forms of indecent representation of women are very common nowadays. Though India has law on this point but the crimes are still reported every day.

Various cyber crimes against women

Women are victimized more often by some specific notorious crimes in the era of technology and digitalization targeting their repute, owing to their gender vulnerabilities. The crimes against women in science and technology are given below.

Cyber harassment

Cyber harassment is characterized by a repetitive behaviour intended to disturb or upset or annoy a person through the medium of internet. The use of emails and social networking sites are generally done to target women for harassment by various ways which may include blackmailing, threatening, bullying, cheating, impersonation etc. undoubtedly being a victim of online harassment creates annoyance and anxiety. Cyber sexual harassment is an intimidating and menacing as the physical or offline sexual harassment. The internet is largely abused as a medium, as cyber harassment has many forms and its incidence is growing in numbers.[1]

Cyber stalking

Stalking in common parlance means a harassing or threatening behaviour which an individual exhibits towards the other. If an individual uses cyber space for stalking then it is called cyber stalking. Thus cyber stalking is an online course of conduct of a person by which the targeted person is terrorized, embarrassed, ashamed, molested, outraged or frightened.[2] The women and children are targeted most. They are online harassed and abused with the use of internet.

Cyber pornography

This is another threat to women and children because this includes publishing pornographic materials in pornography websites by using computers and internet. Women are becoming the main victim of this flip side of technology. Information technology has intensified the nature of the crime of cyber pornography, as it has made it much easier to create and distribute pornographic material through internet. Such material could be transmitted all over the world in matter of seconds.[3]

Morphing

Morphing is editing the original picture so as to make it look completely or largely different. Often criminally minded elements of the cyber world download pictures of girls from websites such as Facebook and then morph it with another picture in compromising situation so as to represent that those women were indulging in such acts. Often the next step after this is to blackmail those women through the threat of releasing the morphed images and diminishing the status of those women in society.[4]

Cyber defamation

With the aid of internet and computers when someone publishes any derogatory or defamatory information of one in cyber space, it is called cyber defamation. Although cyber defamation can be made against both men and women but women are more vulnerable.

Email Spoofing

E-mail spoofing is a term used to describe fraudulent email activity in which the sender address and other parts of the email header are altered to appear as though the email originated from a different source. By changing certain properties of the email, such as the From, Return-Path and Reply-To fields, ill intentioned users can make the email appear to be from someone other than the actual sender.

Hacking

The word 'hacking' has been much used and abused in the information technology lexicon. Computer hacking is the accessing of a computer system without the express or implied permission of the owner of that computer system. Hacking is an intentional and coordinated activity. It is preplanned process, where first a target is identified; its security features are studied; tools are developed (password and programmes) to gain unauthorized access and impair the normal (programmed) functioning of a computer or computer system (or network).[5] These types of crimes are committed against the women mostly.

Cyber bullying

Cyber bullying means sending messages to unknown person which is of an intimidating or threatening nature.

Laws on cyber crimes against women

The crimes against women in science and technology are new. As per Resolution adopted by the General Assembly of the United Nations[6] on Model Law on Electronic Commerce, 1996 as adopted by the United Nation Commission on International Trade Law (UNCITRAL), Indian Parliament has enacted Information Technology Act, 2000. This Act was enacted to give protection of electronic commerce and communication. So the main object is to facilitate international trade. Later this Act was amended in the year 2008 to curb the new crimes against the women in the era of science and technology.

Beside this Act, India Penal Code, 1860 is also applicable to curb these types of menaces. After the 2012 Delhi Gang Rape case (Nirbhaya Case) there has been a huge outcry over bringing out new reforms and penal provisions so as to protect women against the criminally minded. The 2013 Criminal Law (Amendment) Act contains several additions to the Indian Penal Code, such as to sections 354, 354 A, 354 B, 354 C & 354 D, with the assistance of these sections now the issues of MMS scandals, pornography, morphing, defamation can be dealt in proper manner.

Section 67 of Information Technology Act, 2000 deals with publication or transmission of obscene information in electronic form. So any obscene publication or transmission in electronic form is covered by this section not by section 292 of Indian Penal Code which does not deal with electronic substances. Unlike other crimes like Cyber Stalking, Cyber Defamation, Morphing, Email Spoofing, Cyber Pornography is considered an exceptional case which has been covered by the Information Technology Act 2000 to a certain extent by Section 67 of the Information Technology Act 2000.

Cyber stalking is not covered by the Information Technology Act, 2000. It can be booked under section 72 of the said Act by which an offender may be prosecuted for breach of confidentiality and privacy. The accused may also be prosecuted under Section 441 of the Indian Penal Code for criminal trespass and Section 509 of the Indian Penal Code again for outraging the modesty of women.

Cyber defamation is not defined by the Information Technology Act 2000. It is well explained in section 499 of Indian Penal Code. Whoever defames another shall be punished under section 500 of the Code, whereas section 501 of the Code deals with printing and engraving matter known to be defamatory.

Section 43 of Information Technology Act is a very important provision in the sense that it identifies ten different causes of causing damage to computer, computer system and computer network. Likewise section 43A states about failure to protect any sensitive personal data or information.[7] Whereas according to section 66 of the Act, if any person dishonestly or fraudulently does any act referred to in section 43, he shall be punishable. Section 66A was created to curb the menace of sending offensive messages by means of a computer resource or a communication device. Section 66C is meant to protect the identity of a user in the online medium. The objective of the section is to protect the privacy of all or any online users, including their personal information or data. The offences of creating clone websites, e-mail frauds, e-mail forgeries, data theft, loss of privacy etc. are covered by section 65D of the IT Act. Section 66E of the IT Act deals with punishment for violation privacy of a person. Such as knowingly captures, publishes or transmits the images of a private area of any person without consent. Section 66E should now be applied in conjunction with section 354A (Sexual harassment and punishment for sexual harassment), 354B (Assaults or use of criminal force to woman with intent to disrobe), 354C (Voyeurism) and 354D (Stalking) as introduced by the Criminal Law (Amendment) Act, 2013.

Sections 66 (hacking of the computer system; first proviso to the said section states that whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value, its utility or affects injuriously by any means, commits hacking) of the Information Technology Act 2000. The perpetrator can also be booked under the Indian Penal Code for criminal trespass under Section 441, Section 290 for committing public nuisance, Section 292A for printing or publishing grossly indecent or scurrilous matter or matter intended to blackmail and under Section 501 for defamation.

Section 67A of the IT Act deals with punishment for publishing or transmitting of material containing sexually explicit act or conduct etc. in electronic form.

Various reasons for Cyber crimes

The reasons for the increasing crimes against women in science and technology as stated above are mentioned below –

(i) Very few provisions of these types of crimes as mention above are covered by the specific provisions of Information Technology Act, 2000. So proper prosecution cannot be done due to the absence of proper legal provisions in India

(ii) Transcendental nature of Internet is one of the main reasons for the growth of cyber crime so whereas Section 75 of the Information Technology Act deals with the offences or contravention committed outside India but it is not talking about the jurisdiction of the crimes committed in the cyberspace specially the question of place for reporting the case arises when the crime is committed in one place affected at another place and then reported at another place.

(iii) Woman and child cyber harassment and related cyber-crimes remain overwhelmingly underreported due to associated stigma and propensity of parents/guardians to not involve police in such matters.

(iv) Process of reporting such these types of crimes against woman needs to be simplified and identity of women involved protected to ensure such crimes do not go unreported. It is necessary simplify and strengthen these types of crimes investigation involving woman and children. Cyber laws have not been formulated properly and the procedure for registering a complaint is not known by woman.

(v) Woman harassment and exploitation in cyber space is increasing with updated technology and anonymity. It takes huge time for investigation and many times cases are unsolved due to lack of Cyber Forensics laboratories.

Suggestions

After discussing all about the crimes as stated above, some suggestions are put forward to make it more effective –

(i) There should be a Digital Police Portal or E-Portal where woman can report their problems online. This could reduce the number of cases which are not reported due to associated stigma and propensity of parents/guardians to not involve police in such matters. The portal will also maintain the database of criminals which could really help law enforcement agencies.

(ii) The increasing numbers of crimes against women are a great concern for any state however, cybercrimes make it even more challenging as criminals have the opportunity to create fake identities and then after indulge in illegal activities. To counter this, government should make stricter laws to apply on the Internet Service Providers (ISP), as they alone have the complete record of all the data being accessed by anyone surfing on net. ISPs should be made to report any suspicious activities that any individual is indulging into, this will help to curb crimes in nascent stage.

(iii) Legislation needs to make stricter regulation for cyber cafes, who should keep a record of their customers who utilized their internet services, often people, go to cyber cafes to indulge in criminal activities so as their own IP addresses are not revealed in any future investigation. This is another manner to mask identity.

(iv) Cyber Police Stations and Cyber Crime Cells should be set up in each State for reporting and investigation of Cyber Crime cases.

(v) Don't share passwords. Use your discretion and keep those passwords private and complicated.

(vi) Don't leave your webcam connected There are too many apps capable of turning on your camera and slyly recording your movements without your knowledge. As a precaution disable camera permission and keep the lens of your camera closed or covered when not in use.

(vii) The investigating agencies and prosecutors should be well trained and equipped with the knowledge of computer and internet.

(viii) All operating systems should be updated on the devices. They are very important to keep safe. Security updates and patches keep the latest threats away. The devices should be secured with anti-virus software.

(ix) It is needed to collaborate both police force and cyber forensic laboratories together for better investigation.

(x) Girls should be made aware about all types of cybercrimes and how to handle them. Spreading awareness regarding safe internet uses and complying procedure should have done among the woman.

Conclusion

In science and technology these types of crimes against women are increasing not only in but throughout the world. Since cyber world does not recognize any geographical boundaries, it is really tough job to frame laws to cover each and every aspect. however, it is not possible to eliminate these types of crimes but it is quite possible to check them. In order to prevent these, it is important to make public aware of using the computers and modern technology for betterment of the society. The judiciary should also make the application of laws more stringent to check these types of crimes. No doubt the I.T Act is a welcome step in the cyber world it needs to be suitably modified so as to make it more effective and powerful to combat these types of crimes. If technology is becoming better day by day there is also a need for the protection by changing the existing laws or amending the provisions of the existing Act and the protection is required not only at national level but also international level.

Footnotes:

1 Ms Goswami Garima & Dr. Yazdani Ghulam (2018), Combating Cyber Crimes against Women: Need for Effective Laws. Indian Bar Review Vol. 45(3), New Delhi: Bar Council of India Trust, p. 165

2 Dr. Ahmad Farooq, (2005). Cyber Law in India (p. 339). Delhi: New Era Law Publications

3 Ms Goswami Garima & Dr. Yazdani Ghulam (2018), Combating Cyber Crimes against Women: Need for Effective Laws. Indian Bar Re-

view Vol. 45(3), New Delhi: Bar Council of India Trust, p. 166

4 Ibid, p. 167

5 Sharma Vakul, (2018), Information Technology Law and Practice (pp. 170-171). New Delhi: Universal Law Publishing

6 United Nations General Assembly Resolution A/RES/51/162, adopted on 30th January, 1997, Retrieved March 10, 2021 from http://www.un.org/documents/ga/res/51/ares51-162.htm

7 Sharma Vakul, (2018), Information Technology Law and Practice (p. 113). New Delhi: Universal Law Publishing

❑❑❑

07

COMMERCE MANAGEMENT AND CYBERSECURITY

Dr. Sharad Ranganath Darandale
Associate Professor and Head,
Department of Commerce,
MES's. Arts, Commerce & Science College
Sonai, Tal:- Newasa, Dist:- Ahmednagar

****

ABSTRACT

Cyber security is a big challenge before economic and trade economy. E-Commerce security any nations is a part of the information security from work and is specifically applied to the components that affect e-commerce that includes computer security. Data security and other wider realms of the information security framework,Commerce Management security has its own particular security and is one of the highest visible security components that affect the end through their daily payment interaction with business.

Keywords: -Cyber security, Commerce, Management, E- Commerce,Security threats, Security issues.

Introduction:-

Cyber security is a topic of working inCommercial Management. Apart from this, no country can do secure trade with other countries. The foundation of success in the digital world is having the proper cyber security measures in place to protect consumers, employees and the business itself from constant security threats. Cyber security is woven into the very fabric of business operations and has special impact on the e-commerce sector. Today, privacy and security are a major concern for electronic technologies.

Management commerce shares security

concerns with other technologies in the field. Privacy concerns have been found, revealing a lack of trust is a variety of contexts, including commerce, electronic health records, e-recruitment technology and social networking and this has directly influenced users (Shankar Sen-2003). Web e-commerce applications that handle payments (online banking, using debit cards, credit cards, electronic transaction and others) have more compliance issue,at increased risk from being targeted than other websites and there aregreater consequence if there is data loss or alteration. Privacy has become a major concern for consumers with the rise of identity theft and impersonation and any concern for consumers must be treated as a major concern for e-commerce providers (Carr, I-2003).

Threats of cyber security:-

From identify theft and fraud to corporate hacking attacks;cyber security has never more important for e-commerce sites, large or smaller ones. An attacker over whelms a server with bogus traffic, causing the website or application hosted there to slow down or become unavailable. It is found in recent survey that 60% of respondents saying they are worried about DDoSattacks and 39% admitting it is likely their organization has been targeted.Beware by watching youtube video, anyone can learn to send DDoS attacks (Dr. Subhash Chandra-2001).

E-Commerce;-

E-commerce is the buying and selling of goods and services or the transmitting of funds or data, over an electronic network, primarily the internet. The terms e-commerce and e-business are often used interchangeably.The terms e-tail is also sometimes used in thereference to transactional process for online shopping. Recent years have exponentially witnessed the growth of e-commerce. The growth of e-commerce as a business technology is the result of such internet driven initiative. It has created a universal platform for buying and selling goods services and driving important business process inside the organization (Dr.Farooq Ahmad 1992).

Cyber Attacks and Security for Commerce Management:-

In the world,like the wolf's eyes that always preys on the hen's pen, ahackers eyes always scurries to steal your online stores data. Hackers are ripping off credit card information, personal identity credentials and even sensitive organization data from online databases. The internet is not a safe place to hoardyour data anymore. For e-commerce business, the risk is even grave (C.S.V.Murthy-2002).

The most common cyber security threats include scammers impersonality a business, the sending of fraudulent emails and viruses and malware. Cyber attacks can impact business finances reputation, operations, valuation and staff. As cyber attacks are more likely to occur.It is important to understand the short-term and long-term effect cyber attacks could have on your business (Prasad.R.S-2004).

Importance of cyber security:-

Cyber security is important because it protects all categories of data from theft and damage. This includes sensitive data, personally identifiableinformation (PII), protected health information (PHI),personalinformation, intellectual property data, and governmental and industry information systems. Protect your business against cyber security threats and make the most of online opportunities. No business with an online presence is immune to a cyber-attack, and the financial, physical and legal implications of an attack on any business can be absolutely devastating (Pandoy Ashish -2006).

Data Leak protection:-

It is the most personal threat to cyber security is data leaks, which can be extremely damaging to both an individual business.All business hold a range of data, from customer insight to employee data which often contents sensitive information.Which can easily be put at risk if business does not take a number of steps to protect cyber security management can be described as everything onorganization does to protect its information system and computer networks from cyber attacks, intrusions, malware and various types of data breaches (Nagpal Rohas-2008).

Conclusion:-

Cybercrime has started to create a fear in the minds of many people linked to the network mostly worried to e-commerce technology at its success lies in theinteraction. People inthe commercial sector need to be careful about this, otherwise cybercrime will do a lot of harm in the future.

Reference:-

1. Shankar Sen (2002)Human Right and Law Enforcement. 1st Ed, Concept Publication New Delhi.

2. Carr, I(2003) Anonymity . the Internet and Criminal Law IssuesIn C Nicoll ,J.E.T Prins, J.M.C Asser Press,PP-197-206

3. Dr.Subhash Chandra(2001)Information Technology Act and its Drawbacks, National Conference on Cyber law and Legal Education, December 2001 NALSAR University of Law ,Print House Hyderabad.

4. Dr. Farooq Ahmad (1992) Cyber Law in India (Law on Internet)Poineer Book Delhi.

5. C.S.V.Murthy(2002) E-commerce, Himalaya Publishing House 1st Edition Delhi.

6. Prasad.R.S (2004) Cybercrime and Introduction, 3658 A Nabhi Publication Jaipur .

7. Pandey Ashish (2006) Cyber Criminal detention, and prevention JBAPublisher New Delhi.

8. Nagpal Rohas (2008) Cyber Crime and Corporate Liability CCH India New Delhi.

❑❑❑

08

Humanities and Cyber Security

Prof. Neeta Bokil
Head, Dept. of Political Science,
Haribhai V. Desai College,
Pune,(Maharashtra), India

****

Abstract

Usage of internet has grown to be a everyday ordinary for majority of humans for daily transactions. The wide variety of netcustomers has grown relatively and so does cyber-crimes. Cyber-crime is the crime this is carried outthe use of pc and network. The danger of cyber-crime is an ever gift and growingtruth in each the non-public and expert sectors. With the appearance of net, antique crimes have taken on a brand new appearance. The motive of this studies is to make recognitionconcerning cyber-crimes which might begoing on in today's international and additionally to create recognition of improved cyber safety. This paper triesto investigatethe attention of cyber-crime amongstnetcustomers with special age organizationsand academic qualifications. Linear Regression Model has been implemented for studyingeach the objectives. This paper unearths that there's a dating exists among the age organizationsand academic qualification of the respondents. So, it's far the responsibility of every onenetcustomers to be aware about the cyber-crime and safety and additionallyassist others with the aid of using growing recognition amongst them.

a) Objectives of the study:

1.To examine the education level of the people and the awareness of cyber-crime and security.

2. To examine the effect of Cyber secu-

rity.

3. To find out the internet usage of people.

4. To evaluate the level of awareness on safety while using personal computers and internet among internet users regarding cyber-crimes.

Keywords: Cyber-crime, Cyber criminals, Cyber security, Internet, IT Act, Awareness.

Introduction:

The net in India is developing rapidly. It has given upward push to new possibilities with inside thediscipline of entertainment, business, sports, education, and plenty ofextra. With the arrival and growing use of net, the corporations have crossed the obstacles of neighborhood markets and are achieving out to clientsplaced in eacha part of the world. Computers are broadlyutilized inorganizationsnow no longer best as a device for processing facts, however additionally for gaining strategic and aggressive advantage. Computers may be used each for optimistic and unfavourable reasons. The abuse of net has given start to new age crimes that are addressed with the aid of using the Information Technology Act, 2000.As factsaround the world has come to beextra accessible, it has additionallycome to beextrasusceptible to misuse. India is at the radar of cyber criminals with developing cyber-assaults on Indian establishment. India rank 0.33 as a supply of malicious interestat thenet after US and China, 2d as supply of malicious code and fourth and 8 as supply or foundation for internetassaults and communityassaults. According to the Indian Computer Emergency Response Team (CERT-In), 27,482 instances of cybercrime had beensaid from January to June (2017). These encompass phishing, virus or malicious code, defacements, scanning or probing, web website online intrusions, ransomware and denial-of-provider assaults.The net in India is developing rapidly. It has given upward push to new possibilities withinside the discipline of entertainment, business, sports, education, and plenty ofextra. With the arrival and growing use of net, the corporations have crossed the obstacles of neighborhood markets and are achieving out to clientsplaced in eacha part of the world. Computers are broadlyutilized inorganizationsnow no longerbest as a device for processing facts, however additionally for gaining strategic and aggressive advantage. Computers may be used each for optimistic and unfavourable reasons. The abuse of net has given start to new age crimes that are addressed with the aid of using the Information Technology Act, 2000.As factsaround the world has come to beextra accessible, it has additionallycome to be extrasusceptible to misuse. India is at the radar of cyber criminals with developing cyber-assaults on Indian establishment. India rank 0.33 as a supply of malicious interestat thenet after US and China, 2d as supply of malicious code and fourth and 8 as supply or foundation for internetassaults and communityassaults. According to the Indian Computer Emergency Response Team (CERT-In), 27,482 instances of cybercrime had beensaid from January to June (2017). These encompass phishing, virus or malicious code, defacements, scanning or probing, web website online intrusions, ransomware and denial-of-providerassaults.

Understanding the Cyber Crimes:

Cyber-crime refers to any crime that includes a laptop or a network. It is an illegal act in whichwithinside thelaptop is both a device or a goal or both. It is the crook sports devoted via the usage of digital communications media. It is taking something of the laptop over the internet. The time period Cyber Crime has been described neither in Indian Parliament nor withinside the Information Technology (IT) Act,2000. In India, IT Act, 2000 offers with the offenses associated with cyber-crime. Registration of Cyber Crimes in India takes locationbelow the 3vast heads which might be the IT Act, the Indian Penal Code (IPC) and different State Level

Legislations (SLL). Several Cyber Cells we replaced up to deal withcompletely the instances which might be registered below cyber-crimes in India. It is a quickdevelopinglocation of crime. Cyber criminals are exploiting the Internet to dedicate a variousvariety of crooksports. In the past, cyber-crime becomedevotedin particular with the aid of usingpeople or small businesses however now the cyber criminals constitutes of numerousbusinesses/classwhich includes Professional hackers, prepared hackers, youngsters and teenagersamong the age organization of 6-18 years, scammers, phishers, insiders, malware authors, spammers, etc.

Categories of Cyber Crimes: The important classes of cyber-crimes may bewidely categorized beneath the subsequent 4 companies on the premisein their goal and impacts:

1. Crimes towards Individuals: These sort of crime are accomplished to damage unique individuals. These consists of hacking, cracking, harassment through emails, cyber-stalking, cyber bullying, defamation, dissemination of obscene material, electronic mail spoofing, SMS spoofing, carding, dishonest and fraud, toddler pornography, attackthrough threat, denial of provider attack, forgery, and phishing.

2. Crimes towards Property: There are cybercrimes accomplished to damage the assets of an Individual. They may be categorized as – Intellectual assets crimes, cyber-squatting, cyber vandalism, hacking pc system, pc vandalism, pc forgery, transmitting viruses and malicious software program to harm information, Trojan horses, cyber trespass, Internet time thefts, theft or stealing cashwhilstcash transfers ,etc.

3. Crimes towards Government /Firm /Company /Group of individuals: These styles of crimes encompass cyber terrorism, ownership of unauthorized information, distribution of pirated software program, internet jacking, salami attacks, good judgment bombs, etc. The criminals in thosedesires to terrorize the residents of the country.

4. Crimes towards Society: All the above noted crimes have their direct or obliqueaffectat the society at large. Therefore, all such crimes are protectedon thiswhich includes pornography, online gambling, forgery, sale of unlawful articles, phishing, cyber terrorism, etc.

The everyday end users of Internet-enabled devices and services, who vastly outnumber security experts and researchers, are most closely engaged with cybersecurity. Their voices can be drowned out in the general clamour of voices speaking about cybersecurity. When the end users' voices are heard, their responses are usually constrained by specific questions that are formulated by the major stakeholders in the field. Yet, it is important to consider the end users' unprompted perspectives, opinions, and perceptions of cybersecurity, so that the social desirability bias does not influence their responses.Human-centred security researchers study and improve the interface where humans and security-related technologies meet. Their usual research philosophy is positivist, i.e. revealing general laws of behaviours and highlighting causal relationships within the research space. As such, the researchers and experts choose the research topics, formulate the research questions, develop studies and design experiments. These researchers are investigating important and crucial aspects of human-centred security, and their solutions make a huge difference to the field as a whole.

Social cybersecurity is both a new scientific and a new engineering field. It is a computational social science with a large foot in the area of applied research. Drawing on a huge range of disciplines the new technologies and findings in social cybersecurity have near immediate application on the internet. The findings and methods are relevant to policy makers, scholars, and corporations. Social cybersecurity uses computational social science techniques to identify, counter, and measure (or assess) the impact of communication objectives. The methods and findings in this area are critical, and advance industry-accepted practices for communication, journalism and marketing research. The field itself has a theory, application, and policy component. The methods build on work in high dimensional network analysis, data science, machine learning, natural language processing and agent-based simulation. These methods are used to provide evidence about who is manipulating social media and the internet for/against you or your organization, what methods are being used, and how these social manipulation methods can be countered. They also support cyber diplomacy. Social cybersecurity uses computational social science techniques to identify, counter, and measure (or assess), the impact of influence campaigns, and to identify and inoculate those at risk against such campaigns. The methods and findings in this area are critical, and advance practices for intelligence and forensics research. These methods also provide scalable techniques for assessing and predicting the impact of influence operations carried out through social media, and for securing social activity on the internet and mitigating the effects of malicious and undue influence. As such they are critical for creating a more secure and resilient society.Influence campaigns vary widely, and who is at risk in part depends on those conducting the influence campaign and in part on the context. For example, in our research we found that influence campaigns appearing to come from state-level actors during the elections in Western Europe and the US from 2016 to 2020 were often aimed at minorities. For example, they targeted women, ethnic minorities, and the LGBQT community. In contrast, in India as COVID-19 ramped up internal non-state groups launched anti-Muslim campaigns. As movies like the Black Panther and Captain Marvel were released individual's launched campaigns against the movies. In the elections in the Asia Pacific region influence campaigns often take the form of promoting pro-China candidates. Many influence campaigns are aimed at specific individuals trying to recruit them to a new cause, or engage them in insider threat activity.

Conclusion and Suggestions:

With the boomwithinside thecustomers of net, the boom in cyber-crimes also can be seen. There are diversesorts of cyber-crimes which might begoing on in daily life. But the human beingsaren'taware about all such types. Majority of the human beings recognise handiestapproximately hacking and virus/ worms. They aren'taware about phishing, defamation, identification theft, cyber stalking etc. It is the want of today's global to have expertise approximatelythose crimes which might berelated to the net. The take a look atsuggests that 48% of the respondents percentage their non-publicinformation with differentindividuals even they don't recognise them closely.55% of respondents have agreed that their PCs are frequentlybrokenvia way of means of viruses. The netcustomers struggled with junk mail emails, phishing calls and emails requesting their touchystatistics like cell no., financial institution account, address, etc. It is the obligationof every one folks to be aware about the simple cyber safety. Cyber safetyrefers back to thetechnology and strategieswhich might bedesigned to guard computers, networks and facts from unauthorized get admission to and assaultsbroughtthrough the netvia way of means of cyber criminals. The human being shave to be aware about the simple cyber securities which include they have to:

a) Install a security suites such as Avast Internet Security, Kaspersky antivirus, McAfee antivirus, Norton Antivirus, etc. to protect the computer against threats such as viruses and worms.

b) Activate Network Threat Protection, Firewall, and Antivirus.

c) Always use strong passwords preferably alphanumeric.

d) Communicate personal information only via phone or secure web sites.

e) Do not click on links, download files or open attachments in emails from unknown senders.

f) Beware of links in emails that ask for personal information or popups.

g) Check that all antivirus software and computer operating system are up-to-date.

h) Double check the spelling of a website, URL, HTTP addresses etc.

Government is likewise making efforts to have a manipulate on cyber-crimes. It has made cyber legal guidelines to assisthumans studydiverse cyber-crimes and cyber safety. Information Technology(IT) Act 2000 offers with cyber associated crimes. Not handiest the authoritieshoweverhumanshave to additionally paintings hand in hand to trap the criminals. People who've been a sufferer of any of those cyber-crimes have to come ahead and record a criticismin opposition to them in unique cybercrime cells. This will trulyassist to address the cyber-crimes. Thus, cognizance of cyber-crimes and safety is a want of an hour.

References:

1. Aggarwal, Gifty (2015), General Awareness on Cyber Crime. International Journal of Advanced Research in Computer Science and Software Engineering.Vol 5, Issue 8.

2. Aparna and Chauhan, Meenal (2012), Preventing Cyber Crime: A Study Regarding Awareness of Cyber Crime in Tricity. International Journal of Enterprise Computing and Business Systems, January, Vol 2, Issue 1.

3. Archana Chanuvai Narahari and Vrajesh Shah (2016).Cyber Crime and Security – A Study on Awareness among Young Netizens of Anand.International Journal of Advance Research and Innovative Ideas in Education.Vol-2 Issue-6.

4. Avais, M. Abdullah et.al. (2014), Awareness regarding cyber victimization among students of University of Sindh, Jamsharo. International Journal of Asian Social Science, Vol. 4(5): 632-641

5.Hasan et al., (2015), Perception and Awareness of Young Internet Users towards Cybercrime: Evidence from Malaysia. Journal of Social Sciences, Vol. 11 (4): 395.404

6. Jamil D. and Khan M.N.A. (2011), Data Protection Act in India with Compared To the European Union Countries. International Journal of Electrical and Computer Sciences, Vol: 11 No: 06.

7. Mehta, Saroj and Singh, Vikram (2013), A Study of Awareness aboutCyber laws in the Indian Society. International Journal of Computing and Business Research, January, Vol.4, Issue. 1.

8. Parmar, Aniruddhsinh and Patel Kuntal (2016), Critical Study and Analysis of Cyber Law Awareness among Netizens. Conference: International Conference on ICT for Sustainable Development, At http://link.springer.com/chapter/10.1007%2F978-981-10-0135-2_32, Volume: 409

9. Singaravelu, S and Pillai, K. Perumal (2014), B.Ed. Students Awareness on Cybercrime in Perambalur District. International Journal of Teacher Educational Research (IJTER) Vol.3 No.3 March.

10. The Times of India(July 22, 2017), http://timesofindia.indiatimes.com/india/one-cybercrime-in-india-every-10-minutes/article show/59707605.cms

❑❑❑

09

A STUDY OF CHALLENGES OF CYBER SECURITY AND ITS EMERGNING TRENDS ON MODERN TECHNOLOGIES

DR.RUPESH DHUMAJI BANSODE
MODERN COLLEGE PUNE

****

Cyber Security plays an important role in the field of information technology.Securing the information have become one of the biggest challenges in the present day. Whenever we think about the cyber security the first thing that comes to our mind is ‘cybercrimes’ which are increasing immensely day by day. Various Governments and companies are taking many measures in order to prevent these cybercrimes. Besides various measures cyber security is still a very big concern to many. This paper mainly focuses on challenges faced by cyber security on the latest technologies .It also focuses on latest about the cyber security techniques, ethics and the trends changing the face of cyber security.

Keywords: cyber security, cybercrime, cyber ethics, social media, cloud computing, android apps.

INTRODUCTION:

Today man is able to send and receive any form of data may be an e-mail or an audio or video just by the click of a button but did he ever think how securely his data id being transmitted or sent to the other person safely without any leakage of information?? The answer lies in cyber security. Today Internet is the fastest growing infrastructure in everyday life. In today’s technical environment many latest technologies are changing the face of the mankind. But due to these emerging technologies we are unable to safeguard our private information in a very effective way and hence these days cybercrimes are increasing day by day. Today more than 60 percent of total commercial transactions are done online, so this field required a high quality of security for transparent and best transactions. Hence cyber security has become a latest issue. The scope of cyber security is not just limited to securing the information in IT industry but also to various other fields like cyber space etc.

Even the latest technologies like cloud computing, mobile computing, E-commerce, net banking etc also needs high level of security. Since these technologies hold some important information regarding a person their security has become a must thing. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic wellbeing. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as governmental policy. The fight against cybercrime needs a comprehensive and a safer approach. Given that technical measures alone cannot prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cybercrime effectively. Today many nations and governments are imposing strict laws on cyber securities in order to prevent the loss of some important information. Every individual must also be trained on this cyber security and save themselves from these increasing cybercrimes

2. CYBER CRIME Cybercrime is a term for any illegal activity that uses a computer as its primary means of commission and theft. The U.S. Department of Justice expands the definition of cybercrime to include any illegal activity that uses a computer for the storage of evidence. The growing list of cybercrimes includes crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying and terrorism which have become as major problem to people and nations. Usually in common man's language cybercrime may be defined as crime committed using a computer and the internet to steel a person's identity or sell contraband or stalk victims or disrupt operations with malevolent programs. As day by day technology is playing in major role in a person's life the cybercrimes also will increase along with the technological advances.

1 CYBER SECURITY

Privacy and security of the data will always be top security measures that any organization takes care. We are presently living in a world where all the information is maintained in a digital or a cyber-form. Social networking sites provide a space where users feel safe as they interact with friends and family. In the case of home users, cyber-criminals would continue to target social media sites to steal personal data. Not only social networking but also during bank transactions a person must take all the required security measures.

Incidents	Jan-June2012	Jan-June2013	% Increase/(decrease)
Fraud	2439	2490	2
Intrusion	2203	1726	(22)
Spam	291	614	111
Maliciouscode	353	442	25
Cyber Harassment	173	233	35
Content related	10	42	320
Intrusion Attempts	55	24	(56)
Denial of services	12	10	(17)
Vulnerability reports	45	11	(76)
Total	5581	5592	

The above Comparison of Cyber Security Incidents reported to Cyber999 in Malaysia from January–June 2012 and 2013 clearly exhibits the cyber security threats. As crime is increasing even the security measures are also increasing. According to the survey of U.S. technology and healthcare executives nationwide, Silicon Valley Bank found that companies believe cyber attacks are a serious threat to both their data and their business continuity.

98% of companies are maintaining or increasing their cyber security resources and of those, half are increasing resources devoted to online attacks this year

The majority of companies are preparing for when, not if, cyberattacks occur

Only one-third are completely confident in the security of their information and even less confident about the security measures of their business partners.

There will be new attacks on Android operating system based devices, but it will not be on massive scale. The fact tablets share the same operating system as smart phones means they will be soon targeted by the same malware as those platforms. The number of malware specimens for Macs would continue to grow, though much less than in the case of PCs. Windows 8 will allow users to develop applications for virtually any device (PCs, tablets and smart phones) running Windows 8, so it will be possible to develop malicious applications like those for Android, hence these are some of the predicted trends in cyber security.

4. TRENDS CHANGING CYBER SECURITY Here mentioned below are some of the trends that are having a huge impact on cyber security.

4.1 Web servers:

The threat of attacks on web applications to extract data or to distribute malicious code persists. Cyber criminals distribute their malicious code via legitimate web servers they've compromised. But data-stealing attacks, many of which get the attention of media, are also a big threat. Now, we need a greater emphasis on protecting web servers and web applications. Web servers are especially the best platform for these cyber criminals to steal the data. Hence one must always use a safer browser especially during important transactions in order not to fall as a prey for these crimes.

4.2 Cloud computing and its services

These days all small, medium and large companies are slowly adopting cloud services.

In other words the world is slowly moving towards the clouds. This latest trend presents a big challenge for cyber security, as traffic can go around traditional points of inspection. Additionally, as the number of applications available in the cloud grows, policy controls for web applications and cloud services will also need to evolve in order to prevent the loss of valuable information. Though cloud services are developing their own models still a lot of issues are being brought up about their security. Cloud may provide immense opportunities but it should always be noted that as the cloud evolves so as its security concerns increase.

4.3 APT's and targeted attacks

APT (Advanced Persistent Threat) is a whole new level of cyber crime ware. For years network security capabilities such as web filtering or IPS have played a key part in identifying such targeted attacks (mostly after the initial compromise). As attackers grow bolder and employ more vague techniques, network security must integrate with other security services in order to detect attacks. Hence one must improve our security techniques in order to prevent more threats coming in the future.

4.4 Mobile Networks

Today we are able to connect to anyone in any part of the world. But for these mobile networks security is a very big concern. These days firewalls and other security measures are becoming porous as people are using devices such as tablets, phones, PC's etc all of which again require extra securities apart from those present in the applications used. We must always think about the security issues of these mobile networks. Further mobile networks are highly prone to these cybercrimes a lot of care must be taken in case of their security issues.

4.1 IPv6: New internet protocol

IPv6 is the new Internet protocol which is replacing IPv4 (the older version), which has been a backbone of our networks in general and the Internet at large. Protecting IPv6 is not just a question of porting IPv4 capabilities. While IPv6 is a wholesale replacement in making more IP addresses available, there are some very fundamental changes to the protocol which need to be considered in security policy. Hence it is always better to switch to IPv6 as soon as possible in order to reduce the risks regarding cybercrime.

4.5 Cloud computing and its services

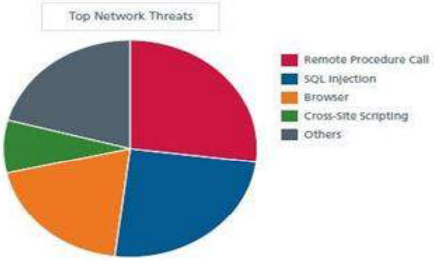
These days all small, medium and large companies are slowly adopting cloud services. In other words the world is slowly moving towards the clouds. This latest trend presents a big challenge for cyber security, as traffic can go around traditional points of inspection. Additionally, as the number of applications available in the cloud grows, policy controls for web applications and cloud services will also need to evolve in order to prevent the loss of valuable information. Though cloud services are developing their own models still a lot of issues are being brought up about their security. Cloud may provide immense opportunities but it should always be noted that as the cloud evolves so as its security concerns increase.

4.6 APT's and targeted attacks

APT (Advanced Persistent Threat) is a whole new level of cyber crime ware. For years network security capabilities such as web filtering or IPS have played a key part in identifying such targeted attacks (mostly after the initial compromise). As attackers grow bolder and employ more vague techniques, network security must integrate with other security services in order to detect attacks. Hence one must improve our security techniques in order to prevent more threats coming in the future.

4.7 Mobile Networks

Today we are able to connect to anyone in any part of the world. But for these mobile networks security is a very big concern. These days firewalls and other security measures are becoming porous as people are using devices such as tablets, phones, PC's etc all of which again require extra securities apart from those present in the applications used. We must always think about the security issues of these mobile networks. Further mobile networks are highly prone to these cybercrimes a lot of care must be taken in case of their security issues.



The above pie chart shows about the major threats for networks and cyber security.

ROLE OF SOCIAL MEDIA IN CYBER SECURITY

As we become more social in an increasingly connected world, companies must find new ways to protect personal information. Social media plays a huge role in cyber security and will contribute a lot to personal cyber threats. Social media adoption among personnel is skyrocketing and so is the threat of attack. Since social media or social networking sites are almost used by most of them every day it has become a huge platform for the cyber criminals for hacking private information and stealing valuable data.

In a world where we're quick to give up our personal information, companies have to ensure they're just as quick in identifying threats, responding in real time, and avoiding a breach of any kind. Since people are easily attracted by these social media the hackers use them as a bait to get the information and the data they require. Hence people must take appropriate measures especially in dealing with social media in order to prevent the loss of their information.

The ability of individuals to share information with an audience of millions is at the heart of the particular challenge that social media presents to businesses. In addition to giving anyone the power to disseminate commercially sensitive information, social media also gives the same power to spread false information, which can be just being as damaging. The rapid spread of false information through social media is among the emerging risks identified in Global Risks 2013 report.

Though social media can be used for cybercrimes these companies cannot afford to stop using social media as it plays an important role in publicity of a company. Instead, they must have solutions that will notify them of the threat in order to fix it before any real damage is done. However companies should understand this and recognise the importance of analysing the information especially in social conversations and provide appropriate security solutions in order to stay away from risks. One must handle social media by using certain policies and right technologies.

2 CYBER SECURITY TECHNIQUES

6.1 Access control and password security

The concept of user name and password has been fundamental way of protecting our information. This may be one of the first measures regarding cyber security.

6.2 Authentication of data

The documents that we receive must always be authenticated be before downloading that is it should be checked if it has originated from a trusted and a reliable source and that they are not altered. Authenticating of these documents is usually done by the antivirus software present in the devices. Thus a good anti virus software is also essential to protect the devices from viruses.

6.3 Malware scanners

This is software that usually scans all the files and documents present in the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware.

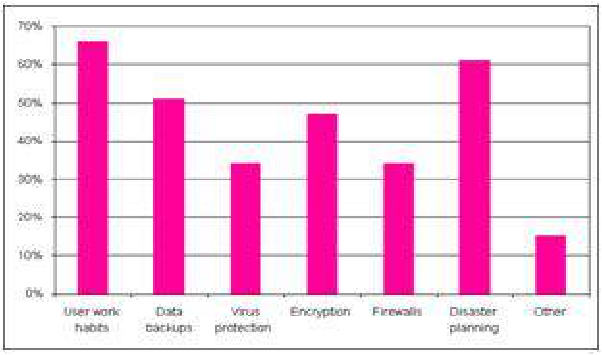
6.4 Firewalls

A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. All messages entering or leaving the internet pass through the firewall present, which examines each message and blocks those that do not meet the specified security criteria. Hence firewalls play an important role in detecting the malware.

6.5 Anti-virus software

Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered. An anti virus software is a must and basic necessity for every system.

Table II: Techniques on cyber security



7. CYBER ETHICS Cyber ethics are nothing but the code of the internet. When we practice these cyber ethics there are good chances of us using the internet in a proper and safer way. The below are a few of them:

DO use the Internet to communicate and interact with other people. Email and instant

Messaging make it easy to stay in touch with friends and family members, communicate with work colleagues, and share ideas and information with people across town or halfway around the world

Don't be a bully on the Internet. Do not call people names, lie about them, send embarrassing pictures of them, or do anything else to try to hurt them.

Internet is considered as world's largest library with information on any topic in any subject area, so using this information in a correct and legal way is always essential.

Do not operate others accounts using their passwords.

Never try to send any kind of malware to other's systems and make them corrupt.

Never share your personal information to anyone as there is a good chance of others misusing it and finally you would end up in a trouble.

When you're online never pretend to the other person, and never try to create fake accounts on someone else as it would land you as well as the other person into trouble.

Always adhere to copyrighted information and download games or videos only if they are permissible. The above are a few cyber ethics one must follow while using the internet. We are always thought proper rules from out very early stages the same here we apply in cyber space.

8. CONCLUSION

Computer security is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. Cyber crime continues to diverge down different paths with each New Year that passes and so does the security of the information. The latest and disruptive technologies, along with the new cyber tools and threats that come to light each day, are challenging organizations with not only how they secure their infrastructure, but how they require new platforms and intelligence to do so. There is no perfect solution for cyberc rimes but we should try our level best to minimize them in order to have a safe and secure future in cyber space.

REFERENCES

1 A Sophos Article 04.12v1.dNA, eight trends changing network security by James Lyne.

2 Cyber Security: Understanding Cybercrimes- Sunit Belapure Nina Godbole

3 Computer Security Practices in Non Profit Organisations – A NetAction Report by Audrie Krause.

4 A Look back on Cyber Security 2012 by Luis corrons – Panda Labs.

5 International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 Page nos.68 – 71 ISSN 2229-5518, "Study of Cloud Computing in HealthCare Industry " by G.Nikhita Reddy, G.J.Ugander Reddy

6 IEEE Security and Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2013.

7 CIO Asia, September 3rd, H1 2013: Cyber security in malasia by Avanthi Kumar.

8. Paper on cyber security challenges reddy

❑❑❑

10

Cyber Threat's in the Era of Digital Banking

Mr. Vaibhav Vijay Kadam
M.A.-II, Economics,
Sir Parshurambhau College, Pune

****

Introduction:

The integral activity of our early twenty-first century was revolutionized in the era of globalization by Internet banking or online banking. India has third largest internet population in the world after China and United Stated. More than half of the population is connected to web these days and every individual has easy access of internet for their daily routine purposes like banking, entertainment, education etc. The availability and use of smart phones have really added weightage to the remarkable growth in the internet.The banking sector is one of the major beneficiaries of the Internet revolution and the growth ofbanking technology products have been remarkably increasing.The prevalent gain of Internet banking is that people can pay out the services sitting at home, without visiting the branch. This helps customers to complete their transactions in the fraction of time, thus saving both time and effort. Internet banking system proves to be very versatile in completing transactions like balanceinquiry, withdrawal, deposits, viewing the bank statement, and record of recent transaction.

The development of computers has made a great impact in the banking sector however along with it grew the different ways people would fall prey to different attacks. With the expansion of internet technologies, cyber-crimes have evolved worldwide and its nature and pattern have become more complex. The demand of online services has made a challenge for providing security to the customers, mainly due to increase in cybercrimes, which is serious threat to the financial institutions and banks. Cybercrimes can take many forms like E-laundry, ATM fraud, credit card fraud, etc.The spectaculargrowth in cybercrimes is the main problem for financial institutions in the 21st century.

Research Methodology:

The research study will be carried out with the help ofsecondary data. Besides, the knowledgeable persons ofthe study area and concerned officers will also consulted and information supplemented to our secondary data.Information presented in current research project are collected from various reports prepared by national and international agencies on banking and finance.This Information is collected from various authentic websites and also some journals and e-contents relating to impact of cyber security on Indian Banking System are also referred.

Review of Literature:

'Cyber Attacks in the Banking Industry' by Adharsh Manivannan DhatchinaMoorthy Faculty of Science and TechnologyBournemouth, United KingdomThe studyconcludes that there is a need to raiseconsciousness among consumers about the presence of cybercrime in the handling of online banking and confidential financial data and how to defend themselves against these external challenges.

'An Evaluative Study on Internet Banking Security amongSelected Indian Bank Customers' by V. Vimala, Avinashi lingam University, Coimbatore. This present study is carried out with the help of a suitable research instrument. 50 customers were selected and with the help of their responses, analysis is made few suggestions.

Objectives of the Study:

1. To Study the Recent Trend in Indian Banking Industry.

2. To Study the Role ofInformation Technology in Indian Banking System.

3. To Highlight the Cyber Threat in Indian Banking System.

4. To Highlight Various Challenges Faced by Banks in the Cyber SecurityScenario.

5. To Discuss the Methods to Protect from Cyber Attacks

What is Cyber Security?

Cyber Security in banks involves measures to protect the computer assets, information and networks from unauthorised users and preparedness to business continuity and Disaster Recovery.In today's connected world, everyone benefits from advanced cyberdefence programs. It encompasses Information Security, Application Security and Network Security and Disaster Recovery.At an individual level, a cybersecurity attack can result in everything from identity theft, to extortion attempts, to the loss of important data like photos, documents etc. Everyone relies on critical infrastructure like power plants, hospitals, and financial service companies. Securing these and other organizations is essential to keeping our society functioning.

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacksfor over many years, information security has held confidentiality, integrity and availability (known as the CIA triad) to be the core principles.These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. However, other principles such as authenticity, non-repudiation and accountability are also now becoming key considerations.Some of the common threats faced by the Banks are Malware, Ransomware, Phishing, Spear Phishing/Whaling, SQL injection Attack, Cross site Scripting,Denial of Service (DoS), Social Engineering, Website Defacement etc. Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

Technology in Banking:

Information Technology has made a revolution in each and every sphere of human life.Banks have been the earliest in India to adopt technology by automating systems and streamlining their processes.Banks play a vital role in nation-building, especially in a growing economy like India.It is like a central nerve to a nation's economy as it caters to the financial needs of credit in all the domains of the society.Globalization, liberalization and privatization have brought remarkable changes in the banking service sector in India. Ever since the days of globalization and privatisation in early 1990's, computerisation, and technology in general, has come to stay in banks in India. Banking in India is now re-defined with technology. Today's banking is associated more with these electronic delivery channels like ATMs, Mobile, PoS Terminals and Online modes than with any physical human being.Indian Banking System has reached every nook and corner of the country.Indian Banking System is no longer kept to just the metropolitans, yet has come to try and to the remote corners of the nation.The growth and advancements in technology has led to a paradigm shift in the entire banking operations and systems. Further the development of e-banking created a massive change in terms of fulfilling customers' divergent needs.

The current technological environment facilitated in providing multiple and innovative contemporary services to the customers. Computer, telecommunications and internet have revolutionized banking service by offering alternate services by shifting towards internet banking. This enabled customers to access banking services in different ways on their smart phones and computers. The traditional over-the-counter banking is slowly losing its prominence due to self-service techniques and competitive pressures by banks. Expectations of the customers have increased due to the impact of technology, increase in modern technology and increase in global literacy levels. Digital banking is the future of Indian banking system.

Cyber Threat'sin Indian Banking System:

Cybercrime is a major problem in this world and mostly all banking organizations rely on the internet.Banks are susceptible to many types of online frauds and cybercrimes. Cybercriminals are targeting banks because their data is more valuable, normally cybercriminals obtain their customer data from social networks like Facebook.Cyber-attacks have become an easy option forcybercriminals to access other confidential data through the internet, normally hackers are targeting customer's data and funds, as well as the bank's core systems. These cyber-attacks are commonly done by malware and phishing.Skimming, malware attacks, compromise of credentials by insiders etc has also become very common. Mobile banking and various applications provided by banks are also utilized by criminals and software vulnerabilities in banks apps and Aadhar based account frauds by some business correspondents are also surfaced.The main aim of these attacks is to take over the user's bank accounts and funds in such a way the attacker occupies the funds without proper knowledge of the user. In some situations, to enter banks and steal a large amount of money, cybercriminals use banking passwords such as PIN, password, certificates, etc. while in other circumstances, they may try to steal all the money and transfer the funds into mule accounts. Cyber attackers often aim to damage the bank's reputation and then block bank servers so that consumers are unable to access their accounts.Nowadays, mobile banking has become a tool for pilfering confidential credentials and their user has become prey to phishing attacks. There are often reports in the Press, about cases of banks becoming targets of attacks like hacking taking advantages of existing vulnerabilities in the system. The recent attack called "WannaCry" is neither the beginning, certainly nor the end in this game. Such attacks will only increase day by day and banks' spending on Information Security should be much higher and not just higher but should also be transparent and conspicuous to drive the criminals away deterring them from embarking on any such misadventure of attacking the bank data

According to Symantec Report; Cyber criminals caused unprecedented levels of disruption of IT services with relatively simple IT tools and cloud services. Governments are targeted for cyberattacks and the focus is shifting from economic espionage to politically motivated sabotage and subversion. The cloud has become a dangerous place and vulnerabilities in cloud infrastructure provide the next frontier for cybercrime. Hence, for security purposes, banks have now strengthened their perimeter infrastructure by managing their security operation Centres and through following tools:

· Vulnerability Management.

· NBAD (Network Behaviour Anomaly Detection).

· Anti-APT (Anti Advanced Persistent Threat).

· DDOS (Distributed Denial of Service).

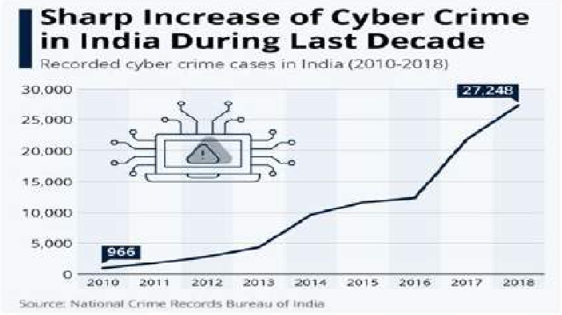
· Anti-Phishing, Malware Monitoring.

· PIM (Privilege Identity Management).

· FIM (File Integrity Management).

· WAF (Web Application Filtering

Cybersecurity has extended beyond Data Centre perimeter, to end points, the cloud and using analytics, IP profiling to outwit the cyber adversaries. The attackers take advantage of endpoint vulnerabilities and poor security controls and have been changing the pattern of attacks to escapedetection.



Above graph is showing sharp increase of cybercrimes in India during last decade (All Sectors). We can clearly see the boost in cybercrimes after 2016. From this we can infer it may have affected the banking sector as well. Bank's need to understand that Cyber Security is an ongoing battle. Adding new IT infra structure like new digital assets, new applications, networks mechanisms for accessing them needs utmost care and should be integrated with the cyber security plans. Focus on evolvingcyber trends, threat vectors and new vulnerabilities, new exploits will help the banks to build and refresh resilient cyber security strategies.

Types of Cyber Attacks:

Denial-of-service (DoS): This attack is performed over the network user's computer to make it inaccessible to the user by flooding them with messages to trigger the crash.

Phishing: Phishing is the process of acquiring the username and password of the user without his knowledge. These user login details can be anything like a bank account or social media login credentials

Malware: Malware is a type of software that spreads viruses through devices to other computers to crash the system. This can also crash remotely connected network computers.

Spam emails: Spam emails are emails that are pushed inside the user's mail account without prior permission. It can be junk advertisement postings or anything inappropriate to the user.

Spamming: Spamming is a method of messaging system to send a spam message to many recipients for advertising.

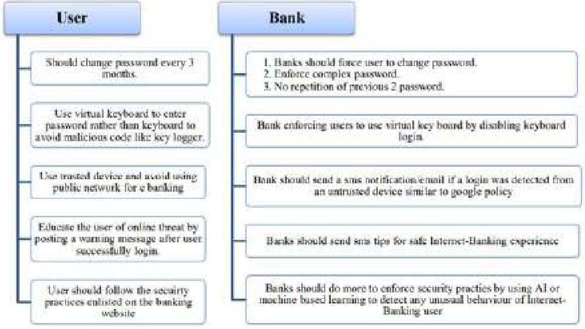
Spyware: It is malicious software installed in a user's computer without their knowledge hacker can access all the files and their stored file in the system.

Challenges of Cyber Security:

Cybercrimes are more prevalent in those organizations who have not implemented baseline cyber security defence. Many cyber criminals are exploiting the known network vulnerabilities of organisations who have not even implemented baseline cyber security defence. The cyber adversaries keep scanning all the connected systems/devices in the cyber space for easy targets who are laggards in cyber security implementation. Identity is a response to a need, and unless that need is clearly understood, and actually expressed as something that the business wants to address the banks will be at great loss.While assessing cyber risk of an organisation the critical phase is identifying critical assets, valuable information, threats and risks associated with that information, and outlining the risk of breach of such information.

In banks, there can be leakage of personal data, stolen card data and unauthorized data sharing due to customer privacy violation. With the growth of the technology, cyber-attacks also took new shapes in the form of next-generation ransomware, web attacks etc.Cyber-attacks in banks, generally, take in form of extortion of funds from individuals to organizations. The confidential credential is being stolen by phishing mails and syphoning of funds through whaling.It is a challenge for banks and financial institutions, to manage threats from multiple cyber-attacks, as consumers want the assurance from bank for protection of data. The major challenge is the lack of awareness of cyber threats and their serious implications by bank's staff and customers. It is also difficult for banks to manage and adhere to the regulatory compliance in India, as the volume of regulations has increased over the past few years.

User and Bank Awareness:



User

Should change password every 3 months.

Use virtual keyboard to enter password rather than keyboard to avoid malicious code like key logger.

Use trusted device and avoid using public network for e banking

Educate the user of online threat by posting a warning message after user successfully login.

User should follow the security practices enlisted on the banking website

Bank

1. Banks should force user to change password.
2. Enforce complex password.
3. No repetition of previous 2 password.

Bank enforcing users to use virtual key board by disabling keyboard login

Bank should send a sms notification/email if a login was detected from an untrusted device similar to google policy

Banks should send sms tips for safe Internet-Banking experience

Banks should do more to enforce security practies by using AI or machine based learning to detect any unusall behaviour of Internet-Banking user

Technology to Improve Banking System:

Technologies used to maintain a security system in the banking sector

Firewall for Banking application:

A firewall is a barrier between the internet and your computer or network. Using a firewall, you can secure your system from a hacker. Some of the viruses are spread through the internet that can block by a firewall. There are two types of firewall

• Personal firewall • Hardware firewall

The disadvantage of firewall in bank Banks use the same firewall used in companies firewall do not do much. last seven years no one adds any updates to the firewall.

Two-factor authentication:

Banks have introduced a multilayer approach to online banking login under a new method of strong customer authentication (SCA). Weak login details can be stolen easily from social media like name, address, phone number, etc and if the hacker penetrated the first layer of defence, they would have to access the sensitive data of customer like payment history or banking card number and many banks are using a method of sending password via message.

Findings of the Study:

Digital banking is the future of Indian Banking System.

Cybercriminals are targeting banks because their data is more valuable, normally cybercriminals obtain their customer data from social networks.

In last decade number of cybercrimes cases is increased very rapidly.

We can clearly see the boost in cybercrimes cases after 2016.

Need to enhance efficiency of technologies used to in security system in the banking sector

Conclusion:

The outcome of the research work on the Internet banking helped to identify the precautionary checklist open to for a number of issues in the internet banking era.Now days, traditional way of banking transactions have been switched by E-banking. It has also been observed that financial institutions have overlooked some essential aspects relating to technology, which demands huge attention. The lack of awareness and inadequate knowledge to customers and banking officials has also simplified the work for cyber criminals.Threat intelligence technology is also essential which will reduce the cyber threat vulnerabilities.A critical infrastructure is also required to be built to avoid cybercrimes in financial institutions and banks. The cooperation of Indian Government and industrial groups is also required to strengthen the legal framework for cyber security.But in the end, people must be aware of their credentials and ensure that it is not misused, special efforts must be made by banks to spread awareness and ensure that the customers do not fall prey to the scams. These measures can increase cybersecurity in the banking sector.

References:

https://dbie.rbi.org.in/

https://cybervolunteer.mha.gov.in/

https://cybercrime.gov.in/

https://www.mha.gov.in/division_of_mha/cyber-and-information-security-cis-division

https://securityboulevard.com/2021/01/the-rising-online-banking-frauds-in-india/

https://www.statista.com/

https://cyber.gc.ca/en/guidance/how-use-online-banking-securely-itsap00080

❑❑❑

11

THE NEED OF CYBER SECURITY IN COLLEGE LIBRARIES

Manasi M. Rasal
Librarian,
Karmaveer Bhaurao Patil College,
Vashi, Navi Mumbai

****

Abstract:

In the age of information technology, the use of internet has become mandatory in every field. Everyone can easily do their work at home with the help of their desktop, laptop, tablet or Android phone. The internet covers most areas of life, no matter how hard a person tries to stay away from the internet, he cannot stay away from it. From daily grocery shopping, to paying various bills, exchanging money, completing school and college admissions, you have to use the internet in one or more places. While internet saves a lot of time and money, it is just as important to consider the other side of the coin as it is to take care of the pros and cons of the internet.To take advantage of any online service, you first need to connect your device to the internet and enter your basic but confidential information before your online process.

Where there is a wealth, there is a greater chance of theft. In the same way, stealing online in a place where you have confidential and important information is a cybercrime. Cyber criminals use a variety of methods to steal information from your device or that you fill out online.For this, fraudsters resort to e-mails and virus attacks. Misuse of this confidential information can result in the loss of valuable data on your device as well as financial difficulties. Cyber security is important to keep the confidential information of the Internet user safe.

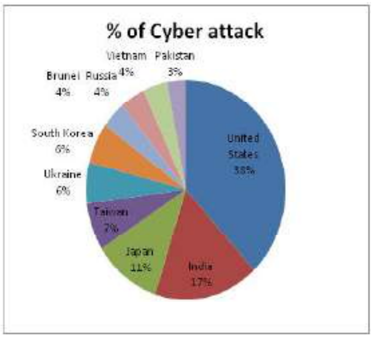
Cyber Security plays an important role in protecting the information provided by the user during the internet usage, the information on the device through which the internet is connected.

Criminals are always searching the different ways to steal information, so you have to be equally careful so that cyber security doesn't come in handy every time.

Keywords : Cyber Crime, Data Security, Cyber Crime Variants, Cyber Safety.

Introduction:

As the impact of revolution of Information Technology, it has become mandatory for all sectors to use internet. The higher the use of information technology, the greater the risk of cyber attacks.



According to the Cyber Security Statistics 2021 report, the United States (38%) ranks first among the top ten countries in terms of cyber attacks in the world, followed by India (17%). College libraries have also computerized using this technology.It is now important to protect computerized data responsibly as much as it is appreciated that libraries are 100% computerized.Internet-based computer systems are used to make library services easy and accessible at any time. Connecting to an Internet computer increases the risk of computer information being stolen. Such information is important for the relevant library.When cyber criminals steal or destroy such information using misconduct, the loss is irreparable from the point of view of the library. Cyber security is a must, not just in libraries, but in all places where computers or any of your other devices are connected to the Internet.According to The Hindu newspaper, when mobile phones worth an average of 120 million are lost or stolen every year, the chances of data theft are high. In just 18 months, 3.17 lakh cyber crime cases have been registered in India. They also says "As per the data maintained, since its inception 3,17,439 cybercrime incidents and 5,771 FIR's have been registered up to February 28, 2021 in the country which includes, 21,562 cybercrime incidents and 87 FIRs in Karnataka and 50,806 cybercrime incidents and 534 FIRs in Maharashtra."

Given the rising tide of cybercrime, the need for cyber security is growing exponentially.

The need of Cyber Security:

With the advent of the Internet, many of the tasks at home have become much easier. In order to complete e-commerce, e-shopping transactions, the user has to provide confidential information such as credit, debit card information, personal information etc. As a result, every user's computer or mobile device is being connected to the Internet, which has led to the possibility of theft of confidential information from the user's device.Considering the number of cyber attacks that occur every year, the number of cyber attacks is also increasing every year. The need for cyber security has also increased with the growing number of users due to the benefits of the Internet.

Types of Cyber Crime:

As technology evolves, the nature of cyber attacks appears to be changing. The following types of cyber attacks are prevalent considering the current situation.

Malware:

This is a common form of cyber attack and is a software program designed to harm the Internet user and harm the user's system. e.g. Botnets, Adware, Ransomware, Spyware, Trojans, Viruses.

Zero Day:

In this type of attack, loopholes are detected and the user's software is targeted and damaged.

SQL Injection (SQL Injection):

SQL stands for Structured Language Query. Hackers use this method to steal or gain control of data from a user's database.

Denial-of-service attack:

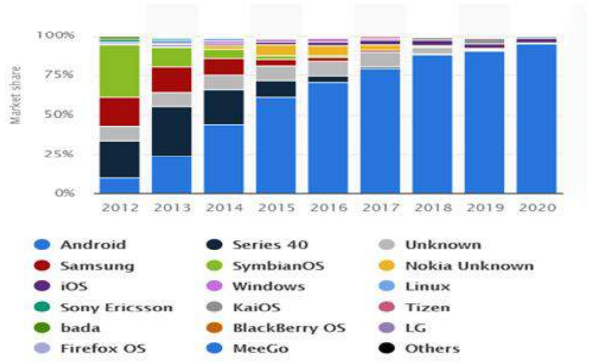
In this type, hackers disrupt the functioning of computer systems and networks. Algorithms can crash. This can interfere with the important work of any individual or organization.

Phishing:

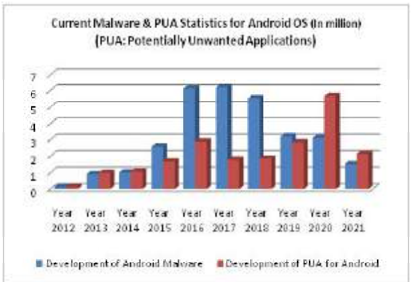
A cyber criminal sends a link to a user via Fake email or Fake SMS. After falling prey to such fraudulent messages, the user gives his personal information like Login ID, password, Credit / Debit Card details. This can lead to danger.

Man-in-the-middle attack:

In this type of cyber attack, hackers interact with the user to gain complete information based on incomplete information available, which the user is not aware of.+



Given the growing number of mobiles and the growing number of operating systems, the Android operating system, which was only 10% on mobile devices in 2012, will be used on about 95% of mobile devices in 2021. In terms of cyber security, if the Android operating system is enabled to withstand various cyber attacks, about 95% of mobile devices will be able to survive cyber attacks. Although the number of unsolicited applications that are not used on mobile has been increasing in the last ten years, the number of unsolicited applications in 2021 is much lower than in 2020.


Current Malware & PUA Statistics for Android OS (In million)
(PUA: Potentially Unwanted Applications)

Security from Cyber Attacks:

Internet use has become an integral part of this age of technology. But not everyone has enough knowledge of the internet.Many people with insufficient knowledge fall prey to these fraudulent e-mails and messages and share their confidential information with strangers or on links. We can avoid cyber attacks by following these steps.

Use of Antivirus:

The main function of antivirus is to prevent viruses from coming through the internet, blocking fake websites and programs. If antivirus is installed on the system, your system can be protected from such viruses.

Updating software and systems regularly:

Hackers try to tamper with software by detecting vulnerabilities. Software engineers are constantly striving to make your software risk-free. They are doing updated versions of the software by correcting the vulnerabilities in your software. Updating software and systems from time to time can avoid potential risks.

Updating software and systems regularly:

Hackers try to tamper with software by detecting vulnerabilities. Software engineers are constantly striving to make your software risk-free. They are doing updated versions of the software by correcting the vulnerabilities in your software. Updating software and systems from time to time can avoid potential risks.

Updating software and systems regularly:

Hackers try to tamper with software by detecting vulnerabilities. Software engineers are constantly striving to make your software risk-free. They are doing updated versions of the software by correcting the vulnerabilities in your

software. Updating software and systems from time to time can avoid potential risks.

Do not open anonymous e-mails:

Some hackers send emails in this manner only to gain access to your device so that they can take control of the system, so avoid opening such anonymous emails as much as possible.

Use of Strong password:

Most of the users choose their password without any worries and choose a very simple and common password which will make it easier for hackers to hack your account. It should be changed from time to time without leaving a permanent password.

Use of a secure Wi-Fi network:

Many users are looking for free Wi- Fi to save their network data. Such Wi- Finetworks can make users a victim of MAN-IN-THE-MIDDLE ATTACK.

Conclusion:

Software is being used in college libraries and data of most of the books in the library is stored on software. Protecting this archived data has become just as important.Today, the idea of data protection does not seem to have come to fruition, but the realization that the need for data protection has arisen in a real sense is evident from the above discussion. For data protection, it is important to strictly adhere to the above and to back up the library data from time to time. Offline accessioning of books is equally important.

References:

https://www.thehindu.com/sci-tech/technology/317-lakhs-cybercrimes-in-india-in-just-18-months-says-govt/article34027225.ece

https://askmarathi.com/cyber-security-mhanje-kay-in-marathi/#2_%E0%A4%9C%E0%A5% 80%E0%A4%B0%E0%A5 %8B_%E0%A4%A1%E0%A5%87_Zero-Day

https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=5803&context=libphilprac

https://www.springernature.com/gp/librarians/the-link/blog/blogposts-news-initiatives/protecting-libraries-from-cyber-attack/18782884

https://www.researchgate.net/publication/284435163_Enhancing_information_security_in_Academic_Libraries

https://www.av-test.org/en/statistics/malware/

https://purplesec.us/resources/cyber-security-statistics/

https://purplesec.us/prevent-cyber-attacks/

https://www.statista.com/statistics/262157/market-share-held-by-mobile-operating-systems-in-india/

https://www.visualcapitalist.com/cyber-attacks-worldwide-2006-2020/

❑❑❑

12

Cybersecurity in Humanities: Issues and Reflections

Dr. Meenal Kshirsagar
Head, Dept of Political Science,
Dr. D.Y.Patil Arts, Commerce & Science
College, Pimpri, Pune

****

Abstract:

This research paper recognizes the salience of cybersecurity as a fact of daily life. Given its ubiquity, scale, and scope. Cybersecurity has become a fundamental feature of the world human live in and has created a fundamentally new reality for almost everyone in the developed world and increasingly for people in the developing world. This paper examines an important aspect of this new international reality, namely the network of institutions responsible for addressing threats to the security of cyberspace and security in humanities transmitted via cyber venues. In this context, institutions are located at the intersection of two important lines of inquiry in social science, namely in the long tradition of institutional analysis in humanities and the nascent area of theorizing about cyberpolitics in humanities.

Key words: Core Assumptions in Cybersecurity, Structuring the New Context, Response to Security Threats and Cyber Crime, Complex array of organizations, Issues in Cybersecurity, Reflections.

Introduction:

With the evolution of Europeanintegration, cybersecurity took a new turn, seeking to connect domestic, humanities and international politics,and to signal potentials for diffusion of institutional development. Subsequently, the conceptualframe of reference shifted to focus on the "demand" and the "supply" driving the development ofinternational institutions including humanities.Subsequently, the concept of regime emerged as an important anchor in the field of cybersecurity. Thisresearchpaper, focus on the formal aspects of regimes, namely the humanities manifestations,rather than on underlying norms and principles. While the literature tends to argue that consensuson norms precedes the formation of institution. The cyber domain the reversedynamics hold, namely that social sciences may well be the precursors for formalizing norms andprinciples that, in turn, might consolidate and strengthen the institutions themselves.At this writing, yet another shift has taken place, namely from institution-centered issues tomatters of broadly defined governance. The current institutional landscape managing security issues in the cyber domain is notsufficiently resilient to address existing and future issues and reflections effectively.

Core Assumptions in Cybersecurity:

At least three features of cyberspace are seriously at odds with core assumptions in humanities related to international relations, thus potentially seriously limiting the portability of theory from the traditional into the cyber domain.

· First is the fact that cyberspace is managed by the private sector – albeit with the support and direction of the dominant power in world politics, the United States. The involvement of the state-system in the management of cyberspace is a relatively recent development; the entire cyber domain is managed by non-state entities, an important aspect of scale and scope in international relations.

· Second, the usual mechanisms for tracking activities in the physical world – statistics, standards, are not readily portable to the cyber domain. An international consensus on the differences and similarities is yet to be fully established.

· Third, the very nature of the "virtual" is distinct from that which is physical. Threats in the "virtual" domain are often identified after the fact, rather than tracked "in process." In the cyber domain, there is not only no early warning system, but there are alsoas yet few early signals of a cyber threat, if any.

Structuring the New Context:

Throughout the early years of Internet development, security was not established ormaintained only a formal or planned institutional framework; instead, the critical roles of threatdetection and mitigation were largely left to the private sector. Companies were expected to handlesecurity for their own products, and users accepted some inherent risk or liability. However, thisapproach was never suited to handle significant growth in vulnerabilities. Individual corporationslacked incentives to share information, and more importantly, lacked the legal authority to deal withemerging national threats or to prosecute criminal networks. As a result, response to cyber incidentsremained closeted and uncoordinated, with private entities adopting a largely reactive approach. Observing this situation, several non-profit organizations attempted to fill the organizationalgap by providing volunteer response teams, information sharing networks, and security guidelines.By focusing on issues that spanned the corporate barrier, these non-profit organizations establisheda foundation for coordinated community response to emerging cyber threats. Although they were Institutional Foundations for Cyber Security often successful at mitigating localized security issues, non-profit organizations lacked the requisiteauthority and resources to effectively respond to crises of global or national scope.

Over the better part of a decade, the convergence of four distinct but interconnected trendscreated demands for formal interventions involving governments and international coordination.

· First, Internet usage continued to rise, coupled with an expansion in forms of use.

· Second, many governments recognized that cyber vulnerabilities continued to threaten not only the security of their own networks but also those of their citizens involved in routine activities on a daily basis.

· Third, there was a noted absence of coordinated industry response or of efforts to develop cooperative threat reduction strategies, thereby reinforcing an unambiguous gap-in-governance.

· Finally, a growing set of cyber incidents, large and small, signaled to governments the potential impact of their failure to address the emerging threat. In response to these trends, governments, in various ways, mobilized significant national and international resources towards the creation of a broad cyber security framework.

Response to Security Threats and Cyber Crime:

A theoretical approach to in the field ofhumanities at the international level, generallyaddressed by scholars in the field of international relations in social sciences are based on historical and conceptualfoundations different from those of institutional analysis at the national level generally addressedby scholars in the field of comparative politics. While there are some common concerns andshared presumptions, the overall motivations, assumptions, and perspectives on the underlying problems differ considerably.

In some sense, the lack of dramatic success thus far is unsurprising. Efforts to halt the spread of cybercrime suffer from a number of inherent challenges.

· First, in contrast with traditional crime, the criminality of cyber activities remains ill-defined. In social sciences many individuals are not accustomed to reporting cybercrime to law enforcement organizations because issues may be deemed 'minor' or purely technical in nature, or because events on the Internet are deemed outside the jurisdiction of a local police agency. This issue is present in the corporate sphere as well, as many companies view the public acknowledgement of security vulnerabilities as a corporate liability.

· Second, even when crimes are reported, investigation and prosecution remain difficult. Evidence is often ephemeral and transitory, and the global nature of cybercrime presents serious difficulties in pinpointing the location and identity of criminals.

· Lastly, it often proves difficult to assess the true monetary damage of cybercrime; for instance, in the case of information theft or security breach. Given that law enforcement agencies possess limited resources, this ambiguity surrounding the true impact of cybercrime creates difficulties in setting investigative priorities.

Complex Array of Organizations:

The provisions for humanities in cyber security landscape consists of a complex array of organizations that exhibit significant diversity about missions, mandates, interests, opportunities and constraints. It is observed that :

· The current institutional landscape resembles a security patchwork that covers critical areas rather than an umbrella that spans all the known modes and sources of cyber threat.

· Given the multiple contexts and diverse institutional motivations, It will be driven more by institutional imperatives and reactions to crisis than by coordinated assessment and proactive response.

· Due to the complex global agenda at all levels of development, states may not be willing to proceed until international norms are developed, rather they will 'take matters in their own hands' and develop first order rejoinders.

· Cross-sector collaboration among public, private, and volunteer organizations may serve as a temporary measure to cover holes in the current defense network. However, at some point effective institutions will be necessary; they may develop in parallel with rising public awareness.

Issues in Cybersecurity:

Cybersecurity is inherently complicated due to the dynamic nature of the threats and ever-expanding attack surfaces. Ironically, this issue is exacerbated by the rapid advancement of many new technologies like Internet of Things (IoT) devices, 5G infrastructure, cloud-based computing, etc. This is where artificial intelligence (AI) and machine learning (ML) techniques can be called into service, and provide potential solutions in terms of threat detection and mitigation responses in a rapidly changing environment. Contrarily humans are often limited by their innate inability to process information and fail to recognize and respond to attack patterns in the multi-dimensional, multi-faceted world. The recent innovations have proven machines can defeat even the best human pilot in air-to-air combat. The global cyber threat continues to evolve at a rapid pace, with a rising number of data breaches each year.The global cyber threat continues to evolve at a rapid pace, with a rising number of data breaches each year.

Cyber-related developments have both dramatically altered the nature of security threats and expanded the landscape of potential tools for countering those threats. Experts from multiple disciplines, including humanities, electrical engineering, software engineering, computer science, and computer engineering, have a laser focus on cybersecurity, but that focus has been primarily on technical or data challenges, such as identification and prevention of malware, prevention of denial-of-service attacks, self-fixing code, unauthorized data breaches, tools for the cyber analyst, and privacy. Indeed, cybersecurity is often characterized as the set of techniques used to protect the integrity of networks, programs, and data from attack, damage, or unauthorized access. These techniques have undisputed value, but they address only technological challenges, not the human behaviors and motivations that shape those challenges.

The tools of cybersecurity have obvious relevance for national security. Intelligence analysts, however, seek to understand a different but related set of critical problems—those that involve cyber-mediated communication (communication that takes place through computer networks). To understand this phenomenon, it is necessary to integrate insights about constantly evolving technology with understanding of fundamentally human phenomena.

Reflections:

Experts in cybersecurity focus on attacks made on and through the cyber infrastructure that are intended to interfere with technology, steal or destroy information, or steal money or identities. While cybersecurity experts do draw on social science research social cybersecurity researchers have a different approach: they focus on activities aimed at influencing or manipulating individuals, groups, or communities, particularly activities that have large consequences for social groups, organizations, and countries. The solutions to some problems, such as denial-of-service attacks, malware distribution, and insider threats, require both types of expertise, but the emphasis in the social science fields is quite different.

· Take the sociopolitical context of cyber activity into account both methodologically and empirically;

· Integrate theory and research on influence, persuasion, and manipulation with study of human behaviour in the cyber-mediated environment; and

· Focus on identifying operationally useful applications of their research.

The field of social science cybersecurity does not simply supplant the important work of research. It is the field build on some existing work and extend other work to generate new knowledge and in some cases develop new theory and methods that arise from the transdisciplinary approach for studying the cyber environment. Social cybersecurity is a computational social science, one of a growing number of social science fields that are using digital data and developing computational tools and models. Computational social science is not the application of computer science techniques to social science problems and data, it is the use of social science theories to drive the development of new computational techniques, combined with further development of those theories using computational techniques for data collection, analysis, and simulation.

Conclusion:

Cybersecurity in humanities, on the one hand social scientists and policy analysts and computer scientists and engineers on the other have not always recognized the implications of each other's perspectives for their own research. For example, computer scientists' attempts to identify disinformation usually begin with fact checking. However, most disinformation campaigns rely less on blatant falsehood than on other strategies, such as illogic, satire, facts out of context, misuse of statistics, dismissal of topics, intimidation, appeals to ethnic bias, and simple distraction, all topics of research. Similarly, when social science researchers seek to invent or reinvent computer science techniques, the results typically do not scale, are difficult to maintain, and lack generalizability. For example, affect control theory and a valuable computational model of human emotions based on social psychology cannot be scaled to handle large social groups and populations. Computational social science, in contrast, requires deep engagement in and integration of knowledge, theories, and methods from both computer science and social science. Social cybersecurity science is often viewed as going beyond the interdisciplinary approach of integrating the methods and knowledge of diverse disciplines, having become a truly transdisciplinary science in the sense that it is creating new knowledge, theories, and methods.

References:

· SocialCyber-Security -CASOS - Carnegie Mellon Universityhttp://www.casos.cs.cmu.edu › projects › projectsPDFby KM Carley· Cited by 39.

· Social and Behavioural Science in Cyber Security Research ...https://medium.com › cybersoton › social-and-behavio...

· Social science and cybersecurity: a key challenge for the futurehttps://observatoire-fic.com › social-science-and-cybers...

· M.S.Bhatt and AsherefIlliyan, “International Technology in the Indian Economy”, New Central Publications, New Delhi, 2009.

· S.K.Bansal, “Cyber Crime”, A P H Publishing Corporation, New Delhi, 2013.

❑❑❑

13

E-Commerce & Cyber Security in India

Asst. Prof Sweenal Stany Fereira

Asst.Prof Hycintha Malcolm Andrades
St Gonsalo Garcia College of Arts &
Commerce, Vasai

****

ABSTRACT:

E-Commerce has redefined the conduction of Business in India and across the globe. Use of Electronic medium and Internet is the distinguishing feature of E- Commerce to Traditional commerce. Till last year, E-Commerce was used to buy premium & Non-Daily products by Indian Consumers. However the Covid-19 pandemic has shown a major shift in the buying - selling pattern. Majority of Indian consumers preferred online shopping, Retailers & MSMEs have shown willingness to adopt E-commerce.

This online platform comes along with its own set of opportunities and threats. Various stakeholders while reaping the benefits of online purchases and sales, have simultaneously been hit by the technical glitches. Issue of Security has always been a major concern. Cyber Criminals have exploited the vulnerabilities of Covid Crisis. There have been rising reports of Data breaches & other cyber crimes, highly alarming the adoption of Cyber Security measures.

This paper briefly addresses Impact of various factors on the growth of E-commerce, various types of cyber security threats to E-commerce and cyber security measures.

Key Words: E-Commerce, Cyber Threats, Cyber Security

INTRODUCTION:

Oxford Advanced American Dictionary defines **E commerce** as "business that is conducted on the Internet". It refers to using the internet for buying and selling of goods and services and transfer of money and data to execute these transactions. Eg Clothes purchased on Myntra app & payment made via Debit card. The business transactions can be in following ways: Business to Business (B2B), Business to Customer (B2C), Customer to Business (C2B), Customer to Customer (C2C). As of now, e-commerce is one of the fastest growing industries globally.

Online business has its own set of pros & cons. A Reach to larger market share, better customer insights through tracking & analysis, unlimited opportunities to scale up or scale down the trade, similarly better buying opportunities available to customers are a few advantages of Online trade. Also there are challenges unique to this online business model like IT Security threats, frauds etc

The Internet Engineering Task Force (IETF) defines a threat as, "A potential for violation of security, which exists when there is an entity, circumstance, action, or event that could cause harm." Eg: Phishing. According to a report, the ecommerce industry experiences up to 32.4% of all successful threats annually. Credit card frauds, phishing, spamming, malware and other financial frauds pose **Security threat** to E Commerce business. These threats can be deadly to the users and therefore proper security measures need to be taken i.e adoption of cyber security measures.

As consumers shift online, there is greater need for cyber security services. **Cyber security** is a method to ensure that the computer resources, computer networks and its data is safe from malicious attacks & continues to operate. Eg: use of strong passwords

Cyber security, also called Information Technology security, is the technique of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed for exploitation.

OBJECTIVES:

- To understand the Ecommerce Industry & Factors responsible for its growth

- To study various cyber security threats & its measures

SIGNIFICANCE OF STUDY:

With online business here to stay and rule the way trade is carried out, it becomes important to understand the same, along with the opportunities & threats that it possesses and to study the cyber security measures to overcome the cyber threats.

RESEARCH METHODOLOGY:

This paper is purely based on conceptual studies. The Secondary data is collected from newspapers, journals, research articles, websites & various reports on the subject.

FINDINGS:

The growing E-Commerce Industry in India:

The way business is done in India has been majorly changed and has been transformed by Ecommerce. Indian E-commerce industry is estimated to grow to US$200 billion by 2026 from US$38.5 billion of 2017.According to RedSeer, the number of online shoppers in India is estimated to cross 250 million by 2022. As per the report by IBEF dated 2nd June 2021, Indian E Commerce will reach US$ 99 billion by 2024, growing at a 27% CAGR over 2019-24

- Factors contributing to the growth of Indian Ecommerce Industry:

- Increasing internet & Smartphone penetration in Indian markets

-The ongoing digital transformation in India

-COVID-19 crisis: in a recent survey conducted by LocalCircles, a community social media platform,49% Indians preferred Ecommerce sites & apps for shopping in the last 12 months. In Spite of Traditional markets opening in June 2020, customers choose online mode to fulfill their shopping needs

-Initiative of Ecommerce platforms to digitize MSMEs: In 2020, Amazon pledged to digitalize 10 million MSMEs; In February 2021,Flipkart partnered with Maharashtra State Khadi & Village Industries Board & Maharashtra Small Scale Industries Development corporation to bring local artisans & small & medium businesses into the purview of e commerce; In February 2021, Zomato entered into agreement with ministry of Housing & Urban Affairs to introduce 300 street food vendors on its portal.

-Introduction of JioMart, Indian Online grocery store which aims to strengthen its hold in E-commerce & digital payment services after entering into agreement with Infibeam Avenues.

-Robust consumer demand, according to Retailers Association of India (RAI), the retail industry achieved 93% of pre-covid sales in February 2021

-Easy credit available to the customers

-Increasing Investments with cumulative FDI inflows as 100% FDI allowed in Single Brand Retail Sector & 51% in Multi-Brand Retail

The above data indicates a significant shift of consumers toward online shopping.

E-Commerce and Cyber threats

With an increase in technology advancements, more businesses, people & organizations have come closer than ever before, paving the way for growth of Economy. However these progressions make the system vulnerable to various threats which are exploited by cyber criminals. As per the article, "India becomes favorite destination for cyber criminals amid covid-19" in Business Standard dated 5th April 2021, In February 2021 - there were 377.5 million brute force attacks worldwide as compared to 93.1 million worldwide in the beginning of 2020.

Thus as systems get more Interlocked, another significant factor hovering over is the rising number of data breaches & sober cyber attacks.

- Major Common security threats to Ecommerce Business in India include:

- Financial Frauds: Cyber Criminals make unauthorized transactions, leading to huge losses to business houses. Eg: Credit card Frauds or Fake returns & Refund Fraud

-Spam: Spammers leave infected links, spamming affects website's security as well affects the speed

-Phishing: Hackers trick the customers to reveal their sensitive information by presenting fake copy of authentic website

-Bots: Hackers use this technique to change the pricing of online stores

-DDoS Attacks: Attacker intends to crash website by flooding numerous request

-SQL Injections: Attacker injects malicious code in the database by targeting query submission

-XSS: Website visitors are targeted by infecting online store with malign code

-Malware: Sensitive data can easily be swiped by these programs present in the infected system. Eg: spyware, viruses, trojan horse & ransomware

The above security threats have a potential to disrupt major business activities causing electric blackouts, theft of sensitive data, loss of customer trust, financial loss to the business house etc. According to the Inc24 report, cyber security incidents amounted to 208,456 in 2018. In 2019, estimated loss of Rs 1.25 lakh cr occurred due to cyber crimes. According to a study by IBM Security, the average total cost of a data breach in India touched Rs 14 crore in 2020, an increase of 9.4 percent from last year. According to a K7 Computing report, Tier II cities are more prone to cyber security threats.

E-Commerce and Cyber Security measures:

As the scale of online shopping increases, there is greater need to protect the online business from the vulnerable cyber threats. Ecom giants like Amazon India faced the security breach of almost 400,000 seller's data. Zomato faced a similar incident where data of 17 mn users was stolen by cyber criminals. Companies are exposed to bigger threats in areas of virtual data centres.

- Constant effort to implement security infrastructure is a stronghold against Cyber Security threats, few of them listed as below:

-upgrading to HTTPS, having SSL certificate & HTTP protocol has become a standard now

-Securing Servers by use of complex passwords & usernames

-securing admin panels by enabling panel notification to identify unknown IP attempts logins

-securing payment gateway, ecommerce recommendations must obtain a Payment Card Industry Data Security Standard(PCI DSS) accreditation

-Installation of Anti - Malware software or Anti - virus software

-Use of Firewalls

-Regular Back of data

-opting for secure Ecommerce platforms

-Training staff & Educating Customers to avoid cyber attacks

-being vigilant & keeping an eye on any suspicious online activity

With Indian E Commerce expected to grow and to secure the second largest position by 2034, there is greater need to fix the security issues. Due to Covid-19 pandemic as well, cyber security is attracting a lot of attention from company boards & Governments alike thus increasing demand for cyber security services in India, which is expected to grow about $7.6 billion in 2022 from $4.3 billion at present. Being vigilant about the activities posing threats to the online business is a smart approach.

CONCLUSION AND RECOMMENDATIONS:

The overall study reveals the tremendous potential of Indian e-commerce industry which is to grow in coming years, thus to reap its benefits, security concerns need to be addressed well.

With a lucrative opportunity for growth of Indian Ecommerce business, the responsibility to address the security concerns is the need of the hour. The key is to identify threats and prevent the same.

Even though cyber attacks are recurring and ever evolving, certain attacks and threats can be estimated beforehand. Third party solutions can be implemented. Recently due to Covid-19 pandemic, cyber security has garnered a lot of attention. The cyber security market in India is growing twice as fast as the global market. As cyber attacks are on rise the one thing that will make a significant difference is adopting cyber security measures.

REFERENCES:

Webliography

https://www.cloudways.com/blog/ecommerce-security-tips/

https://inc42.com/resources/as-consumers-shift-online-there-is-greater-need-for-cyber-security-services/

https://www.google.com/url?q=https://www.bigcommerce.com/blog/ecommerce-website-security/%23conclusion&usg=AOvVaw2pjAuCmADF0adbOHdExJFF

https://www.loginradius.com/blog/start-with-identity/2020/11/ecommerce-security/

https://www.getastra.com/blog/knowledge-base/ecommerce-security-threats/

https://www.researchgate.net/publication/351779456_THE_FUTURE_OF_E-COMMERCE_IN_INDIA

https://www.weforum.org/agenda/2020/01/e-commerce-sme-globalization-equality-women/

https://www.weforum.org/agenda/2018/04/42-of-global-e-commerce-is-happening-in-china-heres-why

https://www.ibef.org/industry/

ecommerce.aspx

https://www.ibef.org/industry/retail-india/infographic

https://www.google.com/url?q=https://www.indianretailer.com/article/multi-channel/eretail/future-of-e-retailing-in-india-growth-and-challenges.a6856&usg=AOvVaw2zYuZWUbfZrT2f5maqJBt_

https://retail.economictimes.indiatimes.com/news/e-commerce/e-tailing/e-commerce-revolution-in-india-gets-its-second-wind-post-covid-19/77460376

https://www.google.com/url?q=https://www.business-standard.com/article/technology/tier-ii-cities-more-prone-to-cyber-security-threats-k7-computing-report-119122301209_1.html&usg=AOvVaw3gL2I_ca35zOEC7OnYVIL9

https://wap.business-standard.com/article/companies/indian-cybersecurity-services-expected-to-grow-to-7-6-bn-by-2022-dsci-120052101401_1.html

https://www.thenewsminute.com/article/49-indian-consumers-shopped-e-commerce-sites-apps-last-12-months-survey-145364

https://theprint.in/theprint-valuead-initiative/how-pandemic-fostered-indian-consumers-faith-in-e-commerce-sites/625720/

❑❑❑

14

Fine Arts and Cybersecurity

Mr. Nirmal Ekanath Sitaram
Department of Political Science,
Art’s Commerce And Science College Satral,
Tal:-Rahuri, Dist:-Ahmednagar

****

Introduction: Arts and culture are mirrors of the intact journey of the humanities, connecting people, nations, cultures, civilization, and time. With arts and Humanities projects we are trying to demonstrate that all transformation of nature as oneself depend upon human actions and those are supported by cultural methods of interpretational and understandings. To backdrop its essential is to verify about various miscellaneous signs of threats approaching us, detecting, identifying, we can avoid or imitigate the risks. Doing so-far are steps evolve into the art of security .Protecting data can be form of art as, the cyber security itself is linked with the bridging communities. Protecting Big data is not a single handed task, thus it requires interpreting data correctly and storing it safely in the form of art and to maintain the same intact journey of humanity.

Arts and culture are mirrors of the intact journey of the humanities, connecting people, nations, cultures, civilization, and time.

Arts and culture are mirrors of the entire journey of the humanities, connecting people, continents, cultures, civilization, and time. Through the practice of the arts, we can illustrate a pattern of a way of communication that transcends time and difference. It permits an understanding of our virtues and our limits, our objects as well as our use of signs, symbols, and languages. The language of the arts is shared by all cultures. It can illustrate a basis for an understanding of the universal functioning of the human mind, observing the world and evolving to symbolic forms that have helped and guided humanity with its infinite productions and inventions.

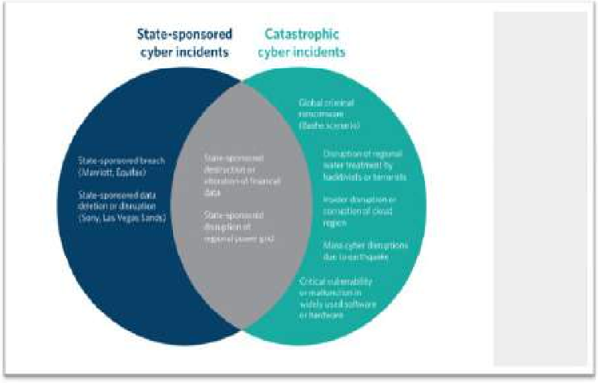
Arts and culture are the materialization of a huge accumulation of knowledge, of scientific and conceptual exploration and knowledge. This gathered data is a record of the development of humanity. With the rise of globalization, humanity has developed the need for faster and faster global processing of memories, shared connections, and equipments. Big Data offers various ways to examine and process knowledge, to analyze, to process information, then to act. It refers to the processing of all data produced by the use of new technologies, for intimate or professional purposes.

Utilizing Big Data, we can foresee new analytical tools and data modeling, carry out new forms of comprehension, improve collective knowledge, anticipate risks, and monitor ecological and other various phenomena in real time. However, it can be a tool of influence and manipulation, and a cause for disruptive opinions of interest within economics, politics, and society as a whole. With the arts, we can imagine beyond facts into something unknown .

We in the game of the arts the forces that created and create the world. According to the esteemed sociologist and historian George Derluguian, it has become difficult to predict the future and more complicated the world becomes, and facing the anger of the common people and the risk of radical upheaval of the political and economic system, it is urgent to think over the relationship between citizens and the state. It contend that the humanities and the arts may be the best tools to fight all forms of ignorance the main cause of all systems is discrimination, prejudice, hatred, and Arts and culture are mirrors of the entire journey of the humanities, bridging people, continents, cultures, civilization, and time conflict.

At this early stage, cybersecurity may more closely resemble the School of Hard Knocks than a College of Arts and Sciences. However, when witnessing the creativity of pen testers or the wiliness of red team competitors, it's hard to see their exploits as anything but dramatic and imaginative creative expressions. And what else is art?

The science is the technology that will help you build a encrusted, in-depth safeguard approach. The art is how to identify the threat, define and document the risk, and form a strategy that allows you to manage your cyber risk as it applies to your atmosphere, user, system, application, data, customers, supply chain, third party support partners, and business process..


State-sponsored cyber incidents
Catastrophic cyber incidents
State-sponsored breach (Marriott, Equifax)
State-sponsored data deletion or disruption (Sony, Las Vegas Sands)
State-sponsored destruction or alteration of financial data
State-sponsored disruption of regional power grid
Global criminal ransomware (Bashe scenario)
Disruption of regional water treatment by hacktivists or terrorists
Insider disruption or corruption of cloud region
Mass cyber disruptions due to earthquake
Critical vulnerability or malfunction in widely used software or hardware

Safety:

Populace:

Users understand hazard and risk and recognize what role they play in the protection strategy. For example, if you see something, say something. Don't wait till somebody surf in behind you through a badge check entry. And don't think about trying to put down the lid to your end-point anti-virus or firewall. In today's remote workforce surroundings, excellent employee security alertness especially related to phishing is essential.

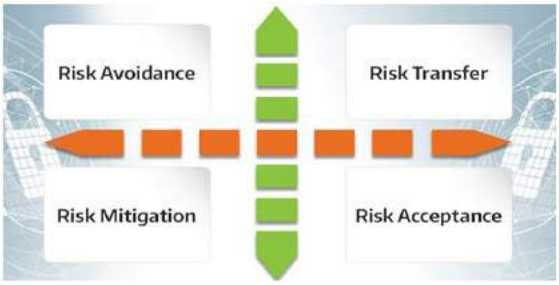
Process: Policies are established, documented, and socialized. Personal laptops should never be connected to the corporate network. Also, need to be attentive to sending sensitive information to your personal email account so you can work from home safely and securely.

Technical ways: Some of the barriers used to detect attackers and breaches are edge security with firewalls, intrusion detection and prevention, sandboxing, and advanced threat detection. Security officials need to become a student of threat, and deploy any possible strategies to protect, detect, and react to threat.

Detecting Factors:

The average mean time to identify an active incident in a network is 197 days. The mean time to contain an incident is 69 days. Detection is a proactive process.

Technicians: Incident response teams need to be identified and trained, and all employees need to be trained on the concept of **"if you see something, say something."**



Conclusion:

The above article represents correlation between the art as the precious form of nature inculcating the values through people bridging with ethics and developing skills to live ,while correlating it with cyber security explains briefly the importance and consensual information shared and sent Online can disrupt the relations and harmony . While learning the topic or subject like 'cybersecurtiy' ethical teachings are given with accordance to arts, humanities and social studies to inculcate the values and ethics so as to develop a sense of responsibility.

Here the article focuses on the arts and cyber security as they are correlated to each other, these days Nobel courses have most of the attention of students and guardians as compared to arts, forgetting that arts humanities are also important to induce the values, culture, ethics, etc.

Reference-

·https://images.carnegieendowment.org/images/article_images/202010-Bateman-Figure-4.png

· 1. Georgi Derlugian. "Nous devons revenir aux theories anarchistes d'autogestion." interview by Alexander Mekhanik et Piotr Skorobogaty.

· 2. Adama Samassékou. "Humanities, or how to quench the thirst for humanity." CIPSH, 2017. 3. Aimé Cesaire, interview with Khalid Chraibi, 1965.

· https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcSWkbwd4XECDPq1sile-hLpMmwemnHzQKcDoQ&usqp=CAU

· https://community.connection.com/wp-content/uploads/2019/04/888093-Risk-Avoider-Risk-Transference.jpg

· https://community.connection.com/cyber-security-three-parts-art-one-part-science/

❑❑❑

15

Impact of Cybersecurity Issues on Financial Inclusion

Mr. Kushal Ramesh Pakhale

Dr. Gorakshanath Kalhapure

****

1) Introduction –

Advanced and Digital financial services hold extraordinary guarantee as a way to empower financial inclusionand along these lines help improve individuals' lives. In any case, cybercrime has become a vital worry in creating and arising nations' monetary business sectors and is taking steps to block worldwide advances in building more comprehensive monetary areas. Over ongoing years, monetary business sectors in Sub-Saharan Africa, the East Asia and Pacific locale, Latin America and South Asia have been influenced by a fast expansion in the quantity of digital episodes and information penetrates – and especially influenced are those business sectors with higher volumes of Digital financial servicesexchanges. While markets in Asia are recording the most noteworthy use paces of versatile banking and advanced installment applications, they are additionally encountering the most elevated volume of cyberattacks on monetary establishments. In 2016, monetary foundations in Bangladesh, Indonesia, Japan, the Philippines, Taiwan and Viet Nam were focused on in a progression of assaults. In Sub-Saharan Africa and Latin America, cybercrime is likewise on the ascent, with digital criminal networks in these two areas becoming quicker than elsewhere. One clarification for these patterns might be the way that Digital financial servicesexchanges are regularly completed utilizing uncertain gadgets and over transmission lines that were not intended to ensure the security of monetary exchanges, which leaves Digital financial servicesframeworks and suppliers more defenseless. Moreover, with created economies developing their guards against cyberattacks, digital lawbreakers (cybercriminals) appear to be moving their thoughtfulness regarding simpler focuses in arising Digital financial servicesmarket and misusing their weaknesses.

Succumbing to a trick or encountering framework access blunders can result in monetary and mental harm and will unquestionably influence a client's certainty and trust in the financial Services. A huge reason for client disappointment with Digital financial servicesprovider is spontaneous framework blackouts. Exploration on the mentalities and practices of low-pay portable cash clients shows that failure to execute because of organization or administration personal time was evaluated as perhaps the best inconvenience and brought about flippant practices that put the clients in danger of being defrauded. The pessimistic encounters demonstrate to deflect Digital financial servicesbuyers from utilizing versatile cash benefits all the more as often as possible and fundamentally diminished the degree of trust in providers and the financial framework altogether. Poor individuals are especially defenseless against misrepresentation and framework access mistakes that can result from a digital occurrence. They are regularly less mindful and taught about friendly designing attacks, they are bound to utilize gadgets and channels that are not intended to offer the security required for a monetary exchange and, above all, they would least be able to stand to lose cash. Another issue is that in Developing Countries clients are frequently responsible for misfortunes related with a digital episode, or they bear the weight of demonstrating that they were the person in question. In 2016 the International Telecommunication Union (ITU) and CGAP reviewed 5,220 portable cash clients from Ghana, the Philippines and Tanzania. Deceitful or trick SMSs had been gotten by 83% of the Philippine respondents, 56% of the Ghanaian respondents and 27% of the Tanzanian respondents. In both the Philippines and Tanzania, 17% of the versatile cash clients met detailed having lost cash to a misrepresentation or a trick, while 12% of the Ghanaian respondents made the equivalent admission. Because trust and trust in financial service Provider and installment frameworks are key elements for supported financial inclusion, digital occurrences and their related misfortunes can prevent endeavors to grow admittance to monetary services. Besides, these sorts of episodes and clients' negative encounters can spread rapidly by overhearing people's conversations and may possibly wind up sprinkled across the media. In the wake of such harm, it's anything but a great deal of time and exertion to modify notorieties and individuals' trust.

2) The present status of Cyber Security Issues in developing nationsfinancial business sectors

Financial Service Providers and their clients, just as monetary area controllers and managers, face difficulties in changing their practices, cycles and arrangements to suitably address the developing danger of cybercrime and innovative disappointments. To all the more likely comprehend the pervasiveness and reasons for these difficulties, in 2018 CGAP led a study of Financial Service Providers, Digital Financial service suppliers, Financial frameworks administrators, policymakers and information security specialists from sub-Saharan Africa. The exploration showed that policymakers know about the issue. They are attempting to foster administrative structures and assemble their own in-house limit with the goal that they can successfully direct and manage the area as well as secure their own information and frameworks. Financial service providers will in general turn out to be more delicate to the danger of cybercrime solely after they have themselves been focused on. More modest Financial service providers tend not to focus on digital dangers over different dangers as the probability of an assault is as yet viewed as little. Extensively talking, portable cash administrators are more ready and better prepared to deal with digital dangers, particularly those administrators that are controlled by worldwide mobile network operators (MNOs), which as of now cling to the global security guidelines set by the telecommunications sector.

2.1) The financial services industry is poorly ready

The industry, in developed, developing, and emerging economies, has perceived the developing dangers of cybercrime. As of late, the business has created principles and direction for financial service providers to assist them with bettering their networks and their clients. The presentation of multifaceted verification and chip cards has altogether diminished the burglary of buyer accreditations, and new apparatuses like AI and man-made brainpower are improving the business misrepresentation discovery and goal measures. Increasingly more financial service providers are putting resources into digital protections and strength.

While digital protections and great online practices are being embraced in developed nations and by huge worldwide financial service providers, medium-sized and more modest financial service providers, and especially those working in agricultural nations, remain underprepared. A survey of more than 700 associations from across Africa tracked down that the financial area lost USD 1.05 trillion because of cyberattacks in 2017. The survey announced that 75% of associations were not utilizing security testing procedures, 60% of associations were not staying up with the latest with network protection patterns and assaults, and 75% of the weaknesses distinguished inside associations included missing patches and programming bundle refreshes. In reality, the survey expresses that "Africa's reserve funds and credit agreeable associations, cooperatives banks and microfinance establishments are the most defenseless because of frail framework shields and assurances

2.2) Policymakers ability requirements restrain understanding and viable guideline and management of cyber security

Cyber criminals are not simply focusing on purchasers and suppliers; national banks and financial institutions can likewise be the objective of assaults. Controllers and managers gather and handle classified and delicate data about the area that can bear some significance with hoodlums or might be sufficient of a resource for lawbreakers to hold them prisoner. One model is Bangladesh's national bank, which succumbed to an online heist in 2016.

Likewise, controllers and chiefs are getting mindful of the need to foster administrative structures, industry direction and administrative cycles to guarantee that the financial sector is executing the vital cycles and frameworks to forestall, distinguish and viably oversee cyberattacks.

Regulators, whose point is to guarantee the dependability of the financial sector, are being called upon to foster suitable administrative structures to react to the difficulties that financial establishments and their clients face and to fortify digital flexibility. As of now, law authorization offices in creating and arising nations are battling to stay aware of changes in innovation, a circumstance that is permitting a cybercrime-based economy to thrive. Programming that empowers scrambled correspondence and virtual private organizations (VPN), from one perspective, can shield activists and dissenters from severe systems in any case, on the other, has permitted cybercriminals to stow away from law implementation. Encryption makes it more trying for law requirement organizations to distinguish malignant web traffic and track the interchanges of criminal gatherings. Simultaneously, hoodlums have created abilities and instruments to impede specialists. Law authorization organizations have since a long time ago battled with an absence of assets (i.e., financing, abilities, gear and preparing) to battle cybercrime, however that is just one of the difficulties they face. It is significantly more hard to seek after transnational lawbreakers.

In many developing nations, enactment tending to cybercrime is deficient, disciplines are inadequate, and the lawful aptitude needed to arraign cybercrimes is hard to come by. There are additionally huge procedural obstacles, including issues of purview, challenges in keeping up guidelines of proof, and the trouble of disclosing complex advanced wrongdoings to juries. Crooks are much of the time left to work without risk of punishment for a few reasons; for instance, nonappearance of satisfactory proof sharing and removal settlements among nations and absence of ability to examine cybercrimes, distinguish or find wrongdoers, or arrest offenders

3) Endeavour for addressing the cyber security issues

Public and private sector drives, including public and global endeavors, are presently arising that look to address the dire requirement for data, specialized guidance, preparing and occurrence reaction. The business sectors in developed, developing nations include various great practice models, where suppliers as well as open area offices have collaborated to share data and offer help to the Financial sector. A portion of these endeavors are driven by the public sector, however most are private sector drove or include public-private partnership.

3.1) A couple of governments put resources into building public cyber security infrastructure for the financial sector

In emerging markets, the cyber security endeavors drove by governments or public offices frequently don't focus on the private sector as clients. Because of restricted limit and assets, public network protection drives will in general zero in on serving public offices and basic foundation - the main resources for market soundness and trustworthiness. However, in any event, for serving their own organizations and market foundation, limit and assets are regularly deficient to adequately prepare and teach public office staff, enroll specialized specialists and offer the help that regulators and administrators need. Normal public help structures are computer emergency response teams (CERTs) or national computer security incident response teams(CSIRTs) that help when an IT or information framework has been attacked. In Africa, an ever increasing number of governments are setting up such designs, with a couple of effectively going. Be that as it may, the computer emergency response teamsand national computer security incident response teamsfrequently need limit and battle to stay aware of the fast changes happening in the digital danger scene, which, thus, impacts on the counsel and backing they can give to industry. Just a modest bunch of nations have computer emergency response teamsthat have some expertise in reacting to monetary area dangers and occurrences. It is typically the situation that the scope of administrations given by these groups is exceptionally restricted, administrations are not accessible every minute of every day and rarely incorporate a crisis reaction line.

3.2Financial service providersand affiliations are driving communitarian endeavors to upgrade their digital strength

In most developed nations, and a few arising and developing nations, private sectors players are collaborating to share danger data and mutually battle financial extortion and cybercrime. As a rule, banking affiliations have started to lead the pack in formalizing trade of digital dangers. Now and then, a couple of entertainers will consent to work together and set up an organization, with different gatherings then, at that point joining over the long haul. Associations come in various structures and they are not generally restricted to financial sector people; they have likewise included firms from the IT, media communications and insight areas. All the more as of late, there has likewise been a sharp expansion in the quantity of digital protection and monetary security organizations, regularly of a more modest size, that see a specialty market in giving network safety items and administrations to financial service providers and fintech organizations. Another advancement is the expansion in digital protection items, particularly among huge global insurance agencies.

4) Conclusion

Banking services are moving to computerized at a consistently quicker rate and, in emerging economies, are progressively being utilized by low-pay and low-proficiency clients. Be that as it may, simultaneous with this advancement, sector players are confronting a developing danger from digital hoodlums trying to assault their frameworks and purchasers. On the off chance that the area is to keep assembling and keeping up shoppers' trust and trust in financial frameworks, it needs to construct its safeguards and capacity to react and recuperate from expected assaults.

Ensuring the financial sector and getting worldwide advances in financial consideration not just relies upon financial service providers improving the security of their own frameworks, yet additionally requires a framework wide way to deal with security. Governments and suppliers need to team up inside their locales just as with peers all throughout the planet to trade insight and backing each other in battling cyber criminals. players with greater limit should furnish their more fragile friends with help, in light of the fact that doing so will give benefits as far as correspondence and will help defend these players own frameworks and the public's trust in the area.

Likewise, banters on digital and information security in the financial sector should be joined by and inserted in conversations on information assurance and the dependable utilization of individual information. Information insurance arrangements and guidelines can't be effective except if the data frameworks and the information they contain are gotten against unapproved access and abuse. Service structures need to require the financial sector to carry out sufficient data and information security principles that guarantee the dependable arrangement of the area's items and administrations, safe preparing of information by its frameworks and mindful utilization of individual information. Given that the improvement local area is advancing financial consideration through computerized and distant financial help arrangements, it's anything but a duty to help the area to oversee digital dangers. As fair entertainers, worldwide associations and improvement accomplices can work with public-private exchange, support powerful approach change cycles and help construct support structures that empower the area to stay aware of the quickly developing danger scene.

❑❑❑

16

Role of Cyber Security in the Global Context

Dr.Jyoti Karve
Assistant Professor,
Rayat Shikshan Sanstha's S.M. Joshi Arts,
Science and Commerce College, Pune

****

ABSTRACT

Cybersecurity is a global phenomenon representing a complex socio-technical challenge for governments, but requiring the involvement of individuals. Although cybersecurity is one of the most important challenges faced by governments today, the visibility and public awareness remains limited. Almost everybody has heard of cybersecurity, however, the urgency and behavior of persons do not reflect high level of awareness. The Internet is all too often considered as a safe environment for sharing information, transactions and controlling the physical world. Yet, cyberwars are already ongoing, and there is an urgent need to be better prepared. The inability to frame cybersecurity has resulted in a failure to develop suitable policies. In this paper, we discuss the challenges in framing policy on cybersecurity and offer strategies for better communicating cybersecurity. Communicating cybersecurity is confronted with paradoxes, which has resulted in society not taking appropriate measures to deal with the threats. The limited visibility, socio-technological complexity, ambiguous impact and the contested nature of fighting cybersecurity complicates policy-making. Framing using utopian or dystopian views might be counterproductive and result in neglecting evidence. Instead, we present evidence-based framing strategies which can help to increase societal and political awareness of cybersecurity and put the issues in perspective.

Keywords: Cybersecurity, information security, cyberphysical system, cyberphysical society,-cyber war, Internet of Things, framing, communication, evidence-based policymaking.

Introduction:

Although most people seem to consider the Internet to be a safe environment and use it on a daily basis using their smart phones, tablets and computers, there are a large number of attacks on a daily basis. Cyberattacks, hacks and security breaches on the Internet are no longer an exception anymore (Arora, Nandkumar, &Telang, 2006). This number is increasing and organizations are incurring higher costs in dealing with these cybersecurity incidents. Although most cyberattacks are harmless, the impact of some is severe. Cybersecurity breaches can range from no or limited impact to Distributed Denial of Services (DDoS), the stealing of data, manipulation of data, identity theft or even taking over control of systems and harm the physical world.

With the adoption the Internet of Things (IoT) in daily life, an increasing number of physical objects feature an IP (Internet Protocol) address for internet connectivity and use the Internet for communication (Hernández-Ramos, Jara, Marýn, &Skarmeta, 2013). Information and communication systems and the physical infrastructure have become intertwined, as information technologies are further integrated into devices and networks. In these cyberphysical systems, the greatest impact occurs when an intruder gains access to the supervisory control access and launches control actions that may cause catastrophic damage. ICT results in a cyberphysical society in which everyday life is interwoven with electronic devices. As such, our living society is becoming ever more dependent on cyberspace, a place in which cyberattacks and cyberwars are common. This might occur high risks, as hackers could take-over medical equipment, automatic-driving cars and flight control, which might be even life threatening.

1. Create Awareness:

The need for cybersecurity is becoming increasingly important due to our dependence on Information and Communication Technology (ICT) across all aspects of our cyberphysical society. Cybersecurity is essential for individuals, for public and non-public organizations, but guaranteeing security often proves to be difficult. The websites of many governments have limited security (Zhao, Zhao, & Zhao, 2010) and might be easily hacked. The issue of security is not limited to the executive power, but is also relevant to political parties, energy infrastructure providers, water boards, road management, ministries, administrative organizations, NGOs and even sporting organizations (such as the International Olympics Committee), all of which have already been the target of breaches and the stealing of information. The hack on World Anti-Doping Agency (WAPA) released the medical record of Olympic athletes to compromise them, whereas the Stuxnet virus was aimed at harming a nuclear infrastructure. Cybersecurity breaches can thus be said to impact all stakeholders in our society.

Interest in cybersecurity issues often focuses on incidents and how to deal with them after the fact, while a concern for prevention and investments in better cybersecurity have lagged behind. This is surprising in a world where there is a continuing battle between hackers and various societal actors attempting to protect the system. Cybersecurity is said to be the new form of war and is viewed as the next platform in modern warfare. Given its importance, why is there so little awareness? and why are we not taking drastic measures to ensure the safety and security of cyberspace?

People have the tendency to select only those parts of a message that they want to hear. One reason is that decision-makers and policymakers, like all people, will react differently depending on objectively equivalent descriptions of the same problem (Levin, Schneider, & Gaeth, 1998). Communication about cybersecurity issues and the urgent need for policies is a difficult endeavor and cannot be easily communicated in a clear and convincing manner. All too often, people point to cybersecurity risk as a means to futurism threats to the polity – to create a security imaginary, a fictionalization that might create a climate of fear (Doty, 2015). Furthermore, the way humans and technology interact, blurs and dissolves the concepts of being 'inside' or 'outside' a cybersecurity space (Leuprecht, Skillicorn, &Tait, 2016). Cybersecurity has been the domain of specialists and experts who are not trained to communicate about the issues. As such, there is a need for message framing, which is strategy for communicating a complex societal problem in such a way that the main arguments are clearly understandable and cannot be easily challenged (De Bruijn, 2017). Although the use of message framing and the need to frame cybersecurity is evident, there is no detailed analysis available.

In this work, we investigate why cybersecurity is not receiving the attention it deserves and how an awareness of the importance of cybersecurity can be created. We start by identifying paradoxes complicating the framing of cybersecurity policies. This is followed by discussing the difficulty of communicating about cybersecurity issues, which has resulted in society not taking appropriate measures to deal with the threats. The challenges are divided into four areas of concern: 1) limited visibility, 2) socio-technological complexity 3) ambiguous impact, related to the strong incentives of market parties to hide the impact, and 4) the contested nature of fighting cybersecurity, for example, measures might need to be taken that violate public values such as privacy. After discussing these issues, we present the need for messages framing, followed by the theoretical background. Finally, we present several frames to deal with these challenges, and call for more research in this emerging area.

2. Cybersecurity: a sea of paradoxes:

Policymaking in the field of cybersecurity is currently facing many paradoxes. The choosing of one direction can be at the expense of another direction, whereas there are arguments for going both ways. Cybersecurity politics and policymaking takes place within a complex ecosystems in which stakeholders from a diverse society, the policy field and government must interact with each other. Responsibilities are distributed over many public entities at both the central and local levels, with diverse problems and challenges, making it difficult to initiate collective action. Society consists of diverse players that might want security, but have varied expectations about the role of government in ensuring safety and security in cyberspace. Governments can play minor or major roles in cybersecurity. Politicians must act upon societal needs, develop policies and allocate resources, while the public institutions need to realize the goals set. This might look like a simple relationship, but the situation is much more complex and subtle, as the roles of stakeholders often conflict and are paradoxical.

One such paradox is that governments want to ensure cybersecurity, but at the same they want access to the data of individuals and organizations for surveillance purposes. The whole discussion of 'backdoor' access to data reveals the paradox encountered by governments. On the one hand, governments want companies and citizens to protect themselves, but on the other hand, they do not want them to use encryption and other cybersecurity measures, as this might allow terrorists and criminals to hide their traces. Governments thus often attempt to balance good and evil by allowing encryption, but requiring backdoors to remotely access the encrypted devices. Such backdoors can also be exploited by others and merely shift cybersecurity threats from the front door elsewhere. Although it might have its merits, it also further complicates cybersecurity – in particular, its visibility.

Cybersecurity breaches cannot be stopped at a nation's borders. In fact, it is difficult to determine where the actual borders are in cyberspace. Where do governments stop? When are they acting within another nation's territory? What happens when there are attacks from another territory and that country denies involvement? Can one country expect another country to take measures against them? Or can one retaliate on servers located outside one's own country? With borders being hard to define and secure, cybersecurity can become a supranational issue, and perhaps is so by its very nature. The differences between countries can be subtle, as the USA and EU are on the same page with the general direction, but foster different values. Often these are founded in the path dependencies influenced by the history of nations. The 9/11 terror attack had a large influence on the USA cybersecurity policy, whereas the Germany constitution, created after the second World War, ensures the privacy to avoid spying of citizens. The paradox is that to address cybersecurity threat, countries need to collaborate; however, they do not trust each other, as their respective activities and intentions might only be partly visible or do not agree on shared values. Collaboration and conflict are intertwined with each other like espionage and war.

Who are the villains? Hackers range from teenagers, freedom fighters, disgruntled employees, to criminal enterprises or state-sponsored endeavors. The motives of attackers are diverse and not always clear. They might include impressing others, gaining prestige and a reputation, jealousy, revenge, profit-making, political agenda or espionage. Moreover, who attacks what is not clear, as attacks cannot easily be traced to the hackers or their motives. Attackers might even be insiders; or outsiders might be helped non-intentionally by insiders through unsafe behavior. Often these activities are masked by normal activities and it is only after damage has occurred that organizations become aware of what was happening. The paradox is that although the impact might be visible, he the attacks and the enemies are hard to determine.

Requirements stipulated by governments might result in significant burdens and costs for companies. Often it is assumed that companies will ensure safety and security for their clients on the internet; however, many companies still ask themselves whether investment in cybersecurity will provide returns in comparison to the cost of a data breach. Data breach costs are associated with resolving the matter, as organizations compensate their clients, pay fines and court fees, invest in forensic and investigation processes, and take counter and preventive measures. Complete protection is never possible and cybersecurity comes at a price.

The reputation of companies and other organizations plays a major role in retaining the trust of clients. Companies do not want to be associated with cybersecurity hacks or viewed as having not taken appropriate security measures. How much do companies spend on cybersecurity? Companies might be reluctant to share information on their cybersecurity spending with the public. The paradox is that too little spending might indicate that they are not well protected, while too much spending might send the message that they are overly concerned – that they might be the potential target of hackers, or simply wasting money. In relation to cybersecurity, it is impossible to take a one-size-fits-all approach to a 'company'. Organizations are diverse and have different demands, a bank and a hospital demand higher levels of security than a restaurant. Moreover, a company's level of knowledge, expertise, experience, their systems, their vulnerability, and the possible impact of a cybersecurity breach are all different. This makes it difficult to talk about companies in general and what is expected from them in cyberspace. How can their security be regulated by governments?

Society is heterogeneous, and as cybersecurity attacks are often not visible, people might not even be aware of them, apart from reports in the media. In addition, most people might not suffer directly from a cyberattack. Banks, credit card companies and shops might take the risks themselves and in this way protect society. The paradox is that while organizations do not benefit from making the problems and attacks visible, this visibility is necessary to create a greater sense of urgency and initiate action.

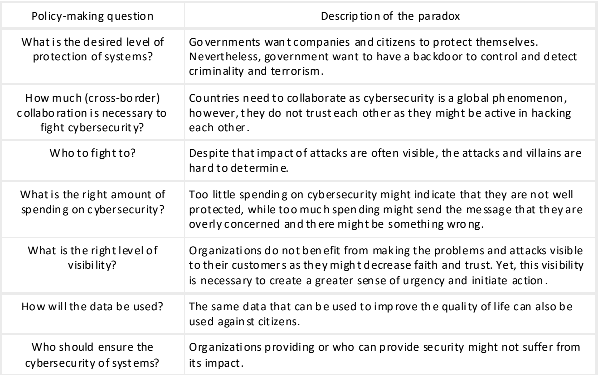
For citizens, the interconnectivity and data generated by devices has resulted in 'an unprecedented improvement in the quality of life' (Elmaghraby&Losavio, 2014, p. 491). At the same time, the vast amount of data available about citizens' location, activities and even emotions, is giving rise to cybersecurity and privacy challenges. The paradox here is that the same data that can be used to improve the quality of life can also be used against citizens. Data-sharing introduces a vulnerability that can be exploited by hackers. Stolen data might be used to blackmail someone, the public availability of health data of an individual might result in difficulties obtaining a mortgage or having to pay higher insurance premiums. Moreover, potential targets might be selected based on the data accessed; for example, sending fake messages with instructions for payment into a bank account based on buying behavior; or phishing, resulting in the installation of malware, which takes control of a system/computer, such that the user cannot access the system unless they pay a ransom (in Bitcoins to avoid traceability). Cybersecurity is a necessity and the question is even if systems connected to the Internet should be even sold without ongoing cybersecurity protection. Why de governments not require the proper protection of systems that are sold by law? Companies and citizens who have spent money on cybersecurity and have monitoring software, firewalls, secure authentication, for example, might also still ask whether their security is working. Would they have been hacked if they had not taken precautions? Is there any return on the investment? You only really understand the importance of security when you do not have it and something happens. Responsibilities are not clear and fragmented among stakeholders. The paradox is that those who can or should provide security might not suffer from the consequences, and can avoid the taking of responsibility. This results in limited urgency to act and no direct need to invest to protect the cyberphysical society.

Despite the risks, people are often not worried about cybersecurity. They have often not experienced any impact and are not interested. Cybersecurity is like infrastructure – you take it for granted and only realize its importance when you experience a problem, but then it is too late. Cybersecurity can also be viewed as a quasi-public good (common good) that nobody owns but everybody is involved in and can be affected. This makes it difficult to pinpoint who should be responsible in taking action and ensuring safety and security.

Who is to blame for all these threats? Are the companies who provide potentially vulnerable software responsible for damages? Are companies that trade without having high levels of cybersecurity in place acting responsibly? Or should we blame individual staff who were aware that their actions might be harmful, or individual citizens who did not sufficiently protect their systems? Or is a government that does not provide appropriate security to its constituents ultimately responsible?

Paradoxes complicate the communication and framing of cybersecurity as the other end of the contradiction can be used as a counterargument. An overview of the paradoxes and underlying policy questions is presented in Table 1. Raising political awareness in such a sea of paradoxes is not easy. Politicians must demonstrate to their constituencies that they are in control, but if nothing happens, public interest and the sense of urgency in relation to cybersecurity will decrease. Politicians would like to ensure the issues remain visible to citizens, but this is difficult. Often cybersecurity is viewed primarily as a technical challenge: as long as it is organized properly and an appropriate budget is allocated nothing else needs to be done. In practice, the issues are not so straightforward, there are no clear responsibilities, boundaries are difficult to define, and the required level of security is also difficult to determine. In addition, the types of measures needed and the level of risk taken are unclear, as is the question of who needs to be protected. Last but not least, people may not be aware that their behavior could be harmful or that they could become under attack.

Table 1. Overview of policy-making paradoxes:



Policy-making question	Description of the paradox
What is the desired level of protection of systems?	Governments want companies and citizens to protect themselves. Nevertheless, government want to have a backdoor to control and detect criminality and terrorism.
How much (cross-border) collaboration is necessary to fight cybersecurity?	Countries need to collaborate as cybersecurity is a global phenomenon, however, they do not trust each other as they might be active in hacking each other.
Who to fight to?	Despite that impact of attacks are often visible, the attacks and villains are hard to determine.
What is the right amount of spending on cybersecurity?	Too little spending on cybersecurity might indicate that they are not well protected, while too much spending might send the message that they are overly concerned and there might be something wrong.
What is the right level of visibility?	Organizations do not benefit from making the problems and attacks visible to their customers as they might decrease faith and trust. Yet, this visibility is necessary to create a greater sense of urgency and initiate action.
How will the data be used?	The same data that can be used to improve the quality of life can also be used against citizens.
Who should ensure the cybersecurity of systems?	Organizations providing or who can provide security might not suffer from its impact.

3. Why is cybersecurity policymaking so challenging?

The overview of stakeholders, their various roles, attitudes and behavior has demonstrated the many paradoxes involved in a complex ecosystem in a cyber physical society. Ignorance, a limited understanding of what needs to be done, limited awareness of the issue despite its significance and urgency, have resulted in a lack of action, planning and policies. What makes communication in this area so challenging? Below, we discuss four reasons why it is difficult for policymakers.

3.1. Intangible nature

When people feel pain they become aware that something is not right. In the same way, often the public only becomes aware of a problem after they experience its impact. The impact of cybersecurity breaches is often not visible in a physical sense, or the precise consequences might not be tangible at all; for example, in the recent US elections, it appears that the Democratic Party was hacked, but the real effect remains unclear (Lipton, Sanger, & Shane, 2016). Moreover, there might be an impact, but not one that is visible, as in the case when financial institutions are required to compensate the victims of online fraud. These financial institutions do not benefit from making these breaches visible, as it might undermine trust in their operation. Consequently, the impact remains largely invisible and intangible to those not directly affected.

Cybersecurity is thus largely invisible to the public. There are no cameras capturing images of military vehicles and combatants, as occurs in regular wars. How can cybersecurity breaches be visualized? Often experts investigate traces of attacks and visualize them on a map, which reveals what is going on and the instruments employed by hackers. What do those maps show? Collecting 'hard' evidence is difficult, and uncertainty remains about the possible victims, the location of the hackers and their motives.

Cybersecurity is often not easy to explain, as there are many aspects. Hackers have the ability to move from one server to another to cover their path and origins. Without extensive effort it is often difficult to find those who carried out an attack. Moreover, even if the initiating computer can be found, this does not mean that the owner carried out the attack. Hackers and security specialists are in a continuous battle to outsmart each other, while politicians must depend on their intelligence agencies and deal with the uncertainties of their analyses.

3.2. Socio-technical dependence:

Cybersecurity concerns both humans and systems, but the complexity of this interaction goes beyond the understanding of most people. Deep knowledge of cybersecurity, of IT infrastructure and the types of attacks that are possible are necessary to understand what is going on. However, it is not merely technology that plays a role. It has often been stated that humans are the weakest link in the cybersecurity chain. Humans play a role in maintaining and updating systems to ensure that the newest defenses are in place, that attacks are detected immediately, and countermeasures can be taken. This also requires policies to be in place and that people understand what is required, as we know that unawareness on the part of users can introduce further vulnerabilities; for example, by using weak passwords, installing untrustworthy software and using insecure devices and applications.

The socio-technical nature of cybersecurity thus complicates the process of finding solutions. In contrast to global warming and climate change, where a polluting energy plant can be replaced by a low carbon emissions plant, there are no straightforward solutions in the field of cybersecurity. People want to be safe and secure, but may not want – or simply do not have the money – to take action. The public expects that the government will take responsibility, but the measures implemented by governments might not be sufficient if individuals do not also take some responsibility.

3.3. Ambiguous impact

It is difficult to judge cybersecurity risks in advance. What impact will there be if data is stolen or altered? Often no physical systems are damaged or money stolen, although there are exceptions, such as the Stuxnet virus in Iran, in which centrifuges were damaged (Langner, 2011).

Most people perceive possible risks as remote. Who the hackers will target next is not known, and organizations and individuals tend to think that they will not be the target of an attack – it might happen to my neighbor or another company, but it will not happen to me. Moreover, when it does happen to someone else, others often think it was their own fault, and that they probably failed to take necessary security measures. This is a fallacy, as despite all their good intentions and countermeasures, there is always the potential that an organization will suffer a cybersecurity attack.

Furthermore, if most people fail to acknowledge that cybersecurity is a problem, the tendency will be to ignore it and fail to take appropriate action. The lack of a sense of urgency in many people results in no common action.

Cybersecurity entails a continuous battle, with both the attackers and those who are protecting us against them remaining constantly on the move. The impact of new attacks and technologies is unclear, as are the defense requirements. What resources are required to fight the unknown? Cybersecurity is never completely guaranteed, which makes it difficult to demonstrate the successes and call for investment. What is the return on investment in cybersecurity measures? This is further complicated, as despite all the best efforts there might always be a risk of cybersecurity violations, and this is a difficult message to convey. Whatever you do, might not be sufficient.

3.4. Contested nature of fighting cybersecurity:

Once the urgent need for cybersecurity has been established, a discussion about the measures that need to be taken is required. Organizations are often uncertain about the measures that need to be taken to improve security. Attackers are often anonymous and it is unclear who the enemy is.

Everybody can be a potential enemy. Even friendly servers or the computers of employees might be hacked and become a threat. To fight cybersecurity, network traffic needs to be monitored, but the human behavior of both friends and enemies can also be tracked. In other words, monitoring comes at the expense of the privacy of individuals. Ensuring cybersecurity thus comes at the cost of other public values, and these measures are contested.

Some argue that cybersecurity is not always for the good. Discussion about the NSA is dominated by privacy issues and its ability to act without oversight from elected politicians or any institutional accountability. The development of surveillance programmers should strike a better balance between security and privacy (Reddick, Chatfield, & Jaramillo, 2015). Moreover, the wording used to frame a problem can have effects, from mobilizing resistance to greater attention being paid to the issue (De Bruijn, 2014).

There is an acknowledged tension between national security and civil rights (Gorham-Oscilowski& Jaeger, 2008), with citizens contesting NSA surveillance programmes and their needs. These findings suggest that governments need to be more efficacious and more transparent in communicating about surveillance programmes if they are to gain greater approval for such programmes (Reddick et al., 2015).

In summary, there is growing concern about the ways in which our lives are increasingly regulated and controlled, whether in relation to ordinary objects or technology (Woolgar & Neyland, 2013). Can the privacy of employees and citizens be sacrificed for the sake of cybersecurity? Do the advantages outweigh the disadvantages?

4. Why do we need framing?:

The challenges discussed in the previous section mean that politicians and policymakers face a difficult task. How do we fight an unknown enemy or someone who denies responsibility in a situation where it is hard to prove that they are the culprit? Also researchers are challenged to frame the outcome of their research in a concise way without Message framing is aimed at communicating a complex problem in a simple and convincing manner.

Cybersecurity specialists often attempt to use message framing, but often fail to get the right message across. They use management guru techniques and manipulate common cognitive vulnerabilities in order to over-dramatize and over-simplify cybersecurity risks (Quigley, Burns, &Stallard, 2015). This does not result in the attention desired: critical systems remain unprotected and behavior does not change or cybersecurity protection is delegated to software and hardware providers including automatic update measures, resulting in people feel cyber-secure and stop paying attention. Instead, the public might recognize the over-dramatization or consider the issue too difficult to deal with, resulting in inertia. Why do these frames not work? One reason is that there is no clear victim and no visible enemy. While the identification of a hero and a villain is commonly used in framing to create a convincing message (De Bruijn, 2017), framing cybersecurity in this way does not result in the desired attention and sense of urgency.

Cybersecurity can be perceived as a problem of the individual or as a problem of society. Presenting it as a collective problem to be tackled by society is difficult for politicians and policymakers, as they do not have much to gain by addressing this topic, the effects of which are largely invisible to the public. All politicians agree that cybersecurity is important and view it as a technological issue that needs to be resolved. Generally speaking, it is a bipartisan issue that they cannot use to differentiate themselves from their political opponents. Nevertheless, the four challenges mentioned above demonstrate that cybersecurity is more than merely a technological problem and that political values are involved.

The problem contexts that define and shape practice are considerably more complex than can be easily explained and captured in a simple frame. Framing requires comprehensive analysis and deep understanding of the context (see Janowski, 2015). This complexity, the uncertainties and multifaceted challenges in cybersecurity means it is difficult to create a simple frame.

5. What is message framing?

Message framing is a strategy for communicating a complex problem in such a way that the main arguments are understood and cannot be easily challenged (De Bruijn, 2017). The characteristics of the source of information as well as of the recipient may influence both the direct and indirect effects (De Vries, 2017). The effect of message framing on decision-making and persuasion has been well researched (Smith & Petty, 1996). One approach that has been used to understand the effects of framing is known as 'prospect theory' (Kahneman & Tversky, 1979). This theory states that people evaluate information in terms of either potential gains (positive framing) or potential losses (negative framing). Preferences can be altered by changing the way information is presented. How people's attitudes and behavior are affected by message framing is dependent on the processing and traits of the receiving party. For example, Maheswaran and Meyers-Levy (1990) found that positively framed messages are more persuasive when the receiver does not read the message in detail, whereas negatively framed messages are more persuasive when detailed processing is emphasized. Furthermore, the context in which a message is framed also determines its effectiveness (Rothman &Salovey, 1997). De Vries, Terwel, and Ellemers (2014) use experiments to show that adding irrelevant information dilutes the impact of highly relevant information.

Message framing requires reducing the complexity to clear and easy to explain messages. As we have seen, cybersecurity is a complex socio-technical phenomenon involving many facets. Attempting to communicate this complexity results in an incomprehensible and unclear story that takes too long to communicate. The essence of message framing is to develop a relatively simple framing of a complex reality: the complexity has to be reduced to a relatively simple message capturing the essence. The reduction of complexity is by definition a debatable solution, as relevant issues might be omitted (De Bruijn, 2017).

Typically, framing positively and negatively results in valence framing effects (Kahneman & Tversky, 1979). This is called the risky choice framework, which reveals the consequences of action or inaction (Levin et al., 1998). In such a strategy, both utopian and dystopian views are presented, creating the desire for action by showing what will happen if no action is taken (dystopian view) or what the result of taking action might be (utopian view). In these frames, people are more likely to take risks when attention is focused on the opportunity to avoid losses than when the focus is on the opportunity to realize gains (Kahneman and Tversky, 1979, Levin et al., 1998): the 'typical pattern is a choice reversal or a choice shift in the direction of less willingness to take a risk when the choices are framed positively than when choices are framed negatively' (Levin et al., 1998, p. 153). Levin et al. (1998) identified three types of frames:

1. The standard risky choice framing – which influences the valences in terms of willingness to take a risk.

2. Attribute framing – which affects the evaluation of object or event characteristics.

3. Goal framing – which influences the persuasiveness of a communication.

Embracing an utopian view can result in the a boomerang effect (De Vries, 2017). De

Vries demonstrates in which positively framed communication about low-carbon technologies result in the perception of being manipulated and may actually lead to opposition in the long run.

De Bruijn (2017) used the Victim-Villain-Hero (VVH) model to understand framing, identifying five criteria of successful frames:

- Frames are catchy
- We intuitively agree with frames
- Frames contain a villain
- Frames challenge your opponent's core values
- Frames tap into social undercurrents

All these approaches remain at a relatively theoretical level and provide limited guidance on how to frame an actual situation. Therefore, we will derive some more specific framing strategies below. While framing is about conveying the message, evidence-based policymaking is about ensuring that it is factual and appropriate data is collected. We argue that although one could view these as conflicting, they should be viewed as complementary. The same evidence can be framed in a different way, resulting in valence framing effects.

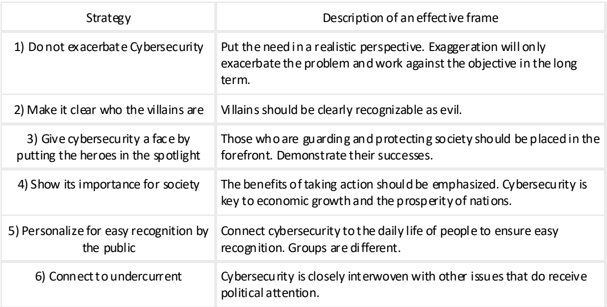
Cybersecurity policy-makers, specialist and scientist are often criticized for not being able to explain their message to the public. Although they have the evidence, they are not always able to convey the message to the public and convince politicians and policymakers to take action. A typical example is environmental science, with scientists unable to convince policymakers of the urgency to reduce carbon emissions (De Vries et al., 2014). What is required to address this failure is evidence-based message framing.

6. Evidence-based message framing strategies:

The concept of 'evidence-based framing' has two implications. First, it means that frames should be based upon facts. Messages that are, for example, purely emotional will not live long, as they are subject to public scrutiny. People will find out that the message is not correct and will start distrusting the messenger. Regaining trust once it is lost takes much more effort or might even be impossible. Messages should thus be grounded in evidence that is collected in such a way that it can be trusted. Second, facts need good frames. Climate scientists have been criticized for not effectively explaining their message to the public – they were unable to frame their message properly (Crompton, 2010). Therefore, there is a need for evidence-based message framing.

In this section, we propose a series of strategies which frame cybersecurity in such a way that more societal and political awareness will be generated. We base our strategies on both the more generic literature on framing, and on empirical research on framing in the specific area of global warming. Table 2 provides an overview of the strategies.

Table 2. Summary of framing strategies:



Strategy	Description of an effective frame
1) Do not exacerbate Cybersecurity	Put the need in a realistic perspective. Exaggeration will only exacerbate the problem and work against the objective in the long term.
2) Make it clear who the villains are	Villains should be clearly recognizable as evil.
3) Give cybersecurity a face by putting the heroes in the spotlight	Those who are guarding and protecting society should be placed in the forefront. Demonstrate their successes.
4) Show its importance for society	The benefits of taking action should be emphasized. Cybersecurity is key to economic growth and the prosperity of nations.
5) Personalize for easy recognition by the public	Connect cybersecurity to the daily life of people to ensure easy recognition. Groups are different.
6) Connect to undercurrent	Cybersecurity is closely interwoven with other issues that do receive political attention.

6.1. Do not exacerbate Cybersecurity

There is a dystopian view of cybersecurity, in which cybercrime is seen as a potential threat everywhere: when you pay for something using a card; when you change the temperature in your living room; when you are driving or walking along the street (cameras are watching you). Some argue that cybercrime will have a devastating impact on our lives: there will be no more privacy, and a big brother society will emerge. In such a society, you will never be safe and the risks will be immense.

The problem with this dystopian way of framing cybersecurity can be summarized in the well-known one-liner: 'Hell does not sell'. This is a lesson learned from discourse on the issue of global warming. Over-dramatizing the impact of global warming ('catastrophic', 'fast', 'irreversible') results in a mixture of denial, apathy and fatalism (O'Neill & Nicholson-Cole, 2009). It also feeds the idea that we are out of control – that the problem can no longer be resolved. The same risk applies in relation to cybersecurity. What impact does the message that you are never safe and the risks are immense actually have on people? Instead of creating a sense of urgency, it might result in denial.

There is another lesson we can learn from the debate about global warming. Once people are in a mood of denial and apathy, they become very receptive to the message that human-made global warming simply does not exist – that it is a hoax. The same could happen in relation to cybersecurity if the risks are overdramatized. For example, billions were spent on the millennium bug, but nothing disastrous happened. The argument might be made that the threat is not as bad as advocated by the experts.

6.2. Make it clear who the villains are:

The problem with framing cybersecurity is that there are often no clear villains: the villains may not visible; the victims may also be villains; the victims might have an interest in not being explicit about the villain; or the presumed villain might be perceived as a hero – as might be the case with hackers. The activist group "Anonymous" might be viewed as a villain or as a hero, dependent on your point of view. The DDoS attack to the Canadian government websites in 2015 after passing the terrorist bill can be viewed as trying to safe privacy of people, but also as an act of terrorism.

The absence of a clear villain makes it harder to frame cybersecurity in an effective way. The implication of this observation is clear: give the villain a face. Provide clear examples of unambiguous villains – cyber gangs that are, without doubt, perpetrating extreme acts. Be explicit about their strategies – how they can ruin the lives of their victims. These villains will of course not represent the whole family of unambiguous and ambiguous villains, but this is not the issue. The issue is that without a clear and unambiguous villain, framing cybersecurity will remain problematic. If there is a clear villain, there will be obvious victims. This helps people to more easily identify with the fight against cybercrime.

Thus, villains need to be clearly recognizable. Such a villain could be a country with already have been the villain in other areas or Nigerians who are notorious for their scam emails. However, only cast unambiguous cybercriminals as the villains. Casting a young hacker as the villain may result in 'sympathy for the enemy' and have an inverse effect.

6.3. Give the fight against cybersecurity a face: put the heroes in the spotlight:

Giving villains a face is important – but the same goes for the heroes. The heroes are those who are protecting us, those whose expertise and dedication we rely on. For most people, our cybersecurity heroes do not have a face. Who are they? Is it possible to meet them? Most people have no clue about the people who are protecting us: Are there special departments of smart people located in basements, or computer nerds sitting in attics? Heroes might be hard to find, and heroes might not look heroic at all.

By making these dedicated people working on our safety and security visible, we gain a better understanding of who is guarding and protecting society. This is a framing strategy that is sometimes used in relation to large infrastructure projects that have the potential to harm the interests of residents or other stakeholders; for example, because they take a lot of time. Giving the people who work on a project a face, a hard working person with a helmet. Reveal the complexity of their work and making explicit the high level of their professionalism might be conducive to a respect for their knowledge and acceptance of their work by others. By giving the 'cyber heroes' a face and revealing what they do, it becomes clear that they are undertaking extremely complex work to keep our systems secure. Select a smart young guy with a degree or a renowned university and make the person visible in the news and at late night shows. They might be the smartest in their class and come from all over the world. If we recognize their expertise and experience, we gain confidence that they are doing a good job. By bringing them to the forefront people can recognize their work and see how their work is done. The public can identify themselves with the 'heroes' and their work and thus with the fight against cybercrime. This can all be further strengthened by also demonstrating the successes of their work: often only failures make the news, while the successes remain invisible.

6.4. Connect cybersecurity to values other than security alone:

In relation to environmental policy in general and global warming in particular, connecting to other values is a well-known framing strategy (De Bruijn, 2017). In order to convince right-wing opponents of the need for environmental policies, for example, these policies are linked to right-wing values, such as strengthening the economy and entrepreneurship. It is argued, for example, that investing in sustainability is good for the economy, will bring jobs and innovation. The idea is that linking a policy to other people's values might make them more receptive to this policy (De Bruijn, 2017).

The same strategy could be applied to the framing of cybersecurity. Investing in cybersecurity could bring economic benefits – not so much because there will be fewer costs of crime, but because countries investing in fighting cybercrime will build up expertise that is of high value. This might strengthen the IT industry, it might make a country a key player in the cybersecurity domain, with the nation becoming an international frontrunner, resulting in the creation of new jobs and the exporting of knowledge. Cybersecurity need not be framed solely as a task of solving problems, but also as creating economic opportunities – which might make it attractive to invest in expertise in cybercrime.

6.5. Personalize for easy recognition:

Society is not homogenous and people have different interests and levels of knowledge and experience. It is crucial to understand that there are multiple audiences (individuals, businesses, nations, societies) which require different messages. Personalization of the message is an important framing strategy, which should ensure that the problem is recognizable in daily life.

If complex and abstract topics such as cybersecurity are made relevant to people's immediate living environment, then they will readily recognize the urgent need to address cybersecurity. For example, companies in high-tech industry will be more receptive to threats of espionage and the risk of their ideas being stolen and used by other organizations, while citizens will better understand the need when faced with the possibility of stolen or blocked credit cards and the risk of losing money. Both groups also require different instruments to ensure their safety in cyberspace.

6.6. Connect to other tangible and clear issues:

Finally, there are always issues that stimulate people much more than cybersecurity, but that are also interwoven with cybersecurity. This is because these other issues are highly visible and have gained some momentum. As such, they can be used to gather support for the fight against cybercrime. The most powerful example is the threat of IS (Islamic State), which can be used to strengthen the argument for cybersecurity. We can emphasize the importance of cybersecurity to deal with the threat of IS, as it relies on the internet to plan terrorist activities: cybersecurity can help in detecting and preventing these. Moreover, their financial resources and plans should be monitored – and we need 'cyber heroes' for that.

Conclusions:

Our society is turning into a cyberphysical society having dependence on Information and Communication Technology (ICT) across all aspects of our daily lives, which makes the need for cybersecurity paramount. The intangible nature of cybersecurity, the socio-technical dependences, the ambiguous impact and contested nature of fighting cybersecurity all make it a challenging area for policymakers. Cybersecurity can be framed in different ways, having different effects on people. Cybersecurity is a complex and multifaceted area which has no clear heroes or villains. The inability to frame cybersecurity has resulted in a failure to take appropriate measures and develop suitable policies. However, there are already ongoing cyberwars, and citizens and governments need to be better prepared. Message framing is a strategy for communicating a complex problem in such a way that the main arguments are understood and cannot be easily challenged. Simple message frames do not work for cybersecurity and therefore evidence-based message framing is necessary. In a similar vein to evidence-based policymaking, messages are framed based on the evidence and use framing strategies. Thinking in terms of framing strategies to communicate a difficult message has profound implications. We argue that it is important to take the evidence as a starting point and avoid utopian and dystopian frames, as these standard messaging strategies might be counterproductive.

Instead, the following six strategies were identified as offering a better way to frame cybersecurity:

1) do not exacerbate cybersecurity,

2) make it clear who the villains are,

3) give cybersecurity a face by putting the heroes in the spotlight,

4) connect cybersecurity to values other than security alone,

5) personalize the message for easy recognition and

6) connect to other tangible and clear issues.

Message framing is not only important or cybersecurity but in many domains of government information. For example, the discussion about privacy, the use of personal files, identify management, Internet governance, public-private systems, and the opening of data are all complex socio-technical areas in which the results of intensive research are not easily to communicate. Cybersecurity specialists and experts, but also researchers and policy-makers, needs to frame their message well to avoid misunderstanding and ambiguity. Capacity building by government and more research about evidence-based framing strategies and its effectiveness is needed.

Acknowledgement:

The authors would like to thank Tomasz Janowski for arranging the reviews and his suggestions.

References:

1. Arora et al., 2006A. Arora, A. Nandkumar, R. Telang Does information security attack frequency increase with vulnerability disclosure? An empirical analysis Information Systems Frontiers, 8 (5) (2006), pp. 350-362 View Record in ScopusGoogle Scholar

2. Crompton, 2010T. Crompton Common cause: The case for working with our cultural values WWF, Oxfam, Friends of the Earth, CPRE, Climate Outreach Information Network (2010)Google Scholar

3. De Bruijn, 2014H. De Bruijn Framing. Over de macht van taal in de politiek Atlas Contact, Amsterdam (2014)Google Scholar

4. De Bruijn, 2017H. De Bruijn The art of framing: How politicians convince us that they

are right Etopia BV (2017)Google Scholar

5. De Vries, 2017G. De Vries How Positive Framing May Fuel Opposition to Low-Carbon Technologies: The Boomerang Model Journal of Language and Social Psychology, 36 (1) (2017), pp. 28-44 View Record in ScopusGoogle Scholar

6. De Vries et al., 2014G. De Vries, B.W. Terwel, N. Ellemers Spare the details, share the relevance: The dilution effect in communications about carbon dioxide capture and storage Journal of Environmental Psychology, 38 (2014), pp. 116-123, 10.1016/j.jenvp.2014.01.003

❑❑❑

17

Cyber Security in E-Commerce

Prof. Mengal Santosh Gangaram
Abasaheb Marathe Arts & New Commerce,
Science College, Rajapur(Vikhare Gothane)
Dist. Ratnagiri (M.S.)

****

Introduction:

E-commerce is new trend in the market. Ecommerce means buying and selling the goods and services, transfer money through internet network. E-commerce providing safe, suitable and immediate payment system for transfer funds to users. Now a day's critical transaction are increased in ecommerce through cybercrime. Cybercrime is internet security threat. Peoples are facing the significant finance and information losses in the transactions. E commerce is growing fast in business technology.

Ecommerce give the opportunities to all business and individual peoples. Small scale business can use the opportunities for convert their business in large scale industries. Due to time bounding and other factors traditional business could not reach up to effectively in sales and profit. They have limitations of time, distance, customer relation and huge shop rents. Majority of organizations spread their business on the web to reach the new markets and earn more profits.

E- Commerce is facing the problem of security threats of cybercrimes. In today's century cyber-crime growing fast in ecommerce through the criminals, who were participate in the process of buy and sell of valuable goods and services. They stole the important financial data through hacking the websites and programs. Skilled cyber criminals mostly attack through malware, and malicious software's, handling control of computers and other some cyber technique. In the future cyber-crimes can commit without knowledge and co-operation of victim. Peoples and business organizations have needed the security from cyber-crime for online transaction. Prevention of cyber-crime in future will require a strong security from cyber threats. The role law is important in security of cyber-crime in online transaction in ecommerce. Most of the technologies are legal and some changes have made in the legal system.

E-Commerce

E- Commerce means a process of purchasing and selling goods and services, transfers the funds and information of transaction through electronic medium like as internet. E –commerce also known as online commerce or e- business. It has been convenient and easy to use for peoples. Anyone can search, shop from anywhere and anytime with electronic device connected to internet. E-commerce transaction occurs either as business to business, business to consumer, consumer to business, consumer to consumer. E-commerce is conducted a variety of applications such as email, shopping carts, web series, File transfer protocol and online catalogue. etc..

Security Threats on E-Commerce

1. Phising –

Phising is popular cyber-crime in ecommerce. Attacker send fake emails to peoples and collect the personal information like as some ID numbers, PAN numbers, bank account details, social security details and other information. Attackers stole the identity and use social engineering to cyber-crime activities. They can also sold the information to the third party for cyber-crimes and reduce the risk of between the cyber-criminal and user of information about financial data.

2. E- Skimming –

E- skimming is the practice of stole personal information through debit and credit cards. Hackers can enter into shopper's bank account through e skimming. Most of the time hackers can use weak e-commerce websites. They can attract to shoppers to malicious domains where they can capture some skimming codes and important information. Hackers can use or send the skimming codes to other remote server where stolen information gathered and used or sold to third party for cyber-crime.

3. Malware and Ransomware -

The destructive software's are use in cyber-crimes. It is comes in various forms. Comparatively most of malware and ransomwares are established more than authentic software every year. No anyone can download deliberately and permit it for access the data in computer or any electronic device. But it can exit and entered in computers and other electronic device of users. Users can loss their important data due to infected computer system by destructive programme.

Best practices for E-commerce security

1. Use strong, Unique passwords –

Most of the cyber-crimes or cyber-attacks are established due to weak password. Most of time users are create weak or short word passwords but cyber attackers crush the weak password and access the data or cheat the financial transactions. It is additional efforts to e –commerce website administrators and they should coerce to customers, business and individual users for creation for strong passwords at the time of registration on e-commerce platforms. User should use at least 08 characters with lowercase and uppercase word, numbers and symbols for strong password. Same passwords are should not use on other platforms and do not share sensitive information for security question of passwords. User should not share personal user ID and passwords to each other.

2. Protecting Device –

User should must ensure that their device protected with latest updated firewalls, antimalware and other solutions of securing computer system against cyber-attacks.

3. Proof against phishing –

Users or shoppers should avoid the fishing attacks. They should not spread their information up to confirmation of support of customer. Government organizations not ask the password and other personal banking information so they should not click on suspicious emails or links and attachments on their emails. Users should check the authentic website with spelling and grammatical errors also check correct domain name and source of email.

4. Implementing Multifactor Authentication–

Ushers should implement the authentication process in the transaction of e-commerce. They should assure about the persons who access the web site of the organization. It may be burden but it is suitable for preventing the cybercrime in e-commerce.

5. Update website –

Shoppers should update their website always because hackers identify the possible weakness in websites. Shoppers using the SaaS e-commerce websites have not worries about the update of websites because these websites are updated automatically in the specific period. But other websites have need to updates time to time for cyber security purpose.

Conclusion –

E-commerce cyber security is one of important round clock practice which includes peoples, online process of purchasing and buying the goods and services and online payments. It gives flexible and suitable system for online transaction to shoppers and customers. But they are worried due to threat of cyber-crime. Cyber security is important for all digital transaction in e-commerce. Shoppers and user should alert from cyber-crimes such as phising, e-skimming, malware and ransomware. They should implement some ways for cyber security through updating websites, using strong password, avoid fishing, implementing the multifactor authentication etc.

Reference –

1. Lech J. Janczewski, Andrew Colarik, Managerial Guide For Handling Cyber-terrorism and Information Warfare, IGI publishing, Hershey, PA, 2005.

2. Dr. Farooq Ahmed, 'Cyber Law in India (laws on Internet)', Pioneer Books, Delhi U.S. App(1992).

3. Dr. Subhash Chandra Gupta, Information technology Act, and its Drawbacks, National Conference on Cyber laws & legal Education, Dec. 22-24th 2001, NALSAR, University of Law, Print House, Hyderabad(2000).

4. Niranjanamurthy M, Kavyashree N, Mr S.Jagannath "M Commerce: Security Challenges Issues and Recommended Secure Payment Method" - IJMIE Volume 2, Issue 8 ISSN: 2249-0558 -2012.

5. www.ijarcce.com

6. www.google.com.

❑❑❑

18

Novels on Cyber Security: A Brief Analytical Sketch

Smt. Poonam Prakashrao Mane
Asst. Teacher,
Z. P. P. S. Waghalwadi, Tq. Ambajogai,
Dist. Beed, Maharashtra

****

Abstract:

Today, Cyber Security plays an important role in the field of information technology. Securinginformation, securing bank details, securing confidential information, securing various personal details have become most of the biggest challenges facing everyone. When thinking about cyber security, thinking ends with cybercrime, which is increasing immensely day by day. However, 'cyber security' and, 'cybercrime', are very different concepts and relate to different areas of expertise. Cyber security has affected many parts of the current generation. Now it is reflected not only in technology, net banking, hacking information, intelligence gathering, but also inmovies, serials, web series and novels.

Books arereally a great sourceof knowledgethat inspires and develops our thoughts and tell us about today's latest thoughts, problems and solutions. Specially, the novels are our favourite books, where everyone reads curiouslytill the end of the novel. So, thecurrent research paper is trying tofocusmainly onfictional novels based on cyber security, where readers can understand the whole concepts of cyber security througha brief analytical sketch of the novels.

Keywords: Cyber security, cybercrime, hacking, novels, cyber safety, attacks, internet.

Introduction:

Today's life has become more digitalized with rapid technological developments. Business, education, shopping, banking transactions, almost everything is on the cyber platform. Cyber security plays an important role in the development of information technology as well as online internet services. Internet services are able to send and receiveany type of data such as an audio, video, an e-mail, a confidential file and any kind of documentsat the click of a button. But in this process, how will be data secured, without leakage of information, itdepends on cyber security. That is why cyber security has become a latest issue of any nation.The scope of cyber security is not just limited to securing the information in IT section, but also various areas ofhuman awareness. Only technical sources cannot prevent any kind of cybercrime, it requires a comprehensive and secure approach, including law enforcement. Many governments today impose strict laws on cyber securities in order to prevent the loss of all kinds of information. Everyone should also be trained in cyber security and protect themselves from cybercrimes.

Discussion and Analysis:

Cyber security is a broad and complex topic that is becoming more important as the world becomes highly interconnected, with networks being used to conduct critical transactions.With each passing year, cybercrime continues to divert different paths.With new cyber tools and threads coming up every day, the latest and disruptive technologies are challenging organizations to not only secure their infrastructure, but also new platforms and intelligence. There is no one-size-fits-all perfect solution to cyber-crime but we must work at our level best to reduce it so that we can have safe and secure future in cyber space. For that we need to explore our knowledge about it and fictional literature is the only source to understand the cyber-crime and itsworld. There is no need for every situation to be at a loss with us.To save us from these disasters, we can increase our wisdom by reading such a literature like cyber security novels. There are some cyber security novels, which teach us valuable lessons to protect ourselves. This research paper presents a brief analytical descriptionof the cyber-security novels.

Bowden Mark. "Worm: The First Digital War" – The Conficker worm infected its first computer in November 2008 and within a month had infiltrated 1.5 million computers in 195 countries. Bank telecommunications, companies and critical government networks were infected, including the British Parliament and the French and German military. No one had ever seen anything like it. By January 2009 the worm lay hidden in at least eight million computers and the botnet of linked computers that it had created was big enough that an attack might crash the world. Surprisingly, the U.S. government was vaguely aware of the threat that Conficker posed, and the task of mounting resistance fell to disparate but gifted group of geeks, internet entrepreneurs, and computer programmers. They formed what come to be called the Conficker Cabal, and began a tireless fight against the worm. But Conficker controllers became aware that their creation was beginning to encounter resistance, they began refining the worm's code to make it more difficult to trace and more powerful testing the Cabal's unity and resolve. Will the Cabal lock down the worm before it is too late? Game is on still the death is not coming. (Bowden, Worm: The First Digital War)

Coleman Gabriella. "Hacker, Hoaxer, Whistle-blower, Spy: The Many Faces of Anonymous"– Here is the ultimate book on the worldwide movement of hackers, pranksters and activists that operates under the non-name Anonymous. This book is known for all of Anonymous deepest, darkest secrets. Half a dozen years ago, anthropologist Gabriella Colman set out to study the rise of this phenomenon just as some of its members were turning to political protest and dangerous disruption. She ended up becoming so closely connected to Anonymous that the tricky story of her inside-outside status as a non-confident, interpreter and erstwhile mouthpiece forms one of the themes of this witty and entirely engrossing book. The narrative brims with details unearthed from within a notoriously mysterious subculture, whose semi-legendary tricksters-such as Topiary, Tflow, Anachaos and Sabu-emerge as complex, diverse, politically and culturally sophisticated people. Propelled by years of chats and encounters with a multitude of hackers, including imprisoned activist Jeremy Hammond and the double agent who helped put him away, Hector Monsegur, Hacker, Hoaxer, Whistle-blower, Spy is filled with insights into the meaning of digital activism and little understand facets of culture in the internet age, including the history of, "trolling", the ethics and metaphysics of hacking, and the origins and manifold meaning of, "the lulz".(Coleman, Hacker, Hoaxer, Whistle-blower, Spy: The Many Faces of Anonymous)

Goodman Marc.Future Crimes: Inside the Digital Underground and the Battle for Our Connected World – From one of the world's leading authorities on global security, Future Crimes takes readers deep into the digital underground to illuminate the alarming ways criminals, corporations and even countries are using new and emerging technologies against you-and how this makes everyone more vulnerable than you ever thought possible. Technological advances have benefited our world in immeasurable ways, but there is an ominous flip side. Criminals are often the earliest and most innovative, adopters of technology. Today's criminals are stealing identities, draining online bank accounts and wiping out computer servers. This is just the beginning of the tsunami of technological threats coming our way. In Future Crimes, Marc Goodman rips opens his database of hundreds of real cases to give us front-row access to these impending perils. Reading likes a sci-fi thriller, but based in startling fact, Future Crimes raises tough questions about the expanding role of technology in our lives. Future Crimes is a call to action for better security measures worldwide, but most importantly, it will empower readers to protect themselves against looming technological threats- before it's too late. (Goodman, Future Crimes: Inside the Digital Underground and the Battle for Our Connected World)

Kaplan Fred. "Dark Territory: The Secret History of Cyber War" – "An important, disturbing and gripping history", the never-before-told story of the computer scientists and the NSA, Pentagon, and White House policymaker who invent and employ cyber wars –where every country can be a major power player and every hacker a mass destroyer. In June 1983, President Reagan watched the movie War Games, in which a teenager unwittingly hacks the Pentagon, and asked his top general if the scenario was plausible. The general said it was. This set in motion the first presidential directive on computer security. From the 1991 Gulf war to conflicts in Haiti, Serbia, Syria, the former Soviet Republics, Iraq and Iran, where cyber warfare played a significant role, Dark Territory chronicles a little-known past that shines an unsettling light on our future. Fred Kaplan probes the inner corridors of the National Security Agency, the beyond-top-secret cyber units in the Pentagon, the "information warfare" squads of the military services, and the national security debates in the White House to reveal the details of the officers, policymakers, scientists and spies who devised this new form of warfare and who have been planning- and fighting –these war of decades. (Kaplan, Dark Territory: The Secret History of Cyber War)

Mitnik Kevin. "Ghost in the Wires: My Adventures as the World's Most Wanted Hacker" – This novel is based on true story, and about one of the most successful and elusive hackers in the world. For years, Kevin Mitnick penetrated computer networks at some of the world's largest corporations. He seemed unstoppable to law enforcement as they followed three steps behind him. Ultimately, Mitnick wanted to try his hand at some of the hardest security systems. He hacked into Pacific Bell, Motorola and Sun Microsystems. The added attention turned the FBI's attention on Mitnick, and he was forced to go on the run. Armed with fake identities and numerous safe houses, Mitnick stayed on the run until he was forced into a showdown with law enforcement. (Mitnik,Ghost in the Wires: My Adventures as the World's Most Wanted Hacker)

Stoll Clifford. "The Cuckoo's Egg"-In this novel, readers are taken to an earlier time. Before the internet was a tool for terrorists, one United States citizen saw the potential for the computers to be used for secret service. Compiling the evidence, he seeks to expose the online spies that threaten national security. While the main character knows what is going on, the question he is faced with is if the authorities will back him up. This tale read like a Sherlock Holmes novel. It is based on the real story of Clifford Stoll. Previously an astronomer, Stoll become a system manager and discover single accounting errors that led him to discover a mysterious invader on the network. Before long, Stoll begins to spy on the spy as his campaign captures the attention of the CIA. (Stoll, The Cuckoo's Egg)

Zegart Amy & Herbert Lin. "Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations" – "We are dropping cyber bombs. We have never done that before". –U.S. Defence Department official. A new era of war fighting is emerging for the U.S. military. Hi-tech weapons have given way to hi tech in a number of instances recently: A computer virus is unleashed that destroy centrifuges in Iran, slowing that country's attempt to build a nuclear weapon. ISIS, which has the made the internet the backbones of its terror operation, finds its network based command and control systems overwhelmed in a cyber-attack. A number of

North Korean ballistic missiles fail on launch, reportedly because their systems were compromised by a cyber-campaign. Offensive cyber operations like these have become important components of U.S. defence strategy and their role will grow larger. But just what offensive cyber weapons are and how they could be used remains clouded by security. This new volume by Amy Zegart and Herb Lin is a ground breaking discussion and exploration of cyber weapons with a focus on their strategic dimensions. It brings together many of the leading specialists in the field to provide new and incisive analysis of what former CIA director Michael Hayden has called 'digital combat power' and how the United States should incorporate that power into its national security strategy. (Zegart,Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations)

Zetter Kim. "Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon" – A top cyber security journalist tells the story behind the virus that sabotaged Iran's nuclear efforts and shows how its existence has ushered in a new age of warfare – one in which the digital attack can have the same destructive capability as a megaton bomb. The virus now known as Stuxnet was unlike any other piece of malware built before: Rather than simply hijacking targeted computers or stealing information from them, it proved that a piece of code could escape the digital realm and wreak actual, physical destruction, in this case, on an Iranian nuclear facility. Now journalist tells the whole story behind the world's first cyber weapon, covering its genesis in the corridors of the White House and its effect in Iran. And telling about Countdown to Zero Day also ranges beyond Stuxnet itself, exploring the history of cyber warfare and its future, showing us what might be happen should our infrastructure be targeted by a Stuxnet –style attack, and ultimately, providing a portrait of a world at the edge of a new kind of war. (Zetter,Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon)

Similarly,Haris Shane's@War: The Rise of the Military–Internet Complex; Schneier Bruce'sData and Goliath: The Hidden Battles to Collect Your Data and Control Your World and Krebs Brian'sSpam Nation: the Inside Story of Organized Cybercrime- from Global Epidemic to Your Front Doorare the same categorical books on cyber security. These novels also through lights on current cyber-crimes of technology and suggests peoples to aware of it. These novels help each and every reader about cyber security.

Conclusion:

In this way, novels give us various types of analytical point of view of today's way of life. These novels try to secure reader from cyber-crime by giving some imaginative and real incidents. And this is the main purpose of the present research paper. There is no limit of cyber security, but at last we can now realize it. And now we can try to protect ourselves from it.

Citation:-

Bowden Mark. Worm: The First Digital War. Grove Press, 2012.

Coleman Gabriella. Hacker, Hoaxer, Whistle-blower, Spy: The Many Faces of Anonymous. Verso; Reprint, 2015.

Goodman Marc. Future Crimes: Inside the Digital Underground and the Battle for Our Connected World. Anchor; Reprint, 2016.

Kaplan Fred. Dark Territory: The Secret History of Cyber War. Simon & Schuster; Reprint, 2017.

Mitnik Kevin. "Ghost in the Wires: My Adventures as the World's Most Wanted Hacker. Little, Brown and Company; 1, 2011.

Stoll Clifford. The Cuckoo's Egg. Gallery Books; Reissue, 2005.

Zegart Amy & Herbert Lin. Bytes, Bombs and Spies: The Strategic Dimensions of Offensive Cyber Operations. Broockings Institution, 2018.

Zetter Kim. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. Crown; Reprint, 2015.

19

HOW EMOTIONAL INTELLIGENCE ENRICHES KNOWLEDGE MANAGEMENT

Dr. Aasim Mir
Sr. Assistant Professor,
Department of Management Studies,
Baba Ghulam Shah Badshah University, Rajouri

****

ABSTRACT

Study on assessment and management of emotions is talk of the arena now a days. It has been now very neatly assessed that a person before offering any type of assignment weather regular or temporary must not only be accessed on behavioural or physical parameters but also on emotional parameters. Thus the implantation of Emotional Intelligence practices to evaluate the emotional content of individuals is gaining priority in the market. Emotional Intelligence not only helps in recognition of self and other people emotions but also lays platform for their management as well. The current study shall seek to identify the role played by Emotional Intelligence dimensions in reframing Knowledge Management practices being offered and managed among telecom sector employees in Jammu division of Jammu and Kashmir. The study shall further analyze the impact of individual dimensions considered in the current research study on several dimensions of Knowledge Management on individual basis. The study shall further recommend various suggestions from desired results to improve the overall work mechanism of telecom sector employees in Jammu division of Jammu and Kashmir in particular and for rest of India in general.

KEYWORDS: Emotional Intelligence, Knowledge Management, Transparency, Knowledge Capturing & Storage, Knowledge Acquisition & Creation, Knowledge Dissemination & Transfer, Knowledge Application, Conscientiousness, Adaptability, Innovativeness etc.

INTRODUCTION

Emotional Intelligence represents the ability or capacity to access and manage the emotions of self and also emotions of others. Individuals possessing this intelligent trait contribute well in the form of high performance, job satisfaction, integrated and collaborated teamwork and lower level of turnover intentions. It further enhances self-confidence, self-motivation and ability to face challenges in this dynamic work culture. Higher productivity at work due to effective job satisfaction is also possible only when people are able to understand and manage their emotions well in time. Emotional Intelligence also helps in managing stress and burnout level of people which acts as a hindrance in their potential growth and development (Goleman, 1995). The current study involves several dimension of Emotional Intelligence that seems to having an impact on various dimensions of Knowledge Management. These dimensions include Transparency, Conscientiousness, Adaptability and Innovativeness. Transparency dimension accounts for developing fare practices that directly leads to desired actions and activities. Conscientiousness considers mechanism that holds the fair process for taking responsibilities in order to enhance performance. People with enriched Conscientiousness are able to keep commitments made with others, smoothly achieve objectives and adopt an organized platform. Adaptability helps people to handle rapid and sudden changes that take place in work environment. They further are able to meet augmented demands during rapid changes in environment and are responsible for bringing flexibility while leading several events. Innovativeness accounts for enhancing the scope of thinking with new contemplations and ideas. People possessing this trait are able to find out new sources of ideas, problem solving techniques and augment creative thinking. Knowledge Managementrepresents the process of planning, organizing and managing knowledge related assets so that it can be effectively utilized wherever required. The several dimensions of Knowledge Management that has been adopted to conduct this research study include Knowledge Acquisition & Creation, Knowledge Capturing & Storage, Knowledge Dissemination & Transfer and Knowledge Application. Knowledge Acquisition & Creation are categorized into two fold initiatives i.e. Knowledge Acquisition &Knowledge Creation. Knowledge Creation uses the process of socialization, externalization, internalization and combination of all these to generate a desired set of knowledge whereas Knowledge Acquisition holds the mechanisms of search, sourcing and grafting to acquire knowledge. Knowledge Capturing & Storageholds the process for conversion of knowledge to an explicit form and its storage so that it can be easily retrieved and utilized anytime. Knowledge Dissemination & Transfer brings out ways for diffusion and distribution of desired knowledge for the purpose of enhancing performance and final output. Knowledge Application accounts for identifying and developing new ways of using synthesized data and information that can provide new insights in the form of new opportunities and also add a value chain to existing mechanisms and phenomenon (Nonaka, 1994).

OBJECTIVES OF THE STUDY

1. To analyze the effect of Trustworthiness dimension of Emotional Intelligence on several dimensions of Knowledge Management.

2. To admittance the influence of Conscientiousness dimension of Emotional Intelligence on numerous dimensions of Knowledge Management.

3. To study the role of Adaptability dimension of Emotional Intelligence on voluminous dimensions of Knowledge Management.

4. To examine the influence of Innovativeness dimension of Emotional Intelligence on various dimensions of Knowledge Management.

LITERATURE REVIEW

(Milton, 2005) Emotional Intelligence has been witnessed to play a greater role in understanding and managing emotions of people that enhances greater team and group cohesiveness and efficient flow of knowledge and information between groups and teams. Higher Emotional Intelligence further enhances self-confidence, capacities of networking and also accounts for improving tactical and social skills without which Knowledge Management practices are meaningless. Furthermore higher level of Emotional Intelligence enhances improved decision making and enhancement of social and technical skills.

(Karkoulian, Hareke, Messarra, 2010) conducted a research study to analyze the relationship between knowledge sharing and emotions. It was found that proper recognition and management of emotions accounts for better sharing and dissemination of knowledge domains. Moreover higher the level of Emotional Intelligence, better shall be the capability of sharing and managing knowledge.

(Dulewicz& Higgs, 2000)deliberated a research study by considering Knowledge Management and competitive advantage and also role played by Emotional Intelligence as a moderator. It was found that there exists a strong association between Knowledge Management and competitive advantage. It was further elaborated that Emotional Intelligence has a great and significant level of impact on Knowledge Management and competitive advantage. Individuals with higher level of Emotional Intelligence hold extended level of Knowledge Management practices and competitive advantage as compared to others.

(Vince, 2004) deliberated a study considering Emotional Intelligence, social learning and its application in several organizations. The study found that Emotional Intelligence plays a significant role in enhancing social learning and also improves learning capabilities of individuals.

(Mir Aasim, 2021) conducted a study on evaluating role of Emotional Intelligence dimensions in remodeling Knowledge Management mechanism among agriculture workers. It was found that some dimensions of Emotional Intelligence has a direct and significant impact on Knowledge Management practices while there are also some dimensions of Knowledge Management that does not have any association with various dimensions of Emotional Intelligence.

MATERIAL AND METHODS

The data and information for the current research study shall be collected using both primary as well as secondary information and data. Primary data and information shall be collected using pretested questionnaire regarding several dimensions of Emotional Intelligence and Knowledge Management from telecom sector employees working in Jammu division of Jammu and Kashmir. Secondary data regarding telecom sector shall be collected from various agencies, telecom sector offices and directorate of information and telecommunication government of Jammu and Kashmir. The data and information collected from various sources (respondents) shall be analyzed to workout various relationships whether positive or negative in order to determine the overall framework and future course of recommendations. The study involves a total of 250 respondents who work in telecom sector in telecom department of Jammu and Kashmir.

RESULT AND DISCUSSION

Several dimensions of Emotional Intelligencehave a diversified impact on numerous dimensions of Knowledge Management when analyzed together. The detailed analysis regarding assessing the impact of various dimensions of Emotional Intelligence on various dimensions of Knowledge Management is given below as:

Table 01:

Dimensions & Sub-dimensions	Relationship	Estimates	Standard Estimates	P-Value	Significance (Yes/No)
Transparency – Knowledge Acquisition & Creation	T-KAC	0.243	0.097	0.024	Yes

Table 01 represents the values of analysis between Transparency dimension of Emotional Intelligence and Knowledge Acquisition & Creation dimension of Knowledge Management. The results depicted that Transparency dimension of Emotional Intelligence has a significant impact on Knowledge Acquisition & Creation dimension of Knowledge Management among telecom sector works in Jammu division. It was further found that Transparency supports upgradation of Knowledge Acquisition & Creation pattern of telecom sector workers. The estimated p value is 0.024. The values of Estimates and Standard Estimates have been found to be 0.243 and 0.097.

Table 02:

Dimensions & Sub-dimensions	Relationship	Estimates	Standard Estimates	P-Value	Significance (Yes/No)
Transparency – Knowledge Capturing & Storage	T-KCS	0.133	0.049	0.362	No

Table 02 shows values of analysis between Emotional Intelligence's Transparency dimension and Knowledge Capturing & Storage dimension of Knowledge Management. It has been found that Transparency dimension does not at all have any association with Knowledge Capturing & Storage pattern of telecom sector workers in Jammu division of Jammu and Kashmir. The estimated p value is 0.362. The values of Estimates and Standard Estimates have been found to be 0.133 and 0.049.

Table 03:

Dimensions & Sub-dimensions	Relationship	Estimates	Standard Estimates	P-Value	Significance (Yes/No)
Transparency – Knowledge Dissemination & Transfer	T-KDT	0.230	0.079	0.028	Yes

Table number 03 represents relationship of Emotional Intelligence's Transparency dimension with Knowledge Management's Knowledge Dissemination & Transfer dimension. It was found that there exists a strong positive relationship between Transparency and Knowledge Dissemination & Transfer among telecom sector workers in Jammu division. Further found that Transparency enriches Knowledge Dissemination & Transfer process of workers up to a greater extent. The estimated p value is 0.028. The values of Estimates and Standard Estimates have been found to be 0.230 and 0.079.

Table 04:

Dimensions & Sub- dimensions	Relationship	Estimates	Standard Estimates	P- Value	Significance (Yes/No)
Transparency – Knowledge Application	T – KA	0.134	0.041	0.348	No

Table 04 accounts for presenting association of Transparency dimension and Knowledge Application of telecom sector workers/ employees. Findings revealed that transparency dimension of Emotional Intelligence do not have any association with Knowledge Application mechanism of telecom sector workers. It was further accessed that knowledge application does not even require transparency as a broad target as it is being managed by each employee in terms of competitive scope which is based on narrow target. The estimated p value is 0.348. The values of Estimates and Standard Estimates have been found to be 0.134 and 0.041.

Table 05:

Dimensions &Sub- dimensions	Relationship	Estimates	Standard Estimates	P-Value	Significance (Yes/No)
Conscientiousness - Knowledge Acquisition & Creation	C – KAC	0.227	0.082	0.023	Yes

Table 05 shows values of analysis between Conscientiousness dimension of Emotional Intelligence and Knowledge Acquisition & Creation dimension of Knowledge Management. The study found that there is a strong significant relationship between the two dimensions. It depicts thatConscientiousness dimension of Emotional Intelligence plays a very important role in framing way outs for Knowledge Acquisition & Creation dimension of Knowledge Management. The estimated p value is 0.023. The values of Estimates and Standard Estimates have been found to be 0.227 and 0.082.

Table 06:

Dimensions & Sub- dimensions	Relationship	Estimates	Standard Estimates	P- Value	Significance (Yes/No)
Conscientiousness - Knowledge Capturing & Storage	C – KCS	0.236	0.092	0.031	Yes

The relationship of Conscientiousness dimension and Knowledge Capturing & Storage dimension has been depicted in table number 06. It has been found that there exists a strong and positive relationship between Conscientiousness and Knowledge Capturing & Storage. Conscientiousness has been further found to be working for synthesis of data and information under Knowledge Capturing & Storage dimension. The estimated p value is 0.031. The values of Estimates and Standard Estimates have been found to be 0.236 and 0.092.

Table 07:

Dimensions & Sub- dimensions	Relationship	Estimates	Standard Estimates	P- Value	Significance (Yes/No)
Conscientiousness – Knowledge Dissemination & Transfer	C – KDT	0.136	0.033	0.254	No

Table 07 demonstrates the association of Conscientiousness dimension of Emotional Intelligenceand Knowledge Dissemination & Transfer dimension of Knowledge Management. Study found that there is no significant association between Conscientiousness and Knowledge Dissemination & Transfer. Further Knowledge Dissemination & Transfer dimension itself accounts for pellucidity thus does not require Conscientiousness separately. The estimated p value is 0.254. The values of Estimates and Standard Estimates have been found to be 0.136 and 0.033.

Table 08:

Dimensions & Sub- dimensions	Relationship	Estimates	Standard Estimates	P- Value	Significance (Yes/No)
Conscientiousness - Knowledge Application	C – KA	0.175	0.044	0.240	No

Table 08 has demonstrated the affiliation between Conscientiousness dimension of Emotional Intelligence and Knowledge Application dimension of Knowledge Management. It was found that Conscientiousness and Knowledge Application does not share any linear association as depicted by p value of 0.240. The values of Estimates and Standard Estimates have been found to be 0.175 and 0.044.

Table 09:

Dimensions & Sub-dimensions	Relationship	Estimates	Standard Estimates	P-Value	Significance (Yes/No)
Adaptability - Knowledge Acquisition & Creation	AD – KAC	0.141	0.041	0.233	No

Table 09 has been accounted to draw some facts regarding affiliation of Adaptability dimension of Emotional Intelligence and Knowledge Acquisition & Creation dimension of Knowledge Management. It has been witnessed that Adaptability dimension does not have any role in devising mechanism for Knowledge Acquisition & Creation of telecom sector workers in Jammu division of Jammu and Kashmir. The estimated p value is 0.233. The values of Estimates and Standard Estimates have been found to be 0.141 and 0.041.

Table 10:

Dimensions & Sub-dimensions	Relationship	Estimates	Standard Estimates	P-Value	Significance (Yes/No)
Adaptability - Knowledge Capturing & Storage	AD – KCS	0.218	0.088	0.018	Yes

Adaptability dimension of Emotional Intelligence and Knowledge Capturing & Storage dimension of Knowledge Management has been found to be sharing a strong and significant relationship when studied for telecom sector workers in Jammu division of Jammu and Kashmir. Adaptability has further found to be making an acquiescence schedule for Knowledge Capturing & Storage. The values of analysis have been given in table 10 where p value stands at 0.018. The values of Estimates and Standard Estimates have been found to be 0.218 and 0.088.

Table 11:

Dimensions & Sub-dimensions	Relationship	Estimates	Standard Estimates	P-Value	Significance (Yes/No)
Adaptability – Knowledge Dissemination & Transfer	AD – KDT	0.135	0.050	0.250	No

The association of Adaptability dimension and Knowledge Dissemination & Transfer dimension has been depicted in table number 11 above. From the table values it is viable that Adaptability dimension of Emotional Intelligence and Knowledge Dissemination & Transfer dimension of Knowledge Management does not hold a significant relationship with each other among telecom sector workers in Jammu division. The estimated p value is 0.250. The values of Estimates and Standard Estimates have been found to be 0.135 and 0.050.

Table 12:

Dimensions & Sub- dimensions	Relationship	Estimates	Standard Estimates	P-Value	Significance (Yes/No)
Adaptability - Knowledge Application	AD – KA	0.259	0.082	0.028	Yes

Table 12 considered association of Adaptability and Knowledge Application. The findings showed that Adaptability enhances scope for Knowledge Application among telecom sector workers. It further enhances competitive positioning of Knowledge Application dimension. The estimated p value is 0.028. The values of Estimates and Standard Estimates have been found to be 0.259 and 0.082.

Table 13:

Dimensions & Sub-dimensions	Relationship	Estimates	Standard Estimates	P-Value	Significance (Yes/No)
Innovativeness - Knowledge Acquisition & Creation	INN – KAC	0.133	0.052	0.292	No

Table 13 represents relationship of Innovativeness dimension of Emotional Intelligence with Knowledge Acquisition & Creation dimension of Knowledge Management. It was found that Innovativeness dimension of Emotional Intelligence does not hold any significant association with Knowledge Acquisition & Creation dimension of Knowledge Management. The estimated p value is 0.292. The values of Estimates and Standard Estimates have been found to be 0.133 and 0.052.

Table 14:

Dimensions & Sub-dimensions	Relationship	Estimates	Standard Estimates	P-Value	Significance (Yes/No)
Innovativeness - Knowledge Capturing & Storage	INN – KCS	0.246	0.083	0.027	Yes

The association of Innovativeness dimension of Emotional Intelligence with Knowledge Capturing & Storage dimension of Knowledge Management has been depicted in table 14. It has been assessed that Innovativeness dimension holds a very strong and positive association with Knowledge Capturing & Storage dimension among telecom sector workers in Jammu division with p value of 0.027. The values of Estimates and Standard Estimates have been found to be 0.246 and 0.083.

Table 15:

Dimensions & Sub-dimensions	Relationship	Estimates	Standard Estimates	P-Value	Significance (Yes/No)
Innovativeness - Knowledge Dissemination & Transfer	INN– KDT	0.226	0.081	0.032	Yes

Table number 15 shows values of association between Innovativeness dimension and Knowledge Dissemination & Transfer dimension among telecom sector workers in Jammu division. The table values depict that Innovativeness dimension and Knowledge Dissemination & Transfer dimension holds a highly significant relationship with each other. The estimated p value is 0.032. The values of Estimates and Standard Estimates have been found to be 0.226 and 0.081.

Table 16:

Dimensions & Sub-dimensions	Relationship	Estimates	Standard Estimates	P-Value	Significance (Yes/No)
Innovativeness - Knowledge Application	INN – KA	0.237	0.080	0.026	Yes

Table 16 shows association of Innovativeness dimension of Emotional Intelligence with Knowledge Application dimension of Knowledge Management. It has been found that innovativeness dimension of Emotional Intelligence plays a very important and vital role in managing Knowledge Application pattern of telecom sector workers in Jammu division of Jammu and Kashmir. The estimated p value is 0.026. The values of Estimates and Standard Estimates have been found to be 0.237 and 0.080.

Table 17: Overall Summary

Dimensions & Sub-dimensions	Relationship	Estimates	Standard Estimates	P-Value	Significance (Yes/No)
Transparency – Knowledge Acquisition & Creation	T-KAC	0.243	0.097	0.024	Yes
Transparency – Knowledge Capturing & Storage	T-KCS	0.133	0.049	0.362	No
Transparency – Knowledge Dissemination & Transfer	T-KDT	0.230	0.079	0.028	Yes
Transparency – Knowledge Application	T – KA	0.134	0.041	0.348	No
Conscientiousness - Knowledge Acquisition & Creation	C – KAC	0.227	0.082	0.023	Yes
Conscientiousness - Knowledge Capturing & Storage	C – KCS	0.236	0.092	0.031	Yes
Conscientiousness - Knowledge Dissemination & Transfer	C – KDT	0.136	0.033	0.254	No
Conscientiousness - Knowledge Application	C – KA	0.175	0.044	0.240	No
Adaptability - Knowledge Acquisition & Creation	AD – KAC	0.141	0.041	0.233	No
Adaptability - Knowledge Capturing & Storage	AD – KCS	0.218	0.088	0.018	Yes
Adaptability - Knowledge Dissemination & Transfer	AD – KDT	0.135	0.050	0.250	No
Adaptability - Knowledge Application	AD – KA	0.259	0.082	0.028	Yes
Innovativeness - Knowledge Acquisition & Creation	INN – KAC	0.133	0.052	0.292	No
Innovativeness - Knowledge Capturing & Storage	INN – KCS	0.246	0.083	0.027	Yes
Innovativeness - Knowledge Dissemination & Transfer	INN – KDT	0.226	0.081	0.032	Yes
Innovativeness - Knowledge Application	INN – KA	0.237	0.080	0.026	Yes

CONCLUSION

Emotional Intelligence plays a moderate role in reshaping Knowledge Management practices of telecom sector workers in Jammu division of Jammu and Kashmir. Transparency dimension of Emotional Intelligence has a very significant association with Knowledge Acquisition & Creation and Knowledge Dissemination & Transfer dimension of Knowledge Management but has no association with Knowledge Capturing & Storage and Knowledge Application dimension of Knowledge Management. Moreover Conscientiousness dimension of Emotional Intelligence has the capability of reorienting Knowledge Acquisition & Creation and Knowledge Capturing & Storage dimension of Knowledge Management while does not impact Knowledge Dissemination & Transfer and Knowledge Application dimensions. Furthermore Adaptability has been found to remodeling Knowledge Capturing & Storage and Knowledge Application dimensions while does not show any significance with Knowledge Acquisition & Creation and Knowledge Dissemination & Transfer. Additionally Innovativeness dimension of Emotional Intelligence reorganizes Knowledge Capturing & Storage, Knowledge Dissemination & Transfer and Knowledge Application of telecom sector workers. Moreover Innovativeness shows no positive association with Knowledge Acquisition & Creation.

REFERENCES

1. Dulewicz, V. & Higgs, J. (1998b). "Emotional Intelligence: Can it be measured reliably and validly using competency data?", Competency Journal, 6, (1).

2. Dulewicz, V. & Higgs, J. (1998a). "Emotional Intelligence: Managerial Fad or Valid Construct?", Henley Working Paper 9813, http://www.henley.reading.ac.uk/management/research/mgmt-publications.aspx Accessed 22 July 2010.

3. Goleman, D. (1995). Emotional Intelligence: Why it can matter more than IQ. New York Bantam.

4. Goleman, D. (1998a). Working with Emotional Intelligence. New York: Bantam Books.

5. Goleman, D., Boyatzis, R. & McKee, A. (2001). Primal leadership: The hidden driver of great performance. Harvard Business Review, 1-16.

6. Goleman, D. (2003). Apples and applesauce: Issues and recent developments in Emotional Intelligence,1(3), Available http://www.eiconsortium.org.

7. Karkoulian,S., Harake, N.A., Messarra, L.C.,(2010), Correlates of Organizational Commitment and Knowledge Sharing via Emotional Intelligence: An Empirical Investigation. The Business Review Cambridge, 15(1), 89-96.

8. Milton, N.(2005): Knowledge Management For Teams And Projects. Chandos Publishing, Oxford.

9. Mir Aasim, (2021), Role of Emotional Intelligence Dimensions in Remodeling Knowledge Management Mechanism Among Agriculture Workers, JuniKhyat Journal, ISSN: 2278-4632, Vol-11 Issue-02 No.02.

10. Nonaka I. (1994), A Dynamic Theory of Organizational Knowledge Creation, Organizational Science Journal, 5(1), 14-37.

11. Psilopanagioti, A., Anagnostopoulos, F., Mourtou, E., &Niakas, D. (2012). Emotional Intelligence, emotional labor and job satisfaction among physicians in Greece. MBC Health Service Research,12 (463)

12. Quebbeman, A.J. &Rozell E.J. (2002). Emotional Intelligence and dispositional affectivity as moderators of workplace aggression: The impact on behavior choice. Human Resource Management Review,12(01), 125-143.

13. Quoidbach, J. &Hansenne, M. (2009). The impact of trait Emotional Intelligence on nursing team performance and cohesiveness. Journal of Professional Nursing, 25, 23-29.

14. R. Fatemeh, G. Shohreh& K. Javad. (2014). The effect of training Emotional Intelligence on occupational performance and public health of nurses working in hospitalization wards of Shafa Hospital of Rasht City. Indian Journal of Fundamental and Applied Life Sciences, 04,1063-1070.

15. Shepherd, Barnett, Cooper, Coyle, Moran, Senior, & Walton. (2007). Towards an understanding of British public attitudes concerning human cloning. Journal of Social Science and Medicine, 65(02), 377-392.

16. Shields, A, Dickstein S, Seifer R, Giusti, L. Magee, KD, Spritz, B. (2001). Emotion competence and early school adjustment: A study of preschoolers at risk. Early Education and Development,12,73–96.

17. Vince, R (2004). Uncomfortable Knowledge Management: The impact of emotion on organizational learning.

18. Vince, R. & Martin, L. (1993). "Inside Action Learning: An Exploration of the Psychology and Politics of the Action Learning Model", Management Education and Development, 24, pp.205-15.

❑❑❑

20

STUDY OF WORKING CAPITAL OF VARDHMAN FERTILIZER & SEEDS PRIVATE LIMITED, DISTRICT SOLAPUR, MAHARASHTRA

Asst. Prof. Vijay B. Kadam
Head of Cost & Works Accounting Dept.,
Department of Commerce,
Amruteshwar Arts, Commerce, & Science
College, Vinzar, Tal. Velha, Dist. Pune
Savitribai Phule Pune University (SPPU), Pune,
Maharashtra

****

ABSTRACT

Working capital management is concerned with the problems that arise in attempting to manage the current assets, the current liabilities and the interrelationship that exists between them. This paper tries to make an attempt to study the working capital, components of working capital and liquidity of '**Vardhman Fertilizer & Seeds Private Limited, District Solapur'**.

The paper also tries to study the correlation between liquidity and profitability of this fertilize unit. The study is bases on secondary data collected from annual report of this fertilizer unit for the period of 5 years on website of ministry of company affair of India. In this paper, there is an application of correlation analysis for identity the significant of working capital management include the current ratio and quick ratio on the quiddity positon of this fertilizer units.

KEY WORDS: Working Capital, objectives, Hypothesis, sources of data collection, limitation, Net Working Capital, Net Working Capital Ratio, Current Ratio, Liquid Ratio, Findings, Suggestion, Conclusion & References.

INTRODUCTION

Working capital study of '**Vardhman Fertilizer & Seeds Private Limited, District Solapur' (VFSPLDS)**is of major importance of internal & external analysis because of its relationship with the current day to day operations of business. Funds, collected from different sources are invested in the business for the acquisition of assets. These assets are employed for earning revenue. The basic problem facing the finance manager of an enterprise is to tradeoff between conflicting but equally important goals of liquidity and profitability and vice versa.

NEED OF STUDY

1. To study the need of maintain sufficient working capital of fertilizer units.

2. To check balance between liquidity and short term.

OBJECTIVES OF THE STUDY

1) To study the position of working capital of selected fertilizer units.

2) To make suggestions for the better working capital management of fertilizer units.

HYPOTHESIS

H0: Insufficient working capital has adverse affected in the liquidity of fertilizer units under study.

H1: Insufficient working capital has not effecting in the liquidity of fertilizer units under study.

PERIOD OF STUDY

The present study is undertaken for the period of five accounting year starting from 2012-2013 to 2016-2017. The researcher has selected 2012-2013 as **base year** for the purpose of analysis and evolution.

SOURCES OF DATA COLLECTION

Researcher has used secondary data as main sources for the presented research study. Annual accounting reports such as Income statement position statement are collected form web side of Ministry of Corporate Affairs (MCA), Maharashtra Reginal Division, of Government of India.

LIMITATION OF THE STUDY

1. The study is limited to five year only.

2. Ratio analysis has its own limitations.

3. This study is based on only secondary data of fertilizer units.

NET WORKING CAPITAL

The net working capital is qualitative that indicating the fertilizer units were ability to meet its operation expenses and currents liability. The term net working capital refers to the difference between current assets and current liabilities.

Net Working Capital = Current Assets – Current Liabilities

Current Assets: Cash balance + Banks Balance + short term Marketable Securitas + Sundry Debtors + Bill Receivables + Inventory + Prepaid Expenses + Short Term Loan and advances + Notes etc.

Current Liabilities: Sundry Creditors + Bill Payable + Outstanding Expenses + Short Term Loans + Short Term Borrowings + Dividend Payable + Provisions + Any Short Term Dues etc.

As per the above given numerical table no. 1 and chart no. 2, it has found that all financial years amount of net working capital (NWC) of **'Vardhman Fertilizer & Seeds Private Limited, District Solapur' (LMBTPLDS)**. The total of five years NWC was Rs. 1038,65,865, arithmetical mean of NWC was Rs. 207,73,173, standard derivation was Rs. 183,63,179 and coefficient variance it was 88.40%.

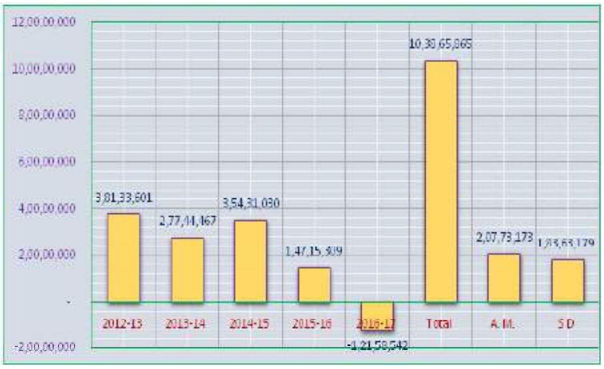
Table No. – 1

Net Working Capital of VFSPLDS

Fertilizer Unit : Solapur	Vardhman Fertilizer & Seeds Pvt. Ltd.			Last 5 Years Figures	
Particulars	2012-2013	2013-2014	2014-2015	2015-2016	2016-2017
A) Current Assets					
1. Current Investment	-	-	-	-	-
2. Inventories	1394,01,660	1453,08,164	1754,55,685	1763,72,714	969,97,541
3. Trade Receivables	372,28,312	498,69,536	507,84,245	202,71,443	226,58,604
4. Cash & Cash Equipment	72,43,476	36,65,919	27,44,317	32,96,109	23,81,005
5. Short Term Lone & Adv.	88,13,594	74,89,101	86,51,625	53,96,921	55,48,925
6. Other Current Assets	8,06,387	5,41,313	7,75,866	5,98,889	2,32,936
Total A)	1934,93,429	2068,74,033	2384,11,738	2059,36,076	1278,19,011
B) Currents Liabilities					
1. Short Term Borrowings	545,38,086	457,05,599	573,81,767	755,77,273	719,67,133
2. Trade Payables	882,99,101	1138,06,624	1211,68,813	943,86,210	495,06,872
3. Short Term Provision	125,22,641	126,44,119	143,59,545	102,83,469	84,16,069
4. Other Current Lia.	-	69,73,224	100,70,583	109,73,815	100,87,479
Total B)	1553,59,828	1791,29,566	2029,80,708	1912,20,767	1399,77,553
Net Working Capital (A-B)	381,33,601	277,44,467	354,31,030	147,15,309	-121,58,542
Total of Last 5 Years Net Working Capital		1038,65,865			
Arithmetical mean (A M)		207,73,173			
Standard Derivation (S D)		183,63,179			
Coefficient of Variance (C V)		88.40%			

Chart No. – 2

Net Working Capital of VFSPLDS



In financial year 2012-2013 the NWC was little high and in 2016-2017 NWC was very low and minus as compare to other financial years. There was no any insufficient short-term investment and net working capital was good all financial years except last year. **This fertilise units was positive net working capital except last year.**

CURRENT RATIO (CR)

Current Assets Ratio also knows as current Ratio, working capital ratio. This ratio expresses the relationship between current assets and current liabilities. The current ratio is calculated by dividing the current assets by current liabilities. Thus can be expressed as pure number or percentage ratio. And the idea current ratio id 2:1. The formulas of current ratio is follows:

Current Assets Ratio = Current Assets / Current Liabilities

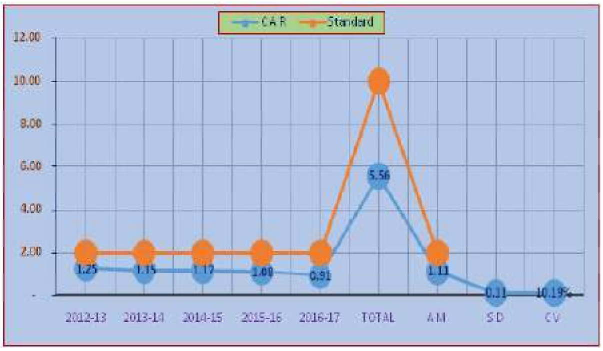
As per the above given numerical table no. 3 and diagram no. 4 has shown the Current Ratio (CR) of **Vardhman Fertilizer & Seeds Private Limited, District Solapur' (LMBTPLDs)**. The CR in year 2012-2013 was 1.25, in 2013-2014 was 1.15, in 2014-2015 was 1.17, in 2015-2016 was 1.08 and 2016-2017 was 0.91. Total of CR in five years was 5.56, arithmetic mean was 1.11, standard derivation was 0.11 and coefficient variance was 10.19%.

Table No. – 3

Current Ratio of VF&SPLDS

Fertilizer Unit : Solapur	Vardhman Fertilizer & Seeds Pvt. Ltd.			Last 5 Years Figures	
Financial Year	C A	C L	C A R	Standard	Remarks
2012 - 2013	1934,93,429	1553,59,828	1.25	2.00	-0.75
2013 - 2014	2068,74,033	1791,29,566	1.15	2.00	-0.85
2014 - 2015	2384,11,738	2029,80,708	1.17	2.00	-0.83
2015 - 2016	2059,36,076	1912,20,767	1.08	2.00	-0.92
2016 - 2017	1278,19,011	1399,77,553	0.91	2.00	-1.09
Total of last 5 Years	9725,34,287	8686,68,422	5.56	10.00	-4.44
Arithmetic Mean (A M)	1945,06,857	1737,33,684	1.11	2.00	-0.89
Standard Derivation (S D)	364,95,228	230,97,086	0.11	-	0.11
Coefficient of Variance (C V)	18.76%	13.29%	10.19%	-	-12.79%

Chart No. – 4
Current Ratio of VF&SPLDS



The CR of five financial years was decreasing order and it was too much below of Standard ratio. In financial year 2014-2015 the CR was high as compare to other years but not sufficient as the standard ratio i.e. 1.17. The chart Show that orange curve line of standard ratio was line shape and blue curve line of CR which was goes little down and below of the Standard Line. **The average CR in five years was 1.11 which was below 0.89 of standard. This fertilizer unit was over trading and under capitalization situation. This CR also shows that there was no short-term solvency position, insufficient & unsatisfactory liquidity.**

LIQUID RATIO

Liquid Ratio also knows 'Quick Ratio', 'Acid Test Ratio' this ratio is concerned with the establishment of relationship between the liquid assets ad quick liabilities. The liquid assets refers to those assets which can be immediately or at a short notice, be converted into cash without loss or diminution value. The ideal quick ratio of 1:1.

Liquid Ratio = Liquid Assets / liquid liabilities

· **Liquid Assets**= All Current Assets – Inventory & Prepaid Expenses

· **Liquid Liabilities** = All Current Liabilities – Bank Overdraft

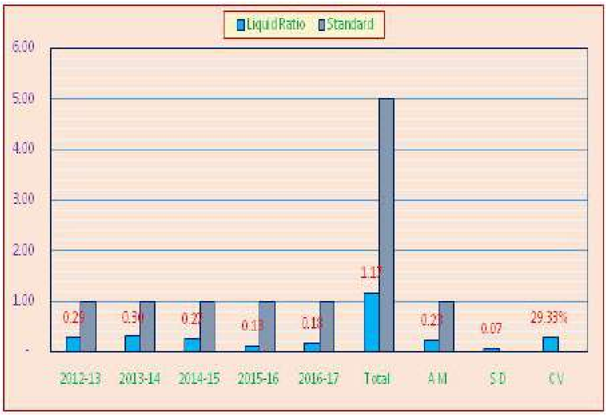
As per the above statistical table no. 5 and diagram no. 6 has shown Liquid Ratio (LR) of**Vardhman Fertilizer & Seeds Private Limited, District Solapur (VF&SPLDS)**. The LR in year 2012-2013 was 0.29, for 2013-2014 was 0.30, for 2014-2015 was 0.27, in 2015-2016 was 0.13 and 2016-2017 it was 0.18. And total of LR in five years was 1.17, arithmetic mean was 0.23, standard derivation was 0.07 and coefficient variance it was 29.33%.

Table No. – 5
Liquid Ratio of VF&SPLDS

Fertilizer Unit : Solapur	Vardhaman Fertilizers & Seed Pvt. Ltd.			Last 5 Years Figures	
Financial Year	L A	L L	LR or QR	STD.	Remarks
2012 - 2013	452,78,175	1553,59,828	0.29	1.00	-0.71
2013 - 2014	540,76,768	1791,29,566	0.30	1.00	-0.70
2014 - 2015	543,04,428	2029,80,708	0.27	1.00	-0.73
2015 - 2016	241,66,441	1912,20,767	0.13	1.00	-0.87
2016 - 2017	252,72,545	1399,77,553	0.18	1.00	-0.82
Total of last 5 Years	2030,98,357	8686,68,422	1.17	5.00	-3.83
Arithmetic Mean (A M)	406,19,671	1737,33,684	0.23	1.00	-0.77
Standard Derivation (S D)	133,88,882	230,97,086	0.07	-	0.07
Coefficient of Variance (CV)	32.96%	13.29%	29.33%	-	-8.94%

The LR of five financial years was decreasing order and it was very lower than standard ratio. In year 2013-2014 the LR was higher and in 2015-2016 it was lower as compare to other years. The chart show that grey bars are standard bars and blue bars of LR were going straight line but overall it was very lower than the Standard bars as compared to all years

Chart No. – 6
Liquid Ratio of VF&SPLDS

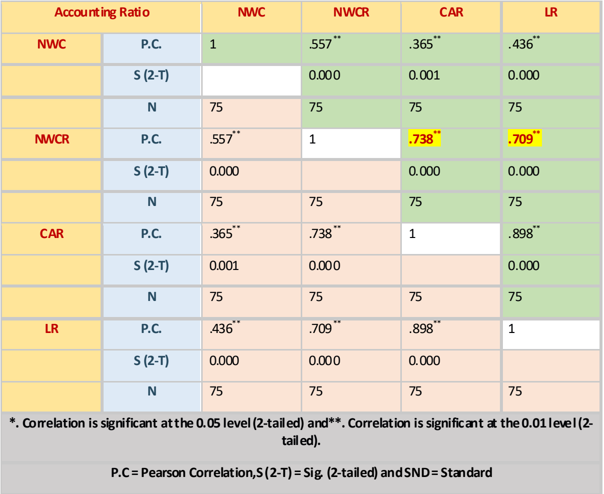


The average liquid ratio was 0.23 in five years which was very lower 0.77 than the standard ratio and it was not maintained sound short-term liquidity. This fertilizer unit was not enable to pay its current liabilities quickly and facing difficulty.

TESTING OF HYPOTHESIS

Table No. 7

Correlation of Accounting Ratio



Accounting Ratio		NWC	NWCR	CAR	LR
NWC	P.C.	1	$.557^{**}$	$.365^{**}$	$.436^{**}$
	S (2-T)		0.000	0.001	0.000
	N	75	75	75	75
NWCR	P.C.	$.557^{**}$	1	$.738^{**}$	$.709^{**}$
	S (2-T)	0.000		0.000	0.000
	N	75	75	75	75
CAR	P.C.	$.365^{**}$	$.738^{**}$	1	$.898^{**}$
	S (2-T)	0.001	0.000		0.000
	N	75	75	75	75
LR	P.C.	$.436^{**}$	$.709^{**}$	$.898^{**}$	1
	S (2-T)	0.000	0.000	0.000	
	N	75	75	75	75

*. Correlation is significant at the 0.05 level (2-tailed) and**. Correlation is significant at the 0.01 level (2-tailed).

P.C = Pearson Correlation,S (2-T) = Sig. (2-tailed) and SND = Standard

"Insufficient working capital has adverse effect in the liquidity and profitability position of fertilizer units under study. Hence alternative hypothesis is accepted (H1),Insufficient working capital has not effecting in the liquidity and profitability position of fertilizer units under study."

The Null Hypothesis (H0) rejected and alternate Hypothesis (H1) is accepted

FINDING

The researcher has found the following some points in the study of working capital of diamond lifter organic fertilizer private limited, district Pune.

1. Net Working Capital of this unit have not any short term investment and liabilities over currents assets and minus all financial years so it was negative NWC.

2. The average Current Assets Ratio (CAR) of this unit for the last five years was 0.66 which is less 1.34 of standard ratio. Form the above analysis it is understand that this unit's short term liquidity is not insufficient and it is very poor.

3. The average Liquid Ratio (LR) one can say that this unit for the last five years was 0.27 which is little less 0.73 of the standard. It is found that above liquidity analysis of this company are not sufficient and it is not good liquid position during the selected period.

SUGGESTION

1. This fertilizer unit should investment at least 1% of their net profit in short-term investments and loan and advance as current assets.

2. This fertilizer unit should reduce at least 10% of short-term borrowings in every financial year.

3. This fertilizer unit should maintain the standard ratios of liquidity such as current assets ratio 2:1, quick ratio 1:1 and standard of cash ratio.

CONCLUSION

As per table number 7 of accounting ratio of **Vardhman Fertilizer & Seeds Private Limited, District Solapur (VF&SPLDS),** there is significant correlation exits between net working capital with liquidity such as current ratio, liquidity ratio of this fertilizer unit. But there is no statistically significant correlation between net working capital and liquidity.

REFERENCES

1. "Research Methodology – Method and Techniques" by C. R. Kothari & Gaurav Garg, Third Edition 2014, New age international Private Limited Publishers, New Delhi.

2. Bhalla V. K. 'Working Capital Management' Chand & Company Pvt. Ltd. New Delhi.

3. 'An accounting study of working capital and its impact on profitability with special reference western Maharashtra' Ph.D. Thesis, The researcher Prof. Vijay B. Kadam.

4. http://www.krishi.maharashtra.gov.in

5. http://www.mca.gov.in

21

Recent Trends in Cyber security

Dr. Rajendra Pawar
Shripatrao Kadam Mahavidyalya Shirwal,
Maharashtra

****

Abstract: Today, due to the modern life style people have joined technology life and using more technology for shopping as well as financial transactions in their cyber space. At the same time , safeguarding of knowledge has become increasingly difficult. In addition, the heavy use and growth of social media, online crime or cybercrime has increased. In the world of information technology, data security plays a significant role. The information security has become one of today's main challenges. Whenever we think of cyber security, we first of all think of 'cybercrimes,' which expand tremendously every day. Different government and businesses take various steps to avoid this form of cybercrime. In addition to numerous cyber protection initiatives, many people are also very worried about it. This paper focuses primarily on cyber security concerns related to the new technology. It also concentrates on the new technologies for cyber security, ethics and developments that impact cyber security.

Keywords: Cyber security, cybercrime, android apps Social networks,

1. Introduction

The process of digitization in all aspects of human life, like healthcare, education, business, etc., has gradually led to the storage of all sorts of information, including sensitive data. Security, is the process of protecting the digitized information from theft or from physical damage while maintaining the confidentiality and availability of information but as technology is growing rapidly, the cybercrime rate also increases both in number and complexity. The reason behind this tremendous growth in cyber-crime is the usage of inadequate software, expired security tools, design flaws, programming errors, easily available online hacking tools, lack of awareness in public, high rates of financial returns, etc. In order to explore the vulnerabilities in the target and thereby to attack the victim, more powerful attack tools are developed by the technical attackers. With this, new attacks in different variations are coming which are difficult to detect. Increase in internet dependency in all walks of life, digital nature of data in huge amounts getting accumulated through online transactions and decentralization of data repositories, has led to the development of effective security algorithms. The continuously changing nature of cybercrime also leads to the difficulty of handling and avoiding emerging threats. The task of securing cyber-space is the most difficult and challenging task as advanced threats play a very active role. Therefore, it is necessary to get insights into the concepts of security defense mechanisms, different techniques and trending topics in the area of information security

1.1 Cyber Crime:

Cybercrime is a term for a crime which uses a PC for robbery and crime of commission. The United States Department of Justice has extended the scope of cybercrime to cover any crime that uses a device for evidence storage. The increasing list of cybercrimes includes computer crimes, such as the spread of network intrusions and pc-viruses, as well as the computer-based variant of established crimes such as theft, stalking, intimidation, and coercion. Often cyber-crimes in common people's language may also be defined as crimes committed using a PC and the web to steal the identity or sell an individual to victims of smuggling or stalking or disrupting operations with malicious programme. As technology has a major role in the lives of an extremely individual day by day, cybercrimes too can increase alongside technological advancements.

1.2 Cyber Security:

Privacy and information protection can be the primary security behaviour which any company cares about continually. We prefer to square measurements currently in a highly digital or cyber-specific environment in which all the data are stored. Social networking sites provide an environment wherever users feel secure while they function with friends and family, cyber criminals also seek to steal personal information via social media sites.

1.3 Scope of The Study:

The interactive structure of the financial environment will be a direct impact on one aspect of the institution's infrastructure and the sensibilities of the financial sector to cybercrimes, in particular attacks on Denial-of-Services. In order to secure all the confidential information from falling into wrong hands, the finance sector should continually track and innovate its systems. The banking sector has always been the leading player in implementing safety systems and behavior and has also been the leading cyber security investment sector.

2. Literature Review

Julian Jang-Jaccard [1] Improving cyber security and protecting critical information infrastructure is important for the security and economic well-being of each country. Safer Internet (and protecting Internet users) have been an important part of the growth of new services and public policy.

Lee, H.; Lee, et al [2]. Various attachment methods have emerged in the past and the key logger is a representative attack tool, which records all user's keyboard data entries and can be easily obtained from the Internet.

Mellado, D.; Mouratidis et al,[3]. Protection is an area in the SPL that has not been studied. Most methods concentrate on implementing safety criteria or properties in the SPL. There were various approaches to variability management and safety criteria from the early stages of production of the product line.

Mohsin, M.; Anwar et al, [4] Whether the established techniques of feature models can be implemented or adapted for cyber security is the challenge in the fields of cyber security. In an approach is proposed in order to enhance the production and the derivative products of safe software product lines (SPLs).

VeenooUpadhyay [5] The wizard asks the user to add "labels" of privacy to select friends, and he uses this feedback to create a classifier using the machine learning pattern, which can be used to allocate privileges to the other user friends automatically. The insight for the design stems from the observation that actual users understand their privacy habits and that friend can see which details they use and reproduce in other friends' settings, based on an implicit set of rules.

Yim, K [6]The main principle of this technique prevents the user from disclosing the actual keyboard data entrance but detects the keyboard data attack techniques. In particular, by producing the random keyboard data, the defender calls for a keyboard input event to secure the user 's actual keyboard data intake by filtering the keyboard data generation.

Nikita TresaCyriacLipsaSadath [7]The paper also discusses the perpetrators of a cyber-attack and the techniques primarily used to achieve their goal. It sheds light on the overall structure of cyber- assault and on its phases and its impact on the financial system.

MdLiakat Ali [8] This study presents a brief overview of the cyber security problems raised by modern developments in technology and innovations; the paper is also focused on the latest cyber security strategies, trends and other ethics in cyber security.

Kutub Thakur [9]Cyber security was used interchangeably for the security of knowledge, where later it sees the human's role in the safety process, although formerly finding this an additional dimension. However, such a debate on cyber safety has major consequences, since it reflects on the ethical part of the whole society. Various systems and models have been developed to solve the problem of cyber security. **J.li [10]** Evaluated firewalls issues and how the routing tables can be configured in a way that minimizes the maximized firewall rule set which helps to avoid performance bottlenecks and limit safety breakthroughs. The problems are NP-full and an heuristic approach has been suggested to demonstrate the efficacy of algorithms using simulations. Two major contributions have also taken place.

3. Cyber Security Techniques:

Cyber-attacks on cyberspace can grow by capitalizing on new techniques. Cyber criminals will most frequently change the current malware signatures to take advantage of new technical faults. In other instances, they actually search for special features of emerging technology to detect weaknesses in malware injection. Cyber criminals are taking advantage of emerging Internet technology and millions and billions of active users to access a huge amount of people easily and effectively using these new technologies.

3.1 Access Control and Password Security:

Security provided by the means of username and passwordis a simple way of providing security for the private information to preserve privacy. This means of providing security is one of the most critical cyber security initiatives.

3.2 Authentication of Data: Until the transmitted information need to be attested that it has come from a reputable supply that was not changed. These documents are often authenticated using a gift from the opposing virus software package inside computers. An honestly opposed virus software package is more essential to protect devices from viruses.

3.3 Malware Scanners:

A software system which sometimes scans all files and documents for malicious code or harmful viruses inside the system. The samples of malicious software systems in this field are generally sorting and noted as malware by viruses, worms, and the Trojan horses.

3.4 Firewall:

Firewall is a software or hardware package which helps separate hackers ,viruses and worms trying to access your PC through the web .The firewall checks all messages that come in and blocks those that fail to meet the security requirements compatible with all messages .Firewalls plays a very vital role in malware detection.

3.5 Role of Social Media in Cyber Security:

In recent modern world, there is a need of interactive businesses which needs to find new ways to secure personal information in more entangled environment. Social media has important role to play in cyber security and in personal cyber-attacks. Adoption of social media among employees is growing and threat of attack is therefore increasing since most of them nearly use social media or social networking sites everyday it is now a massive forum for cyber criminals to hack private information and steal valued information. In recent days, it's very easy to share personal information easily and businesses must make sure that recognise, react in real time and prevent breaches of any kind as quickly as possible. These social media has easily make people to share their private information and hackers can use these information.therefore, people have to take reasonable steps to avoid misuse and loss of their information through these social media.

4. Recent Survey Issues on Cyber Security Trends

Cyber Security concerns the awareness concerning various cyber threats and the implementation of defense policies (i.e countermeasures) to safeguard confidentiality, credibility and availability of digital or IT technologies

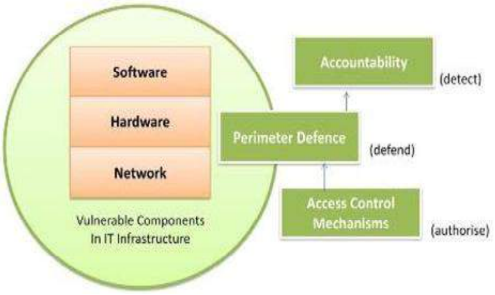


Fig 4.1 Vulnerabilities and Defense Strategies in existing systems

Many cyber security experts consider Malware is the main option for malicious arms to violate the cyber protection efforts of cyberspace. Malware is the widespread class of attacks loaded upon a device, generally without the knowledge of the rightful owner. Like viruses, worms, Trojan horses, spyware and bot executable, malware infects computers in several ways for example propagating from infected devices, trick users into opening tactile file or enticing users to visit websites of malware spreading. Malware could load itself into a USB drive inserted into an infected computer in more concrete cases of malware infection, and then infect any machine into which the computer is then inserted. Malware can spread from the embedded systems and computational logic of devices and equipment. Malware can be introduced in the device life cycle at any time. The victim of malware may vary from end-users, servers and network devices (e.g. routers, switching, etc.) to process control systems like the SCADA. The increase in the number of malware and its complexity are today a major concern in the Internet.

4.1 Phishing Attacks: According to Verizon's latest data violation survey, 32% of the data violations confirmed were attributable to phenomena. The purpose of the assaults is to collect confidential information such as usernames, passwords, the social security numbers and card details by duplicating the victims into believing they connect with a trustworthy person, by either email or by text, and increasingly by means of telephone.

4.2 IoTRansomware:

The internet of things contains several devices, i.e. home equipment and service sensors, which are connected to the network. Climate control devices and refrigerators do not often contain confidential information through their own devices; they may be kept as hostages and are possible targets for hackers to access information in backend systems such as those in power supplies and communication facilities

4.3 Increased Data Privacy Regulation:

The General Data Protection Regulations for Europe(GDPR) was introduced in May 2018 to strengthen European citizens' rights of data privacy and to implement compliance with more rigorous global regulations or severe financial penalties for non-compliance.

4.4 Cyber Attacks on Mobile Devices :

Recent RSA research has concluded that in 2018 " 80% of fraudulent mobile transactions " have risen exponentially with mobile app fraud since 2015 with mobile devices touching each part of our life and working life ,their risk perceptions also grow higher.

4.5 Increased Investment in Automation :

Automation technology is gaining ground in organisations by allowing underemployed cyber security teams to focus on more complex problems,not on routine, often worldly work .According to a recent Ponemon Institute survey, 79% of respondents use security automation tools and frameworks and 50% expect to use security automation in their businesses. In these situations, the first approach to data protection provides an ultimate defense against Cyber-attacks such as database fraud and fitness, and its profound effect on a business .It may enhance efficiency ,but skills and expertise are still necessary to minimize cyber security risk.

4.5 Preventive measures to avoid Cybercrimes:

The five latest emerging trends in cyber security

1. Cyber security skills and organizations are also changing.
2. Protection in the cloud is a top priority.
3. Shift your attention from security and prevention
4. Production centers manage the application and data protection.

Next generation safety digital environments can only determine cybercrime through technological measures; capacity building, organizational structure and global collaboration, along with legislative steps, were also required

5. Conclusion

This paper concludes that the cyber-crime has significant consequences for national and economic security. It is pervasive, violent, ubiquitous and increasingly sophisticated. There are significant risks for many industry agencies, public and private organization's (especially critical infrastructure) for companies and governments alike, it will be necessary for future growth, innovation and competitive advantage to have a cyber-security role in all its components. Every New Year, the security of data, continues to differ from cybercrime by entirely different methods. The newest and most turbulent innovations, along with emerging cyber techniques and regular attacks, are difficult organisations that not only protect their infrastructure but also need new channels and intelligence. However, we do have to do our hardest to attenuate cybercrime so that we can have a healthy and stable future in cyber-houses. The technologies of stable Internet and efficient systems of the next century have been proposed as important research fields for the future. The advancement of global identity management and monitoring techniques to monitor opponents have also become an important issue in the future

6. Conclusion

The enormous increase in Internet access and the progress of Internet-enabled devices, the rising numbers of the population and wide spread use of the Internet, frequently showing highly sensitive personal data with little realization of the implications of information leakage.

We speculate that concerns relating to end user confidentiality will rise in line with the increasing amount of knowledge accessible on the internet in the future.

Furthermore, usability issues are becoming ever more relevant as a way of intuitively learning about and using end-user-oriented protection mechanisms without complicating or profound learning curves to secure the data. Cyber safety practice in the community is built up with innovative patches that rectify existing security and confidentiality problems and move on to them.

Some believe that this revolutionary strategy has failed and will be unable to fulfill future requirements, because the original Internet has been invented in a somewhat different context from how it is used today. An approach to "thinking beyond" is suggested to make better use of the increasingly-demands of the future without referring to the existing computing system and future, but to start again

6. References

[1] Ravi Sharma Study of Latest Emerging Trends on Cyber Security and its challenges to Society International Journal of Scientific & Engineering Research, Volume 3, Issue 6, June-2012 1ISSN 2229-5518.

[2] Lee, H.; Lee, Y.; Lee, K.; Yim, K. Security Assessment on the Mouse Data using Mouse Loggers. In Proceedings of the International Conference on Broadband and Wireless Computing, Communication and Applications, Asan, Korea, 5–7 November 2016

[3] Mellado, D.; Mouratidis, H.;

Fernández-Medina, E. Secure Tropos Framework for Software Product Lines Requirements Engineering. Comput. Stand. Interfaces 2014, 36, 711–722

[4] Mohsin, M.; Anwar, Z.; Zaman, F.; Al-Shaer, E. IoTChecker: A data-driven framework for security analytics of Internet of Things configurations. Comput.Secur. 2017, 70, 199–223

[5] VeenooUpadhyay, SuryakantYadav Study of Cyber Security Challenges Its Emerging Trends: Current Technologies International Journal of Engineering Research and Management (IJERM) ISSN: 2349- 2058, Volume-05, Issue-07, July 2018

[6] Yim, K. A new noise mingling approach to protect the authentication password. In Proceedings of the 2010 International Conference on Complex, Intelligent and Software Intensive Systems, Seoul, Korea, 30 June–2 July 2012

[7] Nikita TresaCyriacLipsaSadath Is Cyber Security Enough- A study on Big Data Security Breaches in Financial Institutions 2019 4th International Conference on Information Systems and Computer Networks (ISCON) GLA University, Mathura, UP, India. Nov 21-22, 2019

[8] MdLiakat Ali Kutub Thakur Beatrice Atobatele Challenges of Cyber Security and the Emerging Trends BSCI'19, July 8, 2019, Auckland, New Zealand

[9] Kutub Thakur1, Meikang Qiu2", Keke Gai3, MdLiakat Ali4 An Investigation on Cyber Security Threats and Security Models 2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing 978-1-4673-9300-3/15

[10] J. Li. The research and application of multi-firewall technology in enterprise network security. Int'l J. of Security and Its Applications, 9(5):153–162, 2015

❑❑❑

22

E-commerce and Cyber Security

Dr. Rekha Chetwani
Asst. Professor,
M.U. College of Commerce, Pimpri, Pune

****

According to the editor-in-chief of International Journal of Electronic Commerce, Vladimir Zwass, 'Electronic commerce is sharing business information, maintaining business relationships and conducting business transactions by means of telecommunications networks'.

E-commerce has an impact on three major stakeholders, namely society, customers and organisations . There are a number of benefits of ecommerce, like, cost reduction, increased efficiency, customisation and global market. There are also few limitations associated with e-commerce . These include information overload, reliability and security issues. Successful e-commerce involves understanding the limitations and working upon it to minimizing its negative impact .

E commerce sites are ocean of personal and financial data for hackers. As far as businesses are concerned, the cost of a breach in loss of data and consequently, loss of customer trust can have high damaging impacts for businesses of all sizes.

Ecommerce business owners are also aware of these issues and are increasing trying to provide better security measures to their customers. Online retailers are adding increasingly innovative technologies to their sites to stay competitive. At the same time cyber attackers are equally sharpening their skills and finding new vulnerabilities to exploit. The best way to stay ahead is to be aware oftypes of attacks andpractice ecommerce security best practices. Ecommerce security primarily refers to the steps taken by ecommerce businesses to protect their business and information from harmful attacks. It primarily includes protocols designed to safeguard information within the business.

Common Ecommerce Security Threats & Issues

Followings are some of the most commonly found security threats that an ecommerce unit needs to protect its business from.

1. Phishing

It is one of the most common security threats of ecommerce where hackers masquerade as legitimate businesses and send emails to your clients. This email is a trick to push them to reveal their sensitive information. They do so by simply presenting a fake copy of legitimate website or anything that makes the customer believe that the request is coming from agenuine business.

2. Financial Frauds

Refund fraud is a common financial fraud. Hackers make unauthorized transactions and wipe out the trail costing businesses significant amounts of losses. They also engage in return of goods and place refunds for illegally acquired products or damaged goods.

3. Spam

Emails also act as one of the highly used mediums for spamming. They often send them via social media inbox and wait for the recipient to click on such messages. Moreover, spamming not only affects website's security, but it also damages website speed too.

4. Bots

There are exclusive bots developed by hackers to scrape websites for their pricing and inventory information. The hackers use such information to change the pricing of online business store, or to garner the best-selling inventory in shopping carts, resulting in a decline in sales and revenue.

5. **DDoS Attacks**

Distributed Denial of Service (DDoS) attacks and DOS (Denial of Service) attacks aim to disrupt the business website and affect overall sales. This type of cyber attacks flood the business servers with numerous requests until they succumb to them and your website crashes

6. **Brute Force Attacks**

These attacks target ecommerce admin panel in order to figure out their password. It uses programs that establish a connection to website and use every possible combination to crack their password.

7. Trojan Horses

Trojan is a type of malicious code or software that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network. Admins and customers might have Trojan Horses downloaded on their systems. It is one amongst the worst network security threats. where attackers use these programs to swipe sensitive information from their computers with ease.

8. E-skimming

E-skimming refers to a method of stealing credit card information and personal data from debit or credit card payment processing pages on ecommerce sites. Hackers gain access to the site either via a successful phishing attempt, brute force attack, XSS, or third-party compromise, then capture in real time the payment information of shoppers when they enter into the checkout page.

9. Malware

Malware is a collective name for a number of malicious software variants, including viruses, ransomware and spyware. When a device or network gets infected with malware or ransomware, it may be locked out of all important data and systems.

Best Practices for Ecommerce Security

Security issues in ecommerce is one of the most attention demanding issue. It can not be overlooked by online businesses. In fact it should be a priority for most online businesses so that their customers are able to enjoy a smooth and safe shopping experience. Commerce security lets customers protect themselves from cyber-attacks and frauds. Followings are some of the ways and means to minimize cyber attacks :

1. Use Strong and unique passwords

As per the 2020 Verizon Data Breach Investigations Report, 37% of credential theft breaches used stolen or weak credentials. Hence, it becomes necessary to make sure that the business, their employees, and customers implement good practices for strong passwords. Strong passwords are at least eight characters and contain upper and lowercase letters, numbers and symbols.

2. Use Https websites

HTTP, which is short for HyperText Transfer Protocol, which is a set of rules for transferring a web page between a web server and your browser. When you browse to a specific URL in your browser, it starts a conversation with the website's server to download everything it needs to render that web page.Having an up-to-date SL certificate and HTTPS protocol has become the standard for businesses.The customers should be educated to use these sites.

3. Payment Gateway Security

While it may make processing payments more convenient, having credit card numbers stored on your database is a liability. It's nothing less than an open invitation for hackers where you put your brand's reputation and your customer's sensitive information on the line.

If you fall victim to a security breach, and hackers get their hands on credit card data, all you can do is to say goodbye to your business because the heavy fines will force you into bankruptcy.

When it comes to ecommerce recommendations, you must obtain a Payment Card Industry Data Security Standard (PCI DSS) accreditation.

4. Antivirus and Anti-Malware Software

Hackers can use stolen credit card information to place orders from anywhere in the world. An antivirus or an anti-fraud software can help with this serious ecommerce issue. They use sophisticated algorithms to flag any malicious transactions to help you can take further action. They provide a fraud risk score which can help proprietors determine if a certain transaction is legitimate.

5. Use Firewalls

Another effective ecommerce recommendation is to use firewall software and plugins that are pocket-friendly yet effective. They keep untrusted networks at bay and regulate traffic that enters and leaves your site. It offers selective permeability and only allows trusted traffic in. They also protect against cyber threats such as SQL injections and cross-site scripting.

6. Secure your website with SSL certificates

Secure sockets layer (SSL) certificates are files that link a key to transactions on different paths on a network. These certificates are associated with credit card details and transactions to regular queries. SSL certificates encrypt data to protect it from interception in between different destinations. The information you send from your end to the server is secure.

If you want to conduct any type of business on your site, you require SSL certificates, so that every process that takes place on your site is secure. Besides, it provides you with a certificate of ownership so hackers can't use your site as a counterfeit for phishing.

7. Employ Multi-Layer Security

You can fortify your security by using various layers of security. You can also use two-factor authentication to squeeze in an additional layer of security. Two-factor authorization requires a standard username and password combination as well as an extra code that is sent as an email to the user or as an SMS to their provided phone number. This ensures that only the user can access the service even if their username and password are at risk.

8. Backup Your Data

Data loss due to hardware malfunction or cyber-attacks is common. You should back up your data by yourself and not trust anyone else to do it for you. Employ automatic backup service so that even if you forget to do it manually, all your data will be backed up automatically. Another option is to choose a managed ecommerce web hosting service that automatically creates backups for you, like Cloudways.

9. Stay Updated

Regularly install security updates and patches as soon as they release because hackers can use bots that identify which websites use outdated software. That makes outdated software a serious liability.

10. Secure Ecommerce Platform

It is important to choose a secure ecommerce platform that regularly updates itself and offers top-notch security. Ecommerce platform tools safeguard you against common threats and frequently provide you with updates.

11. Train Your Staff Better

The staff should be made aware of laws and policies pertaining to the protection of user information. They should be educated not to share login credentials, and you should review the personnel who have access to sensitive customer information.

12. Educate Your Customers

You can solve these ecommerce security threats by educating your customers. Educate them about the risks associated with unsafe security practices. You can demand strong passwords and introduce them to how phishing works.

Strong passwords require a good combination of characters, symbols, and numbers that are near-impossible to brute-force or guess. You can also keep users away from creating profiles with weak passwords. You can also adopt the two-factor authentication system in case they are using weak passwords. Or if the user submitted information is sensitive and susceptible to hacking.

Conclusion

Developing good cyber security is crucial for the success of ecommerce. Organizations can't afford to lose their customers' trust by exposing their personal data.Therefore, the best approach is to spend on ecommerce security as much as the business does for its marketing or web design. It should be treated like an investment and not an expense.

References and Wibligraphy

1. https://www.cloudways.com/blog/ecommerce-security-tips/

2. https://cdn.ttgtmedia.com/search Security/downloads/29578C17.PDF

3. E-COMMERCE : AN INDIAN PERSPECTIVE, Sixth Edition,PHI Learning Pvt. Ltd., 01-Nov-2019 , Joseph P.T.,S.J.

4.https://us.sagepub.com/sites/default/files/upm-assets/9598_book_item_9598.pdf

5. https://www.bigcommerce.com/blog/ecommerce-website-security/#the-biggest-security-threats-to-your-ecommerce-site

6. V. Zwass, 'Structure and macro-level impacts of electronic commerce: from technological infrastructure to electronic marketplaces', http://www.mhhe. com/business/mis/zwass/ecpaper.html (accessed May 2001).

7. https://www.verizon.com/business/resources/reports/dbir/

8. https://vtldesign.com/web-strategy/what-is-https

9. Tavares, Joao, Mishra, Brojo, etl.(July 2018), Handbook of e-Business Security Publisher: CRC Press ISBN: 9781138571303

❑❑❑

23

Cyber Attacks and Cyber Security in the Indian banking industry

Dr. Amol Mane
HoD BBA and BBA (IB) Dept.,
MAEER's MIT Arts, Commerce and Science College, Alandi, Pune

****

Abstract:

Demonetization and corona pandemic has made the customers to make payments through online mode. Banks and customers are going digital. But this change in the banking habits is posing threats to the cyber security. Banks are increasingly updating their cyber system to protect it from the cyber attacks. But the cyber attackers are also coming up with new ways to hack the system and steal the important data of the banks.

The current paper focuses on different types of cyber attacks on banks, cyber security challenges faced by the Indian banks and the suggestions to face these challenges successfully. The study is based on the secondary data collected through websites, research papers, reports on cyber security etc.

Key words: Cyber security, Cyber threat, Indian banks, cyber attacks

Introduction:

Banking sector plays an important role in the development of any economy. It is the life blood of the economy. Customers' data is an important asset of the banks and every bank must take appropriate measures to protect it from the hackers. The development of IT and ICT in the Banking industry has created a great impact on the working of the banks but at the same time it has posed various cyber threats to the banks. The main problem and the challenge faced by the banks in the 21st century is the increase in the cyber crimes and cyber attacks. Cyber attacks on banks and financial institions hase increased spectacularly in recent times.

As per the records of Govt. of India, in 2020, over 2.9 lakh cyber security incidents related to digital banking were reported. According to Indian Computer Emergency Response Team (CERT-In), a total number of 1,59,761; 2,46,514 and 2,90,445 cyber security incidents pertaining to digital banking were reported during 2018, 2019 and 2020, respectively. These incidents included phishing attacks, network scanning and probing, viruses and website hacking etc. The customers and the banks are going digital which is giving rise to such cyber attacks. As the number of customers demanding online banking services is increasing, the mission of providing proper security and convenience becoming a challenge due to several blatant actors collectively referred to as "Cyber-Crime".

In simple words, "Cyber-Crime" is crime done with the help of a computer and an internet. Cyber crime incidents include but are not limited to denial of service, credit card fraud, e-money laundering, spoofing, ATM fraud, spamming identity theft and phishing.

Literature Review:

1. Kesharwani S. K., Sarkar M.P. and Oberoi S have done a study on growing threat of cyber crime in Indian banking sector. The study focuses on the technical aspects of the cyber crimes in the banking sector, cyber threats, challenges of cyber security faced by the banks. The study also explains the measures to be taken by the banks to strengthen the IT system and protect it from the cyber attacks.

2. Rao H.S. has done a research on cyber crime in banking sector. The paper explains different types of cyber crimes in banking sector, various reasons for cyber crimes, impact of cyber crime on banking sector etc. The attempt has also been made to study the hacking of official website of Govt. of Maharashtra, India's forst

ATM card fraud etc., as a case study. The researcher has also given suggestions for to prevent such cyber attacks on the banking and other sectors.

3. Acharya S., and Joshi S have done a study on Impact of Cyber Attacks on banking institutions in India: A study of safety mechanisms and preventive measures. The researchers have studies the impact of cyber crimes on the banking sector, cyber security measures taken by the banks to curb the impact of such cyber crimes, and the need to develop more strengthened cyber security system. The researcher has also presented case studies of cyber attacks on UBI and Cosmos Bank. The researchers have also suggested measures to protect the banking system from cyber attacks.

4. Neeta and Bakshi V.K. have done a study on Cyber crimes in banking sector. The study reflects the increasing use of e-banking in India. The study indicates different types of cyber crime such as hacking, credit card fraud, viruses, spyware, watering hole, DNS Cache positioning, malware based attacks etc. and its impact on banking sector. The authors have also given recommendations to prevent these attacks.

5. Simran, Manvikar A., Joshi V, Guru G have done a study on Cyber crimes – a growing threat to Indian banking sector. The study explains the operations of cybercrimes. The cyber crimes and frauds taken place in Indian banking sector and their detection has also been studies by the authors. The study has given the preventive measures to control the frauds in the banking sector. The study also suggested the use of Artificial Intelligence in detecting the cyber frauds. The researchers have also studied the cyber attacks on some in official website of Govt. of Maharashtra, UTI etc. The researchers have also given suggestions to prevent the cyber crimes in the Indian banking sector.

6. Manivannam A. and Moorthy D have done a study on Cyber attacks in the banking industry. The study shows the role of internet in cybercrime. Different types of cyber attacks, cyber crime cases happened in UK has also been discussed in the research paper. The study also explains the technologies like firewall, two factor authentication etc. to be used to prevent the cyber crimes in the banking industry.

OBJECTIVES OF THE STUDY:

1. To understand different types of cyber attacks on banks

2. To study the cyber security challenges faced by Indian banks

3. To give suggestion to address cyber security threats/challenges.

Need and importance of the study:

The Indian banks and their customers are going digital now-a-days. With the increase in digital transactions by the customers, the cyber attacks are also increasing day by day. The hackers are hacking the websites of the banks, stealing the customers' data, cloning the Debit and Credit Cards, transferring the amount from customers' account to some other accounts. The banking industry and the customers as well are falling pray to cyber threats. It is pertinent to study the cyber threats / challenges in the banks and to give suggestions to prevent such cyber threats. Hence, the researchers has decided to undertake the study on the topic **"Cyber Attacks and Cyber Security in the Indian banking industry"**

Research Methodology:

Present study is based on secondary data. The secondary data has been collected from various reports, research papers, articles, websites etc.

Limitations of the study:

The study is restricted to the cyber attacks and cyber security in Indian banking sector only.

The evolution of cyber attacks in the banking and financial sector:

1. 1971: Discovery of the first virus. It was general cyber attack.

2. 1988: The first "Denial of Service (DoS)" attack "The Morris Worm". It was general cyber attack.

3. 2005: 40 million card accounts of a US-based leading global payments company exposed in a security breach**.** It was directed cyber attack.

4. 2008: an international network hacking group hacked the website of a major US-based MNC bank and the bank has to lose millions of dollars to the hacking group. It was directed cyber attack.

5. 2010: ATM "Jackpotting": An employee of a US-based multinational investment bank installed a malware on the bank's 100 ATMs and stole around US$ 0.3 Mn in over seven months. It was directed cyber attack.

6. 2012: "Flame" the most complex and critical malware attack by the hackers. It was directed cyber attack.

7. 2016: India's major attacks: Nationalized bank - Indian bank's server was compromised by the hackers. It was directed cyber attack.

8. 2017: World's biggest ransomware attack - "WannaCry" and "Notpetya" cyber attack (costing almost US$ 10 billion): affected banks, card payment systems and ATM networks. It was directed cyber attack.

9. 2018: Cosmos Co-operative Bank - A Pune-based leading Co-operative bank had to lose alomst US$ 13.8 mn in cyber attacks. It was strategic cyber attack.

10. 2019: Hackers attacked the server of a Mumbaibased co-operative Indian bank and stole around US$ 0.1 mn. It was strategic cyber attack.

11. 2020: The COVID-19 outbreak and cyber attacks:

• Cyber attacks on Banks and financial institutions increased by 238% during Feb"Apr 2020.

• Indian banking industry and IT industry was attacked by the cyber attackers in the last week of June, 2020. Around 40,000 cyber attacks were attempted by the global hackers. It was strategic cyber attack.

Types of Cyber Attacks[1]:

1. Phishing:

Phishing attacks are meant for stealing user information, such as user credentials and credit card numbers and PINs to access bank account of the victim or take control of social network data.

2. Identity theft:

Type of cybercrime where hackers try to obtain key personal data such as social security no, Aadhar details, credit card or other related to impersonate someone and gain benefit with his/her name.

3. Virus and Trojans:

Viruses are nothing but price of malicious codes that replicate themselves like human virus without the help of human. Trojan virus is a destructive program which unlike viruses does not replicate themselves but spreads like high speed. These are activated by opening spam emails attachments.

4. Vishing:

It is the application of social engineering through telephone to gain access on private personal data from public for the purpose of ransom.

5. Cross side scripting:

Usually used for web applications. This enables attackers to inject client – side scripts into web pages viewed by users. This is used by attacker to bypass access controls.

6. Insider threat:

It is a malicious threat that comes from inside of any organization from people, employees themselves which exposes the system to attackers.

7. Botnet:

It is a type of cyber-attack where a network of private computers are infected with malicious codes and those computers are controlled by a group without the owners cognizance.

8. ATM/Debit/Credit card frauds:

In these kinds of frauds, the fraudster uses a skimming machine typically affixed with the keypad of ATM machine or POS machine such that it does not appear to naked eye. Whenever customer enters his card details along with PIN, details goes to the installed skimmer using which money can be theft.

9. DOS and DDOS: Denial of service (DOS) is a type of attack where the network or services are shut down denying access to service to concerned users. This is accomplished by sending excessive amount of information thereby spamming the network traffic at users end and hence denying legitimate users to access information. DDOS attacked are aimed at large profit organizations. Though this type of attack does not cause loss or theft of vital information, the damage requires lots of money and time to mitigate.

10. Ransom ware:

It is one of the most prominent threats of cyberspace. This is a type of malicious software designed to block access of a computer or a group of computers until a sum of money paid. They give threat to release sensitive data until a sum of money is paid to attackers. Maze is a common type of ransom ware attack.

Cyber Security challenges faced by Indian Banks[2]:

With the increase in online banking transactions, the Indian banks are facing lot of challenges so far as cyber security is concerned. The major cyber security challenges faced by Indian banks are as follows:

1. Application security: It includes tools and methods to protect applications after deployment by monitoring, resolving, and enhancing apps' security along with antivirus programmes, firewalls, and encryption.

2. Infrastructure security: It includes solutions to protect the corporate infrastructure, such as IT platforms, network communications, connected device, data centres etc.

3. Information/data security: It includes tools to protect private, confidential, and sensitive information or data from unauthorised access, misuse, damage, disclosure, modification, disruption etc.

4. Cloud security Tools: It includes application of security procedures and technology to secure cloud computing environment against both internal and external cyber attacks.

5. Identity and access management security: An architecture or security policies enforced to define and manage the roles and access privileges of individual network users, and protect critical and sensitive data.

6. Regulatory focus: to comply with the Reserve Bank of India guidelines on the cyber security framework that focuses on three different areas such as:

- Cyber security and resilience
- Cyber security Operations Centre (C-SOC)
- Cyber security Incident Reporting (CSIR)

7. End-user education: It involves educating bank employees on the importance of protecting sensitive information and security measures to avoid cyber attacks.

Suggestions to address Cyber Threats successfully[2]:

The banks and financial institutions are prone to cyber attacks. Hence, they must build a strong security threat monitoring system by implementing high-tech solutions. Following are the suggestions to the banks to mitigate cyber risks.

1. Prioritize cyber security evaluation:

Cyber criminals are the threats posed by them are dynamic and rapidly growing. The banks may not be prepared every time to prevent that. To protect the sensitive data and the information, banks will have to prioritize their efforts and make more investment in the essential cyber areas that matter a lot. There are various to do so i.e. by separating cyber security from IT/ICT solutions, breaking the value chain by identifying areas where susceptibility and risks are the highest. Banks will have to classify risks through inherent risk evaluation, evaluate the maturity levels of cyber buoyancy, and then focus on bridging the gaps, if any.

2. Securing remote access control:

Bandwidth controls are required to work distantly using remote access management solutions. This will require reviewing remote connectivity solutions and security governance; arranging advanced and strong authentication and authorization; and deciding on the span of services that require protected access. Similarly, digital workspaces and server-based computing, such as virtual desktop-interface, enable those employees who are working remotely to access data through a secured and encrypted connection.

3.Stiff access to third-party service providers:

Mobility restrictions and supply chain disruptions could compromise the security of the alliance partners and vendors that work with banks. By accessing the banking network and assets remotely, such services may also compromise banks' cyber security. Banks may have to prioritize access to and availability of services the other parties offer. This can be achieved by restricting or controlling their access to core infrastructure.

4. Outsourcing cyber security capabilities:

The demand for cyber security is continuously increasing. Banks are having shortages of talented workforce in this area. So, they can think of using new channels such as third party security provider to deal with these issues. If cyber security related work (such as security operations and insider threat detection) is outsourced the Contractors will be able to provide more efficient and leading-edge services.

5. Adopting sophisticated technology solutions and tools: Banks will have to create different layers of defense at different levels in the cyber security ecosystem. Some technology solutions and tools banks can adopt immediately are:

- Zero-trust architecture
- Advanced end-point security systems
- enhance cyber security with Artificial Intelligence etc.

6. Conducting training programs for the employees to create awareness:

Formal training programs should be organized by the banks on cyber security practices to make them aware about phishing, malware and other social engineering attacks. Training program should involve all the facets of cyber attacks and not just focusing on few aspects of cyber awareness. The banks should create the cyber security culture at every level and should regard it as a continuous process.

Conclusion:

To sustain the business during the corona pandemic and succeed thereafter the banks will have to adopt technologies such as cloud, remote access, and Internet of things (IoT). Increased use of such advanced technology and digitization will result in bigger cyber attack threats. The main focus of bank executives will be on achieving business goals while facing cyber security challenges. Banks and financial institutions will have to make huge investments in cyber security and cyber defense to create responsive and tough IT infrastructural facilities. This type of infrastructure will be able to address the present cyber security risks and prepare itself for future cyber threats and challenges. For this to happen the banks management has to come up with the strategies and initiatives and allocate necessary budget for the same. The top management of the banks can initiate such changes.

References:

1. Suman A, Joshi S., "Impact Of Cyber-Attacks On Banking Institutions In India: A Study Of Safety Mechanisms And Preventive Measures" Palarch's Journal Of Archaeology Of Egypt/Egyptology, Vol – 17 Issue 6, 2020, pp.

4656, 4670.

2. Deloitte Touche Tohmatsu Limited, UK, "Cybersecurity in the Indian banking industry: Part 1 - Will 2020 redefine the cybersecurity ecosystem?", November, 2020. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiRydGNwavxAhXE4zgGHQbxBesQFnoECAQQBQ&url=https%3A%2F%2Fwww2.deloitte.com%2Fcontent%2Fdam%2FDeloitte%2Fin%2FDocuments%2Frisk%2Fin-ra-cybersecurity-in-the-indian-banking-industry-noexp.pdf&usg=AOvVaw3Y6OKhbGzAUWwXEtkuZ7Lt

3. Kesharwani S. K., Sarkar M. P., Oberoi S., "Growing Threat of Cyber Crime in Indian Banking Sector", Cyber Nomics, Scholastic Seed, Vol. 1, Issue 04, Spet, 2019 pp. 19-22.

4. Rao H. S., "Cyber Crime in Banking Sector", International Journal of Research – Granthaalayah, Vol. 7, Issue 1, January, 2019, pp.148 – 161.

5. Neeta,Bakshi V. k., "Cyber Crimes in Banking Sector", Aayushi International Interdisciplinary Research Journal, Vol. 6, Issue 5, May, 2019 pp. 25-31.

6. Simran, Manvikar A., Joshi V. Guru J., Kiran S., "Cyber Crimes: A Growing Threat to Indian Banking Sector", International Journal of Engineering Technolgoy, Science and Research, Vol. 5, Issue 1, January, 2018, pp. 926-933.

7. (PDF) CYBER ATTACKS IN THE BANKING INDUSTRY (researchgate.net)

8. http://www.legalserviceindia.com/legal/article-3073-cyber-frauds-in-the-indian-banking-industry.html

9. https://m.rbi.org.in/Scripts/AnnualReportPublications.aspx?Id=1290

10.https://www.business-standard.com/article/finance/over-290-000-cyber-security-incidents-related-to-banking-reported-in-2020-121020401220_1.html

❑❑❑

24

Human based behaviour disorders due to Internet and its remedies

Dr.Bhagyashree S. Puntambekar
M.A.,M.Phil, Ph.D, HOD – Economics,
Rajarshi Chhatrapati Shahu College Kolhapur

****

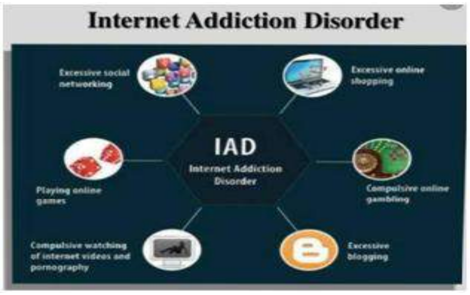
Introduction

In ancient time and Ancientdays, there weremediums for entertainment which werebinded with culture and tradition. But the trend of Internet and information entertainment network had seized all this customs. Though legal stimulating supply has been affected in the covid-19 pandemic, many of the illegal stimulating supplies are captured by the internet mad people by the network of Internet and dark web.

According to the reputed scientific magazine named 'neuron 'it is stated that this network has created a great dilemma in humans mind. Due to excess use of Information's networkmany of the people are affected badly. Their brain has affected on a high proportion. people are changing as per the addiction of internet. But are the changes permanent or temporary ? does this changes affects mind and work ? many of such questions are still unanswered.

Human behavioural disorders

1) Internet addiction disorder- regular increase in use of Information Network, no hesitation to waste time for it, compromises on a large scale with work, relations and health, much more anger if not gained, excitement, anxiety,unsuccessful efforts of using less internet.


Internet Addiction Disorder
Excessive social networking
Excessive online shopping
IAD
Internet Addiction Disorder
Playing online games
Compulsive online gambling
Compulsive watching of internet videos and pornography
Excessive blogging

2) Divorces due to net –Internet has caused parting of the marriages. Loneliness and distancing in relations due tounrestricted use of web. Ignoring each other's needs and giving priority to virtual world.

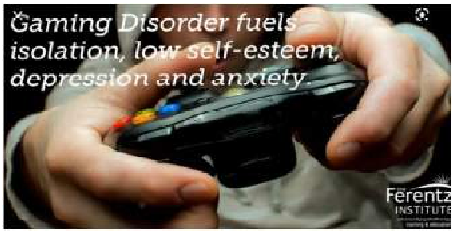
3) Online identity disorder–Confusion between identities inreal and virtual world, resulting in imagination,emotional outbreak, distancing in relations, real world living getting affected.

4) Eagerness for answer - frequently checking of messages and waiting for the replies. Destructive condition due to addiction of regular messaging., increasing depression and sadness anxiety and anger.

5) Dinging -Due to Powerful attraction towards virtual world spending some time in Real world gets difficult which causes mental suffocation and depression.

6) Selphitis - taking lots of photos in selfie mode and publishing them in the virtual world and expecting positive comments on it. Expecting the attention of lots of people.

7) Internet gaming disorder -there are many aspects of internet gaming disorder such as playing with another players with the help of Wi-Fi , strong desire to win the game or Break own score card. Due to this gaming, time, energy and mind power is wasted as well as work , relations and health come at a compromising position.


Gaming Disorder fuels isolation, low self-esteem, depression and anxiety.
Ferentz INSTITUTE

8) Communication addiction disorder (compulsive talking) Communication addiction disorder (CAD) is a supposed behavioural disorder related to the necessity of being in constant communication with other people, even when there is no practical necessity for such communication. CAD has been linked to Internet addiction.Users become addicted to the social elements of the Internet, such as Facebook and YouTube. Users become addicted to one-on-one or group communication in the form of social support, relationships, and entertainment. However, interference with these activities can result in conflict and guilt. This kind of addiction is called problematic social media use.Social network addiction is a dependence of people by connection, updating, and control of their and their friend's social network page. For some people, in fact, the only important thing is to have a lot of friends in the network regardless if they are offline or only virtual; this is particularly true for teenagers as a reinforcement of egos. Sometimes teenagers use social networks to show their idealized image to the others. However, other studies claim that people are using social networks to communicate their real personality and not to promote their idealized identity.

Risk factors

Interpersonal difficulties

It is argued that interpersonal difficulties such as introversion, social problems, and poor face-to-face communication skills often lead to internet addiction. Internet-based relationships offer a safe alternative for people with aforementioned difficulties to escape from the potential rejections and anxieties of interpersonal real-life contact.

Social support

Individuals who lack sufficient social connection and social support are found to run a higher risk of Internet addiction. They resort to virtual relationships and support to alleviate their loneliness. As a matter of fact, the most prevalent applications among Internet addicts are chat rooms, interactive games, instant messaging, or social media. Some empirical studies reveal that conflict between parents and children and not living with mother significantly associated with IA after one year. Protective factors such as quality communication between parents and children and positive youth development are demonstrated, in turn, to reduce the risk of IA.

Psychological factors

Prior addictive or psychiatric history are found to influence the likelihood of being addicted to the Internet. Some individuals with prior psychiatric problems such as depression and anxiety turn to compulsive behaviours to avoid the unpleasant emotions and situation of their psychiatric problems and regard being addicted to the Internet a safer alternative to substance addictive tendency. But it is generally unclear from existing research which is the cause and which is the effect partially due to the fact that comorbidity is common among Internet addicts. The most common co-morbidities that have been linked to IAD are major depression and attention deficit hyperactivity disorder (ADHD). The rate of ADHD and IAD associating is as high as 51.6%.

Internet addicts with no previous significant addictive or psychiatric history are argued to develop an addiction to some of the features of Internet use: anonymity, easy accessibility, and its interactive nature.

Other factors

Parental educational level, age at first use of the Internet, and the frequency of using social networking sites and gaming sites are found to be positively associated with excessive Internet use among adolescents in some European countries, as well as in the USA.

Remedies

Throughout 2014, around 420 million people were addicted to the internet. The American Psychiatric Association has also stated that kids of age 13-17 are almost online constantly. Such statistics show that internet addiction is getting more common and real day by day. If you find yourself or your loved one suffering with this, there are a few things that can be done to overcome it. Such as:

1. Admit it

The first step to solve any sort of problem is to step out of the denial phase and accept that you have a problem. This is you first victory towards becoming better. By verbalising that you have a problem, you become honest with yourself and it brings clarity to the whole situation. Also, it makes you realise how unhealthy the use of internet is for you.

2. Seek Therapy

Now that you have admitted that you have a problem, why not do something about it? You can ask a reliable friend to help you with this or you can seek professional therapy. You will be able to communicate about the emotions that trigger you to go online again and again. When you share these things with someone else, it helps in opening up and then you can also set some goals with them about the behaviour which will keep you in cheque.

3. Limit the Smartphone use

Digital Detox is something you can do on your own if you have the determination and strength to do it. Once you realise that internet addiction is bad for you and it taking control over your life, you can start keeping the distance. You can limit your online session to 30 minutes. You can make some rules about not using the internet after a certain time every day. This will keep you all managed and self-controlled.

4. Socialise

Get over the internet and share some real life experiences. Invite over your friends and have some fun activities with them. Go out more frequently and make your loved ones your priority. Spend time with them, do what you love, and try to maintain your real life relationships more than your internet relationships.

5. Change Communication Patterns

When you are texting your friend all day through your phone, change the pattern, and meet them to talk to them directly face-to-face. Same way, if you are addicted to online games, you can replace them with outdoor games. Or, you can go to video games stores and play there with your friends to keep your hands off your computer and consoles.

6. Follow a Routine

A routine makes you more organised and managed. If you have been living the life abruptly without any routine, you need to change that. Time management is the key to resolve internet addiction issues. You need to make a timetable and make time for several other things along with using internet. This way the urge to cheque on your phone after every short interval will be removed. You can select a time for internet usage as well but it will be the part of the routine.

7. Prioritise your Needs

Focus on the things you want to get done first. It depends on what you do and how you do it. For instance, if you are a student, you can decide on finishing the homework first when you come at home and doing everything later.

Similarly, if you are a businessman, you can prioritise your meetings, your schedules, first and then everything including the internet usage later. This way, you will see how internet addiction was making you miss out the things that are important in your life.

8. Keep Devices Inaccessible

If things are getting out of control and you find yourself getting more addictive day by day. You can take some serious steps by getting rid of your digital devices for a fixed time period, especially the ones bothering you a lot. It could be your gaming console, your smartphone, laptop, etc. You can ask for help from a friend and let him keep your things for a while to keep the necessary space.

9. Find Activities outside

There are many things you can do without the use of computer or smart devices. You can take part in sports team, volunteering programmes, civic groups, and further such communities to feel worthy and spend your quality time.

10. Know the Cause

Why are you so much addicted to the internet ? Is it because you feel so lonely? Or you have nobody to share your emotions with? Or you seek social approval? These are the possible reasons of using internet too much. Find out your reason and sort out a way to resolve it. Once you know the feelings that lead you to the unnecessary use of the internet, you might be able to resolve those issues on your own.

Conclusion

Using these tips can be proven very beneficial when you are willing to get yourself out of this mess. To avoid falling into internet addiction again and again, make sure you know how to control yourself once you realise that you are getting addicted to it. Keeping your eyes and mind open is a good way of staying alert and healthy.

References

Internet articles
Newspaper articles

❑❑❑

25

Cyber Security in Business Management

Mr. Bhairawanath D. Jadhav
Head,
Department of Commerce & Management,
Dahiwadi College Dahiwadi,
Tal-Man, Dist- Satara

****

Introduction

Cyber Securityplayvital role in the field of informationtechnology.Securing the information have become one of the biggest challenges in this digital era. Whenever we think about the cyber security the first thing that comes to our mind is 'cyber crimes' which are increasing immensely day by day. Governments and various companies are taking many measures in order to prevent these cybercrimes. Besides various measures cyber security is still a very big concern to many. This paper mainly focuses on role playing by cyber security in business management. It also focuses on current know how of the cyber security techniques, ethics and the trends changing the face of cyber security.

A well-developed cybersecurity strategy keeps the operational wheels of business rolling.And also, it promotes innovation as well as customer trust - both are essential for continued growth. Today, every business which is based on computer system is required very powerful control system for governing the business activities properly. So, that cybersecurity is very important tool for controlling and protecting the data from theft, damage and hacking. Many people think that cyber security means the software and monitoring that protect their operating system, network, emailand printing devices from malicious attack or data theft. True, this is a large and important part of cyber security for business.Cyberattacks damage the business reputation and trust of customers, this in turn the loss of customers and loss of sales.

The Importance of Cyber Security

Today,Effective cybersecurity is needed to enhance product integrity,operations, customer experience, brand reputation,regulatory compliance,and investor confidence.The business landscape is becoming more interdependent. Business strategies are therefore concentrated on widening and deepening links to resources outside the firm.Competitive advantage is no longer the sum of all efficiencies, but rather the sum of all connections. So, every Company's need to manage a complex ecosystem of stakeholders: partners, customers, investors, and suppliers. Partners for their network must be selected with governance and fiduciary processes that are aligned with their own. If one link is broken anywhere in the ecosystem, the others will weaken too, and business will suffer. It is important to update the cybersecurity technologies that assess behaviour in order to identify potential problems before they can cause harmful to the business operations.

Challenges of Cyber Security

Every organization needs to coordinate its efforts throughout its entire information system byeffective cyber security.

Elements of Cyber Security

Applicationsecurity: Applications require constant updates and testing to ensure these programs are secure from attacks.

Data security: Inside of networks and applications is data. Protecting company and customer information is a separate layer of security.

Network security: The process of protecting the network from unwanted users, attacks and intrusions.

Endpoint security: Remote access is a necessary part of business, but can also be a weak point for data. Endpoint security is the process of protecting remote access to a company's network.

Database and infrastructure security: Everything in a network involves databases and physical equipment. Protecting these devices is equally important.

Cloud security: Many files are in digital environments or "the cloud". Protecting data in a 100% online environment presents a large number of challenges.

Mobile security: Cell phones and tablets involve virtually every type of security challenge in and of themselves.

Identity management: Essentially, this is a process of understanding the access every individual has in an organization.

Disaster recovery/business continuity planning: In the event of a breach, natural disaster or other event data must be protected and business must go on. For this, you'll need a plan.End-user education: Users may be employees accessing the network or customers logging on to a company app. Educating good habits (password changes, 2-factor authentication, etc.) is an important part of cybersecurity.

Conclusion

Today's world of Internet of Things, there are few competitive advantages more critical than trustand excellence in cybersecurity is a distinguishing factor. Therefore, business activities are becoming ever more interconnected. Digital transformation has created an environment of increasingly intensive competition.The key enables for digitization involve big data, cloud, mobility, and collaboration. Security needs to be embedded in the entire business ecosystem. Such systemrequires sufficient speed and volume of data required by daily transactions, while being able to handle the complexity and multiplicity of threats in a digital world.A company needs to strike the right balance between innovation and risk, while developing new products and services.Cybersecurity cannot be guaranteed, but a timely and appropriate reaction can. In brief, to compete and win in today's technology-driven world, companies need to get cybersecurity right.

References: -

https://www.sbir.gov/sites/all/themes/sbir/dawnbreaker/img/documents/Course10-Tutorial1.pdf

https://www.ntt.co.jp/topics_e/CfBE2018/img/201803_Business_Management_and_Cybersecurity.pdf (ntt.co.jp)

cyber security business strategy - Google Search

Cybersecurity As a Business Strategy - Corporate Board Member

(PDF) A Study of Cyber Security Challenges and Its Emerging Trends on Latest Technologies (researchgate.net)

Cyber-Security Policy Decisions in Small Businesses (waldenu.edu)

Small to Medium Enterprise Cyber Security Awareness: An Initial Survey of Western Australian Business

❑❑❑

26

An assessment of cyber security awareness among the college students

Prof. Dr.Premchand Gundu Gaikwad
Head of the Department (History),
RayatShikshan Sanstha's Arts and Commerce College, Madha, District Solapur

****

Abstract – Now a days, every individual depends on the Internet. It has increased the use of electronic gadgets like mobile phone, Laptop, Computers etc. in the day-to-day life, but it has also increased the threat of cybercrimes. In the society the young people are involved in the committing of cybercrime and young people are become victim of cybercrimes due to lack of awareness about cybercrimes and cyber security. young college students are mostly involved in the technological advance and are exposed to cybercrimes. Through this survey-based study paper an attempt has been made to focused on the habits of college students about utilization of social media, precautionative cyber security measures followed by them, their awareness about cyber laws and rules, factors of cyber security management etc.

Key words – cyber security awareness, college student, cybercrimes.

I) Introduction – It is proved that, social media, Internet are very helpful for collecting information on various matters and also useful in storing our data. Now social media /Internet are become an integralpart of our daily life. But on the other hand due to tremendous increase in utilizing modern technology and allied electronic gadget it become very difficult in keeping our private information safe and secure. Information Technology (IT) has moved from a hobby of people with interest in technology to a socially accepted factor that most of us utilise it on daily basis. More dependence on IT has brought a risk for a society as well as individuals, which has clearly surfaced with the increasing incidents in cybercrimes. The abuse of social media, Internet has enhanced new age crimes which are addressed by the Information Technology Act 2000. It is observed that majority of the Internet users are not having proper knowledge of managing social media and are not aware about cyber security as well as cybercrimes. It is also on the basis of many studies; general people are not aware of the proper precautionary measures to overcome the problem of cybercriome3s. implemented cyber laws and rules are also proved as ineffective and has faced many problems tacking the problem of cybercrimes. This study intends to focuse on the awareness of college students about cyber crimes cyber security and cyber laws rules etc.

II) literature Review –

1) A. Shrihari and P. S. Jayashree, (2008), have conducted a study to understand the awareness level of cybercrimes and cyber security measures among the college students in Kochi. Through the study authors have also analysed the awareness among students about the government schemes/programmes to overcome the problems of cybercrimes. Through the study author has focused on the variousprecautions taken by the college students in Kochi.

2) Jigar Shah, (2016), has attempted to explain conceptual model on how to uphold and implement the awareness programmes among the youth regarding cyber security. Author has suggested that, government should organise more awareness programmes and campaigns in various places where the potential net users are in the huge number. Through the study author has found that there is a lack of awareness among youth in case of cyber security measures.

3) Partap Sing Rathod and A. B. Potadar, (2019), have conducted a survey study to analyse the awareness of medical students in the area of cybercrimes and cyber security. Through the study authors have focused on the awareness among the medical student regarding secure website, usage of antivirus, frequency in changing password sharing of password etc. through the study authors have observed that, majority of the students are having good awareness about the cyber security measures.

4) A. K. Mokha, (2017), has attempted to analyzed the awareness of cybercrimes and cyber security measures among the young Internetusers. Through the study author has also examined the relationship between educational level of young people and the awareness of cybercrimes and security; and also examined the relationship between various age groups of respondents and their awareness about cybercrimes and security.

III) Importance of the study – Increasing trend of using social media Internet in Indian young people is not unique. There are several studies which are focused only on the issues like habits of youth in using social media platforms, its adverse impacts on their psychological and health conditions, victimization of cybercrimes etc. but there are very few studies related to assessing awareness among youth about the cybercrimes and cyber security. On this background such type of study is important because it provides the facts about the awareness among youth about cybercrimes and cyber security.

IV) Objectives – 1) To focus on the habits of college students regarding using internet.

2) To understand the perception of college students regarding various cybercrimes.

3) To know about the awareness of college students about the factors of cyber security management.

4) To focus on the precautions, take by the college students with a view of cyber security.

5) To understand the opinion of college students about the barriers in the implementation of cyber security measures to prevent cybercrimes.

6) To understand the opinion of college students about the effectiveness of existing cyber laws and rules as a cyber security measure.

V) Research Methodology– The present study is descriptive in nature. It is based on quantitale and qualitative research analysis. Primary information has collected through interview schedule prepared for college students primary information analyzed with the help of percentile method secondary information collected through study papers articles published in national and international jo0urnals.

VI) Selection of sample – Sample population of 150 college students has been selected through convenient sampling method. The sample population consists of 78 male students and 72 female students.

VII) Geographical Area of the study – The geographical area of the study confined to Pune city only.

VIII) Results and Discussion –

Table No. 1

Age wise and sex wise distribution of the respondents

Age group (years)	Male	Female	Total
18 to 20	27 (18%)	24 (16%)	51 (34%)
20n to 22	38 (25%)	36 (24%)	74 (48%)
Above 22	13 (9%)	12 (8%)	25(17%)
Total	78 (52%)	72 (48%)	150 (100%)

Sample population of the study has consist of 52% male and 48% female respondents. 34% respondents are in the age group of 18 years to 20 years (18% male and 16% female) whereas, 49% respondents are in the age group of 20 years to 22 years (25% male and 24% female). In total 17% of the respondents are above 22 years of age (9% male and 8% female). The proportion of made and female respondents is almost equal in total.

Table No. 2 (A)

Duration of using social network (daily)

Duration	Frequency	Percentage
Less than 1 hour	22	15%
1 hour	41	27%
2 hours to 3 hours	87	58%
Total	150	100%

Table No. 2 (B)

Social media in frequent use (daily)

Duration	Frequency	Percentage
Whats App	14	9%
Facebook	17	11%
You Tube	23	15%
Instagram	18	12%
Internet (Googal)	21	14%
Games	04	3%
All the above	53	36%
Total	150	100%

According to the information provided by the respondents it is observed that majority of the respondents (58%) are spending 2 hours to 3 hours daily to use social network sites. 27% respondents have stated that they are using only 1 hour for exploring social network sites and only 15% respondents are spending less than 1 hour daily for exploring various social network sites for various purposes. It shows that very few of the respondents stay without exploring social network for short duration of time. It indicates the increasing rate of social network addiction among young generation.

A question has been asked to the respondents with a view to know whether they are aware about the various cyber crimes or not. The following table presents the fact in this regard.

Table No. 3

Awareness of the respondents about various cyber crimes

Particulars	Frequency	Percentage
Individual cyber crimes	23	15%
Government cyber crimes	15	10%
Property related cyber crimes	26	17%
All the above	86	58%
Total	150	100%

As per the collected information it is observed that 15% respondents aware about or having knowledge of individual related cyber crimes such as Harassment through e-mail, cyber stalking, cyber bullying, obscene material, cyber defamation, morphing etc. 10% respondents are having knowledge of government related cybercrimes such as – cyber terrorism, cyber warfare, distribution of pirated softwares, etc. where as 17% of the respondents are having awareness about the property related cybercrimes such as – crimes against intellectual property, cyber trespass, computer forgery, cybersquatting, hacking computer system etc. Majority of the respondents have stated that they have good knowledge or awareness about all the above-mentioned types of cybercrimes. The following table presents the facts about the autnessamong college students about the various factors of cyber security management.

Table No. 4

Awareness of the respondents about the factors of cyber security management

Particulars	Frequency	Percentage
Knowledge of cyber security	17	11%
Knowledge of cyber security counter measures	08	5%
Knowledge of password management	24	16%
Knowledge of browser security	13	9%
All the above	88	59%
Total	150	100%

As per the information provided by the respondents it is found that, 11% of them are having the knowledge or have good awareness regarding cyber security, 5% respondents are having awareness and knowledge about cyber security counter measures. 16% respondents are aware about the password management and only 9% of the respondents are aware about the browser security. Majority of the respondents (59%) have stated that they are having good knowledge and awareness about all the above stated factors of cyber security management.

From the study point of view, it is also important to know about the various precautionative measures adopted by the college students with a view to cyber security. The following table presented the facts in this regard.

Table No. 5

Various precautionative measures of cyber security adopted by the respondents

Particulars	Frequency	Percentage
Frequent changes in password	12	8%
Restrictions on social relationships	08	5%
Using of anti-virus software	14	9%
Avoid to exposing of personal information	19	17%
Avoid unknown friendship requests/ web sites	17	11%
All the above	80	53%
Total	150	100%

From the above table it is revealed that 8% of the respondents are frequently changing their password as a precuationative measure for cyber security, while 5% of the respondents have themselves restricted their social relationships with unknown persons with a view to keep cyber security. 9% respondents have stated that they are using anti-virus softwares and 17% have stated that, they are avoide to expose their personal information on social media. 11% respondents have stated that, they are avoide to accept friendship requests by unknown person and also avoide to explore unknown websites. Majority of the respondents (53%) have stated that they have adopted all the above mentioned percutionative measures for cyber security.

Table No. 6

Barriers in the implementation of cybers security measures (Opinions of the respondents)

Particulars	Frequency	Percentage
Legislative inadequacy	16	11%
Ambiguity in definition	12	8%
Lack of awareness among people	20	13%
Jurisdictional problems/issues	04	3%
Lack of techno savvy personnel	21	14%
Dynamic nature of cybercrimes	03	2%
All the above	74	49%
Total	150	100%

The above table dipited the opinions of the respondents about the barriers in the implementation of cyber security measures. In the opinion of 11% respondents, inadequacy of legislations and rules pertaining to the cybercri9mes are the major barrier in the effective implementation of the cyber security measures. According to the 8% respondents various definitions included in the legislation or laws are not proper, there is a ambiguity in these definitions which caused for ineffective implementation of cyber security measures in India. Lack of awareness among the social network users is also one of the major barriers stated by 13% respondents. In the opinion of 3% respondents, issues pertaining to jurisdiction is the major barrier in the proper implementation of cyber security measures. Lack of techno savvy personnel is the major barrier, opined by 14% respondents. Only 2% respondents have opined that, dynamic nature of cybercrime or frequent changes in the modes operandi of cyber offenders creates major barrier in the proper implementation of cyber security measures. In the opinion of 49% respondents all the above-mentioned barriers are equally responsible for ineffective implementation of cyber security measures.

The following table presents the opinion of the respondents regarding the effectiveness of existing cyber laws and rules.

Table No. 7

Effectiveness of existing cyber laws and rules as a cyber security measure

Particulars	Frequency	Percentage
Very effective	69	46%
Not much effective	57	38%
Cannot say	27	18%
Total	150	100%

46% respondents have opined that, the existing cyber laws and rules are very effective, the laws and rules are having effectiveness with a view to prevent cybercrimes. On the contrary

38% respondents have opined that the existing cyber laws and rules are not much effective because there is no any specific provision to protect security of women and children; and there is also some ambiguity in the concepts included in the cyber laws and rules, only 18% of the respondents have not expressed their opinion in this context, because they have not proper and deep knowledge about the cyber laws and rules.

IX) Findings of the study –

i) As per the collected primary information, majority of the respondents are in the age group of 20 years to 22 years. The proportion of male and female respondents is almost equal.

ii) It is found that, majority of the respondents spends 2 to 3 hours daily for exploring various websites, chatting on WhatsApp, browsing, playing games etc. It indicates the increasing rate of social media addiction among youth.

iii) As per the information provided by the respondents, it is found that, majority of them are having good awareness about various types of cyber crimes like cybercrimes related to intellectual property, cybercrimes against women, cybersquatting, hacking etc.

iv) On the basis of collected information, it is found that, majority of the respondents are having good knowledge and awareness about cyber security management, such as knowledge of password management, knowledge of browser security and overall awareness about cyber security measures.

v) It is found that, majority of the respondents are taking various precautions while they are using social media, Internet etc. Majority of them are taking precautionative measures like changes in passwords, using of antivirus software, retractation on social relationship etc.

vi) It is observed that, almost all the respondents are having good knowledge pertaining to the various barriers occurs in the proper implantation of cyber security measures. All the respondents are knowing the various types of these barriers.

vii) Majority of the respondents are positively opined about the effectiveness of existing cyber legislative measures, rules and regulation some of the respondents (18%) have not positively or negatively responded in this regard, due tolack of knowledge about various cyber laws and rules.

X) Suggestions–

1) There is a need of imparting education to the students right from the school level regarding cybercrimes, danger of cybercrime, cyber security measures etc.

2) There should be arrangement of workshops, or orientation programmesthrough the NGOs regarding cyber security management.

3) There should be arrangement of awareness campaigns by the government in the various venues of the districtscities in the states.

4) There is a need of strengthening cyber laws, rules and regulations with a view to bring a sense of security among the youth specially among the female Internet users.

5) The cyber cells must block all the websites which are potentially harm the young generation.

6) The cyber cell must provide support and relief to the victims of cybercrimes.

7) The Internet user should install instruction detection software to get warning about any breach, cybercrimes.

References

1) Shrihari A and P. S. Jayashree, (2018), “A study of awareness of cybercrime among college students: With special reference to kochi International Journal of pure and Applied mathematics, Vol. 119, No. 16.

2) Jigar Shah, (2016), “A study of awareness about cyber laws for Indian youth,” International Journal of Trend in scientific Research and development, Vol. 1, No. 1.

3) Pratap Sing Rathod, and A. B. Potdar,

(2019), “Study of awareness of cyber security among medical students,” Indian Journal of Forensic Medicine and Toxicdogy, Vol. 13, No. 1.

4) W. Alhohani and N. Elfadil, (2020), “Measuring cyber security awareness of students: A case study of Fahad Bin Sultan University,” International Journal of Computer science and mobile computing, Vol. 9, No. 6.

5) A. K. Mokha, (2017), “A study on awareness of cybercrime and security,” Research Journal of Humanities and social sciences,” Vo.8, No. 4.

6) Aparna Chauhan, (2012), “Preventing cybercrime: A study regarding awareness of cybercrime in Tricity,” International Journal of Enterprise Computing and business systems, Vol. 2, No. 1.

7) V. N. Agarwal, (2015), “General awareness on cybercrime,” International Journal of Advanced Research in Computer science and software engineering, Vol. 5, No. 2.

❑❑❑

27

Women Activism and Gender Paritiesin Post-Modern Indian Writing in English

Mr. Sandeep K. Sanap
Associate Professor, Department of English,
Modern College of Arts, Science and
Commerce Ganeshkhind, Pune

****

Abstract

A number of movements and approaches have been aroused in post-modern India in regard to Gender Studies. Feminism, Gender Studies and Women Studies are the epitomesof women activism for gender parities and women empowerment. Woman activism could be one more example of studying women’srights inFeminism and Gender Studies paradigm keenly. The present research aims to state the women activism is a new area of study which gives details of women’s fight against the suppression and efforts to acquire equal rights in the society. This paper also tries to state the selected women’s writing in post-modern India as an apt reflection of women activism. This study revisits the writing of eminent women writers; Baby Kambleand Bama from the perspective of women activism which has not been explored in an in-depth manner so far. The Researcher has also tried to shed some light on the journey of feministmovement which transformed its nature several times and has become the debatable topic in the literary sphere. The birth of women activism is a result of feminism which started long back in western literature.

The attempt has been made in this paper to justify the writing of Bama and Baby Kamble as a women activism in literaturewhich

encourages people to take into account the women's suppression.

Key words: Activism, Feminism, post-modern, suppression, Gender studies, women studies.

Study of woman from the perspective of oppression and discrimination has been started long ago. The equal rights and parities in all spheres of society and emancipation from gender discrimination have been studied globally. The commentary and counter commentary has been delivered by various thinkers and feminist writers. The long discussion on woman and on fundamental rights of woman have been considered as the feminism. This movement started back in around 18th century. The foundation of movement which was grounded in the male writer John Stuart Mill and Frederick Engels' writing for women enfranchisementThe Subjugation of Women in 1884 and The Origin of the Family, Private Property and the Statein 1869 respectively.Until these writers, no articulation came in by women nor by men. Later on, after Simon De Beauvoir'sThe Second Sex, women's problems started to be taken into consideration in more effective ways. Beauvoir's attempt was an attentive commentary on women. Afterwards numerous writers contributed internationally to the feminism:The Feminine Mystic by Betty Friedan in 1963, Thinking about Women in 1968, to cite some of them. These writings in early phase on women represented the women suppression and very much spoke about the fundamental rights of women in the society. This literature on women attempted to shed some light on awareness of self-respect and equality of women in the society. Later,the 18th and the 19th century witnessed transformation of feminism where we can see the major writings of women on fear, anxiety and painful struggle ofacquiring equality in the male dominant society.

Feminism is a wider term in which several ideas and concepts have been emerged. Under this major term the different feminine aspects can be studied according to Julia **Krestiva. She explains:**

Women demand the equal access to the symbolic order - liberal feminism. 2. Women reject the male symbolic order in the name of difference- radical feminism. Femininity extolled. 3. Women rejectthe dichotomy between masculine and feminine as metaphysical (Thorat.pp.234-235).

The whole movement shifted several times but the founding idea of women's fundamental rights and gender equality in the society remained constant in all phases and types of feminism across the world. The result of this movement lead the new coming writers of women issues to contribute actively against women oppression and gender disparities.

This present research is an attempt to set up the notion that the writings of women in Indian writing in English isawoman activism in literature to acquire the parities in the male dominant society. For example, Baby Kamble's Prison We Broke and Bama's Sangati has been taken to justify the woman activism in Indian literature.Among the countless writings and speeches on women suppression in the 21st century,their writings can be considered as women activism for gender parities.Activism is a political term used long back in 920s to denote the political actions during the First World War

Activism At the end of the First World War, activism (in German Aktivismus) denoted active political commitment or engagement among and by intellectuals. Historically it is closely associated with expressionism (q.v.), and as far as drama was concerned it required realistic solutions to social problems. It is particularly associated with Kurt Hiller, who organized the Neuer Club for expressionist poets, and with the magazine Aktion, founded in 1911 by Franz Pfempfert. Now, activism is predominantly a political term. (Dictionary of Literary Terms and Literary Theory. p.9)

From literary perspective the term itself conveys the expectation of social and political change and counters the social problems. According to Online Oxford Learners Dictionary the definition of activism is:

The activity of working to achieve political or social change, especially as a member of an organization with particular aims.

(https://www.oxfordlearners dictionaries.com/definition/english/activism?q =activism+)

The primaryaim of any writer in the literary sphere is to reflect the society withits issues and possible solutions. With this aim, the selected writers Bama and Baby Kamble kept the woman activism going on.Bothof these writers are quite popular for their writing on the downtroddengroup of society. They have successfully portrayed the authentic picture of the life of underprivileged women and their awareness of the women issues is more touching realistic and authentic. Bama's Sangati and Baby Kamble's Prison We Broke are attempts to shed light on self- assertion. They could successfully put forth the pathetic life of women through their writings. Women are a crucial factor of the society who suffers because of the gender discrimination. They have been always kept in ignorance and secondary place. In the male dominant society they rarely find themselves at the right place. They always have been measured by certain criteria by the male dominated society.They have been taught not to speak against injusticebut acceptwhatever they getin their lives. They are even prohibited from participating in the family discussions. But writers like Baby Kamble and Bama have continuously taken efforts to speak against the gender disparities and women disrespect.

Baby Kamble was born and brought up in a countryside village where she found hardly any opportunity for women as a human being. Her family was fairly educated and result of which she got an opportunity to speak up openly against women's oppression. She is very much inspired by Dr. Babasaheb Ambedkar and witnessed Ambedkari movement and social changes. Because of her writing, her name is considered among the eminent writers in India.Through her autobiographical novel, she succeeded in giving the voice to thousands of women who live pathetic life. Similarly, Bama Faustina Soosairaj popularly known as Bama is another persona of eminent women writers in India who broke out for women's suppression. She is aTamil writer who has written several books on women as well as her own community. Sangati is one of her best efforts in which she has successfully portrayed her own life experience and tried to give a voice to the doubly discriminated women.Her Sangatiis a very deep commentary on violence, abuses and molestation of women. Both of these writers took great efforts to make the women aware about their fundamental rights and self-assertion. By picturizing their own life experiences they tried to help other women to achieve a place in the society. The grief they both expressed in their autobiographies is reasonably similar.

We were imprisoned in dark cells, our hands and feet bound by the chain of slavery. (kamble.43)

In the life of women the virtual prison still exists which binds the women by the shackles of slavery. Right from their home, women have been made slaves by their own family members. Families never allow to take women their own decisions nor permit them to participate in important familial discussions. She has been under canonical view all the time in family as well as in society, and always restricted to never live like freewoman. Since long back woman has to obey men. Baby Kamble exhibits this same pathos in her Prison we Broke.

My father locked up my aai in his house, like a bird in a cage. (kamble.5)

Baby Kamble is trying to raise the questions as to why her mother wastreated like a prisoner.Why didn't she defy the maltreatment given to her by her own family members? Women are like birds in cage, whenever men want to release them or lock them depends on their whims. Women should not be prohibited from living freely. They should get all the freedom in the society; they should not be a puppet whose control is in the hands of men. The ill-treatment women receive from men results in estimating themselves as an important personage. They have been taught for generations not to snapback against ignorance and suppression due to their weaknesses. Bama states the women's fear and expressing frustration about themselves being as weak and poor.

My mother said, 'But what can we poor women do? (Sangati. P.104)

This limited mindsets of women is a result of conservative mind of the society.But asan answer to her mother's question Bama's reply is:

But generation by generation we must start thinking for ourselves, taking decisions and daring to act……we must sharpen our minds and learn to live with self-respect.(Sangati.p.104)

Bama here is trying to say that whatever we have faced in the past as a womanshould be changed somewhere. Women should think positively and learn to oppose the discrimination made against her. Women are the subjects of discrimination, always underestimated and placed at secondary position in the society. Although the modern woman is capable of taking the responsibility and live life on her own it is meaningless until she faces the discrimination by the men and society. Her fight against gender disparities is still going on. In one of her interviews, while stating the women's condition, Kamble says:

…women are still slaves. And it is not just Dalit women; I see around me many women from both upper and lower castes. All women are facing problems. Especially women from villages! Their operation doesn't come to light. All cases of the rape are suppressed for fear of family honor, pressures from the dominant communities and political parties. Women works very hard and yet face so many problems…. (kamble.p.154)

The condition of women has not been changed so far, they used to face the gender disparities in the past and it's still going on even in 21st century. Forms of sufferings like cases of domestic violence, rapes and honor killings are still going on. The crime against women is heavily increasing day by day. Nirbhaya rape case and Hathras case are the epitomes which show that woman are not safe and suffer a lot in the modern world. Baby Kamble not only speaks about Dalit women in her autobiography but also depicts women as a community, whether they are from Dalit or upper caste. Women of both the castes are suffering and getting humiliatedbecause of their gender. Baby Kamble conveys that Dalit woman is doubly discriminated by the society. Further, she says that women from villages are the core victims of such gender inequalities. As a woman Kamble is trying to convince that women have been considered as the commodities ofsociety, they never get the desirable place in the society. Their work and dedication to the family is never valued. Similarly,Bama's commentaryon issues of inequality also leaves similar effect on the reader's mind she quotes:

The women, in any case, whatever work they did, they were paid less. Even in the matter of tying the firewood bundles, the boys always got five or six rupees more. (Sangati.p.18)

Women always work harder than men, right from the household things to the professional duty. If so, why do women have to face such kind of inequality? They do several things for their families without expecting anything in return. But at the professional level, as Bama points out, the daily wages women get their value (money) hugely less than the men. Although women are doing men's jobs still they arerejected financial benefits which men get easily. Society imposes extra responsibilities on women. If a woman is working professionally, she is not only bound to only her professional duty, but also has to dothe entire household things after coming home from the office. However, working men never peep into the household things after their office work. It's the male dominant mindset which encourages such types of inequalities in the society and makes women do all the duties.

Bama further states about her moral learning what she has received from her mother:

My mother told me that in our village, they didn't make any differences between boys and girls at birth. But as they raised them, they were more concerned about the boys than the girls. (Sangati.p.3)

Bama depicts the reality of society by stating the above facts. Whatever her mother told her in her childhood about gender parities, she found different in existing life. Girls' gender doesn't matter when they are young but when they grow up they get ignored by their own family. Girls realize that the special attention is offered only to the boys.

Writing such issues in her autobiography Bama tries to make people realize the pain of women whoreceive very less attention because of their gender. Bama also tries to raise the questions such as why such gender disparities take place in the society. When is this going to change? And who is going to change it? Bama and Kamble's griefis same. Both have tried to demonstrate the women who are suffering from all types of discriminations and suppression just because of their gender. Theyjust not only raised the questions and left without any answer but they spoke out about the possible solutions for the betterment of women. Bama and Kamble consciously and actively spoke about the reformsthat can be brought in to improve women's pathetic conditions. Writing of these women became the role model and aframework for the rest of women to get self-respect in the society. Their work helped a lot to make people conscious about gender discrimination which still they are facing. For the sake of awareness in rest of women in India they convey:

I made a firm resolve at a young age, to lead my life according to the path sketched by Dr. Baba Saheb Ambedkar, the light of my life. His principles have exercised a strong influence on me. (kamble.p.115)

Similarly, Bama directs women:

We should educate boys and girls alike, showings no difference them as they grow into adults. We should give the freedom we give our boys. (Sangati.p.123)

Education is the key solution to break the shackles of slavery which has bound women for long. Only through education women can overcome slavery and gender disparities. Bama suggests educating their boys and girls alike would be one more step to change the notion of gender disparities. Parents should offer equal treatment to girls and boys. Bama asserts that only education can make aware the rest of women to get self-respect and equal rights in the society. Here, Bama tries to highlight the importance of education.

Kamble is very much motivated by Dr. Ambedkar's thoughts and principles towards women emancipation and empowerment. Dr. Ambedkar fought for women to bring remarkable change in their life by putting the HinduCode Billin the Parliament House. Taking into cognizance the contribution of Dr. Ambedkar, Kamble suggests to the whole women community to be aware about their fundamental rights and gender parities in the society.

Prison we Broke andSangatiarethe autobiographies of hope. Both thesewriters have expressed their hopes for women emancipation. Bama leaves a very optimistic note regarding gender parities in her Sangati.

Then there will come a day when men and women will live as one, with no difference between them; with equal rights.(Sangati.123) Bama's whole writing, especially Sangati succeeds in making a remarkable move in women activism in the society. More or less Bama and Kamble, both of them have succeeded in giving the direction to the women activism through their writings.

Conclusion:

Writing and speaking openly on women's discrimination is an attempt of showing women activism through literature. Bama and Kamble have included a number of pathetic life experiences in their writings which show pain, discrimination and slavery.This can be considered as a representation of women's life. Such attempts by the women writers and dissemination of self-assertion through their literary work could also be recognized as women activism. Taking into consideration the huge and apt portrayal of women'ssuppression, discrimination, ignoranceand gender differences is another form of feminism which is a powerful assertion of the 'women activism' in Indian writing in English.

REFERENCES

· Abedi Z. Contemporary Dalit Literature: Quest for Liberation. Arise Publishers and Distributors, New Delhi, 2010.

· Anand S. "The Caste System in India". The Power of Culture Archives, April 2006. www.powerofculture.ni/en/current/2006/april/castesystem.html 22/05/2015

· Ashok, Thorat. A Spectrum of Literary Criticism, Noida, Frank Bros. & Co. (Publisher) Ltd, 2010. Print.

· Avinash Sangolkar (2010), Dalit Literature: Emergence and Development, Pratima Publication, Pune

· Bama. Sangati (Events).Oxford University Press, New Delhi, 2009.Print.

· Bagul, Baburao. Presidential Address. Second Maharashtra Buddha Sammelan. Mahad. Dt. 13, 14 February, 1971

· Chavan, Dilip. "Emergence of Dalit Literature in Translation: Towards a Critical Theory." Nation with Discrimination: Literary Voices from the Subalterns. Ed. Arvind Nawale. New Delhi, India: Access, 2011.p. 162. Print.

· Cuddon.J.A, Dictionary of Literary Terms and Literary Theory, Revi.Habib.M.A.R, London, Penguin BooksLtd, 2013.Print.

· Dangle, Arjun. "Dalit Literature: Past, Present and Future" Poisoned Bread - Translations from Modern Marathi Dalit Literature. Ed. Arjun Dangle. Hydrabad, India: Orient Longman, 1992. 235-36. Print.

· Derrida, Jacques. Of Grammatology. Trans. Gayatri Chakravorty Spivak. John Hopkins UP, Baltimore, 1976.

· Dr. Nanda Meshram (2006), Dalit Novels: A Criticism, Dimple Publication, Thane. Dumont, Louis. Homo Hierarchicus: The Caste System and its Implication. University of Chicago Press, Chicago, 1980.p.3. Print.

· Foucault, Michel. 'Two Lectures', in C. Gorden (ed.) Power/Knowledge, Brighten: Harvester, p. 98. Print.

· Ghurye, G. S. Caste and Race in India. Bombay: Popular Prakashan, 1969.P. 06, Print.

· Gramsci, Antonio. Selections from the Prison Notebooks of Antonio Gramsci. Trans. and ed. Quintin Hoare and Geoffrey Nowell Smith. Orient Longman, Chennai, 2004.

· Gupta, Dipankar (ed), Social Stratification. Delhi: Oxford University Press, 1991, p.29, Print.

· Jafrelot, Christophe. Dr. Ambedkar and Untouchability, Delhi, India: Permanent Black. 2005. P. 21 Print.

· Janardhan Waghmare (2002), The Quest for Black Identity, Sugava Publication, Pune

· Jayarama, V. "Hinduism and Caste System". Hinduism, Jainism, Sikhism, Zoroastrianism and Other Resources. http:/www.hindu website.com/Hinduism/hcaste.asp 20 May, 2015

· Kamble, Baby.2009.The prison we broke, Tran. Maya Pandit. Jina Amucha. New Delhi: Orient Blackswan.

· Kumar, Raj. Dalit Personal Narratives: Reading Caste, Nation and Identity. Hydrabad : Orient Black Swan, 2012, P.116.Print.

· Lillard G. Richard, American Life in Autobiographies, Stanford University Press, Standford, 1956, p.1.Print.

· Limbale, Sharankumar. The Outcaste (Akkarmashi)Tr. Santosh Bhoomkar.. New Delhi: Oxford University Press, 2003. Print.

· Naik. D.G. Art of Autobiography, Poona: Vidarbh Marathwada Book Company, 1962 p. 14. Print.

· Nimbalkar, Waman. Dalit Literature: Nature and Role, Nagpur : Pratibha Prakashan, 2006, p. 137. Print.

· Pantavne, Gangadhar. Sahitya: Prakurti Ani Pravrutti. Aurangadad : Swarup Prakashan. 1999. Print.

· Pascal, Roy. Design and Truth of Autobiography, London: Rutledge Pub., 1960, p.12, Print.

· Phadke, Y. D. (Ed.) Mahatma Phule Samagra Wangmaya, Mumbai: Maharashtra State Board of Literature and Culture, 1991. Print.

· Porter J. H. Caste in India. American Anthropologist, Vol. 8, No. 1 (Jan., 1895), P. 24 URL: http:/www.jstore.org/stable658439

· Salunke, A. H. Manusmrutichya Samarthakanchi Sanskriti. Satara, India: Lokwangmaygraha, ed. 6, 2006. P. 3 Print.

· Singh M. K. Ambedkar on Caste and Untouchability. New Delhi, India: Rajat Publications, 2008. P. 135. Print.

· Spivak, Gayatri Chakravorty. "A Literary Representation of the Subaltern: A Woman's Text from the Third World", In Other Worlds: Essays in Cultural Politics. Methuen, New York, 1987.pp.241 – 268.

· Spivak, Gayatri Chakravorty. "Can the Subaltern Speak?" Marxism and the Interpretation of Culture. Ed. Cary Nelson and Lawrence Grossberge. London: Macmillan, 1988. pp.271 – 313.

· Spivak, Gayatri Chakravorty. "French Feminism in an International Frame", In Other Worlds: Essays in Cultural Politics. Methuen, New York, 1987. pp.134 – 153.

· Suraj Yengde (2018): Dalit Cinema, South Asia: Journal of South Asian Studies, DOI: 10.1080/00856401.2018.1471848

· Yengde Suraj, Caste Matters, Penguin Random House India, 2019, India

· Saones, Catherine. Compact Oxford English Dictionary. New York: Oxford University Press Inc. 2001. P. 691. Print.

Webliography:

· https://www.oxfordlearnersdictionaries.com/definition/english/activism?q=activism+

❑❑❑

28

Study of Population Aspects in Solapur District 1961-2001

Dr. S. D. Shinde
Asst. Professor, Department of Geography,
S.K. Mahavidyalaya, Shirwal

Dr. A. V. Pore
Asst. Professor, Department of Geography,
Chhatrapati Shivaji College, Satara

****

ABSTRACT

Population is the main resource for the regional development by representing man-power. In this context Population aspects needs to study. In this paper investigate population aspects like growth rate, density, sex ratio, literacy, rural-urban population, of the study area for the year 2001. Solapur district is located in the western part of the Maharashtra state. It lies between $17^0$10’ north to $18^0$32’north latitude and $74^0$42’east to $75^0$15’east longitude. For the present study data has been collected from Census Handbooks, Socio-Economic Abstract of Solapur District. The rural-urban difference in the population characteristics of the study area is also considerable.

INTRODUCTION

Human resource development is the key to the development of other resources. Only if human resources are developed can other resources on earth be developed. This requires sustainable development of human resources. The study of growth rate, density, sex ratio, literacy, rural-urban populations is the very important because they are pushing the human resource development.

Where there is a favorable natural environment for human life, the population density is high and the adverse natural conditions are low. Population distribution in the world is unequal and different so population characteristics differ from place to place.

OBJECTIVES

To study the selected population characteristics of Solapur District with spatial and temporal perspectives.

STUDY AREA

Solapur District situated in the western part of the Maharashtra state which has been selected for the present study. It lies between 17^0 10’north to 18^0 32’north latitudes and 74^0 42’ east to 76^0 15’ east longitudes. It is administratively sub-divided into 11 tahsils (Fig. 1). It is bounded by Ahmednagar on the north, Osmaanabad on north-east, Gulbarga district from Karnataka state on east-south, Sangli district on the south-west and Pune and Satara on the west side. It covers an area of 14895 sq km. and supports population of 3849543 (258 parsons in per.sq.km). Solapur District is situated entirely in Bhima, Nira, Sina, and Man river basins in south-west Maharashtra. The area comparing 1150 inhabited villages and 10 urban centres and 31.83 percent population live in the urban areas while remaining 68.17 percent live in the rural sector (2001).

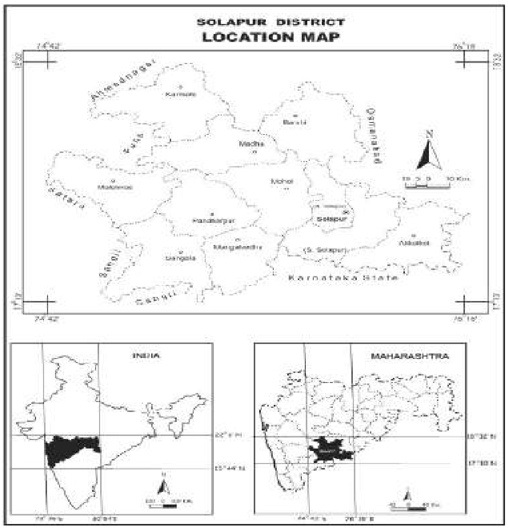


Fig. 1

DATABASE AND METHODOLOGY

For the analysis of existing condition of the various aspects of Population characteristics, related data and information has been collected from secondary sources.

The secondary sources of the data mainly includes Census of India's District Census Handbooks Solapur District, 1961-2001, Town Directory, 2001 etc. The published reports like Socio-economic Review and District Stastical Abstract, Solapur District, 2010, Gazetteer of Solapur District and other governmental reports etc. are also the sources of data in the present investigation.

The collected data have been arranged in tabular form and processed by employing various quantitative techniques. The processed data have been depicted in the form of tables, graphs, diagrams, maps, photo plates etc.

POPULATION CHARACTERISTICS

Population selected aspects like growth rate, density, sex ratio, literacy and rural-urban population etc. needs to study. Population is the main resource for the regional development by representing manpower. The different aspects of population have been assessed as an influencing element on urban phenomena of urban centres of the study area.

Growth Rate

In the study area, 21.17 per cent growth rate of population of decade 1961-71 has been observed. It decreased in 1981, increased in 1991 and again decreased up to 19.14 per cent in 2001 (Table 1 & Fig 3 A). So for as decade 1991-2001 is concern, the growth rate of population was low in Akkalkot tahsil (10.33%) and high in Pandharpur tahsil i.e. 26.90 per cent. It has considerable rural and urban difference (Table 2 & Fig 4 A).

Table: 1

Solapur District: Temporal Changes in Major Population
Aspects, 1961-2001

Population Characteristic	Year	1961	1971	1981	1991	2001
Growth Rate (%)	Total	-	21.17	15.81	23.79	19.14
	Rural	-	22.16	12.54	24.90	14.02
	Urban	-	18.60	24.48	21.11	31.82
Literacy Rate (%)	Total	25.15	33.90	40.67	56.4	71.25
	Rural	19.20	28.20	34.90	34.87	68.26
	Urban	40.60	49.10	54.60	54.36	77.51
Sex Ratio (Females/1000 Males)	Total	933	942	934	935	935
	Rural	945	940	946	930	925
	Urban	914	914	931	945	957

Source: District Census Handbooks, Solapur District, 1961-2001.

Density

Land and people reckoned as the two vital elements, their ratio is taken to be an indispensable consideration in all population studies (Akhilesh Kumar Mishra, Prabuddh Kumar Mishra, 2018). Density of population in the study area found 258 people per sq. km in 2001. In the study area, urban density is high than the rural density. The highest density has been observed in North Solapur tahsil i.e. 1288 person sq. km and the lowest density observed in Karmala tahsil i.e. 145 person per sq km. The spatial variation in density can be grouped in following groups (Table 2 and Fig. 2).

Very high density observed in Solapur North and Pandharpur tahsils which is above the average of study area. These two tahsils are developed in industry and agriculture due to rich water and soil resources.

High density of population is observed in Barshi, Malshiras and Akkalkot tahsil during 200-300 people per sq km. Barshi and Akalkot tahsils have one and three urban centres respectively. Malshiras tahsil developed in agro-based industry.

Moderate density (175-300 people per sq km) found in Madha, Mohal and Sangola tahsils. They are agriculturally developed also agro-based industries and good accessibility are also observed in these tahsils.

Low density of population has been observed in the three tahsils viz. Karmala, Mangalvedha and South Solapur. These tahsils have comparatively low development in agriculture and industry. Though pedolgical condition is good in this part but low rainfall and drought porn nature become barrier in agricultural development.

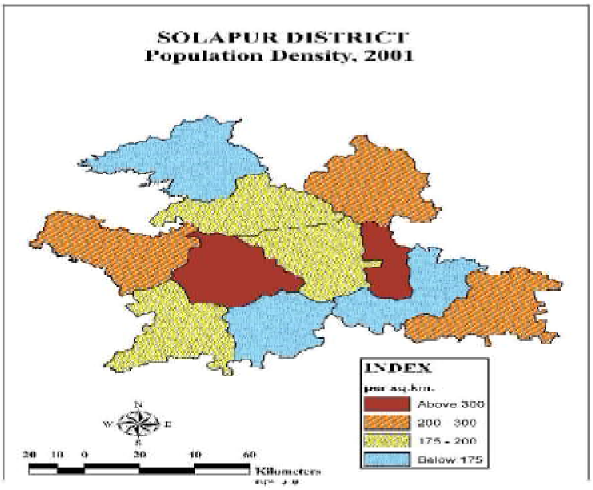


Fig. 2

Table: 2

Solapur District: Spatial Changes in Major Population Aspects, 2001

Sr. No.	Tahsil	T/R/U	Popul-ation	Growth Rate	Sex Ratio	Density	Literacy
		Unit ?	No.	%	(Females/ 1000 Males)	Per sq. km.	%
1.	Karmala	**T**	**233316**	**19.90**	**929**	**145**	**68.66**
		R	211388	20.74	924	132	67.22
		U	21928	12.32	934	4626	82.34
2.	Madha	**T**	**292611**	**16.96**	**928**	**189**	**70.14**
		R	269834	18.05	920	175	68.95
		U	22777	5.48	936	3515	83.81
3.	Barshi	**T**	**340831**	**12.80**	**943**	**230**	**74.09**
		R	236046	10.64	921	163	70.76
		U	104785	17.99	946	2890	81.49
4.	North Solapur	**T**	**960803**	**22.49**	**944**	**1288**	**76.09**
		R	88325	-45.98	925	156	69.38
		U	872478	40.53	962	4886	76.76
5.	Mohol	**T**	**252526**	**24.46**	**920**	**179**	**69.54**
		R	252526	24.46	920	179	69.54
		U	0	0.00	0	0	0.00
6.	Pandharpur	**T**	**402707**	**26.90**	**923**	**309**	**69.78**
		R	311328	31.12	912	242	66.36
		U	91379	14.36	933	5288	80.99
7.	Malshiras	**T**	**422600**	**20.62**	**923**	**278**	**71.67**
		R	422600	20.62	923	278	71.67
		U	0	0.00	0	0	0.00
8.	Sangola	**T**	**272077**	**18.17**	**934**	**175**	**66.28**
		R	243961	16.51	937	165	64.87
		U	28116	34.81	930	409	78.52
9.	Mangalve-dha	**T**	**171261**	**15.02**	**922**	**150**	**66.67**
		R	149555	15.72	915	131	65.07
		U	21706	10.42	929	17365	77.46
10.	South Solapur	**T**	**210774**	**12.62**	**933**	**176**	**67.37**
		R	210774	12.62	933	176	67.37
		U	0	0.00	0	0	0.00
11.	Akkalkot	**T**	**290037**	**10.33**	**961**	**209**	**67.74**
		R	227922	11.41	946	165	66.67
		U	62115	6.55	975	7843	71.63
Solapur District		**T**	**3849543**	**19.14**	**935**	**258**	**71.25**
		R	2624259	14.02	925	180	68.26
		U	1225284	31.82	957	3813	77.51

Source: District Census Handbooks, Solapur District, 1961-2001.

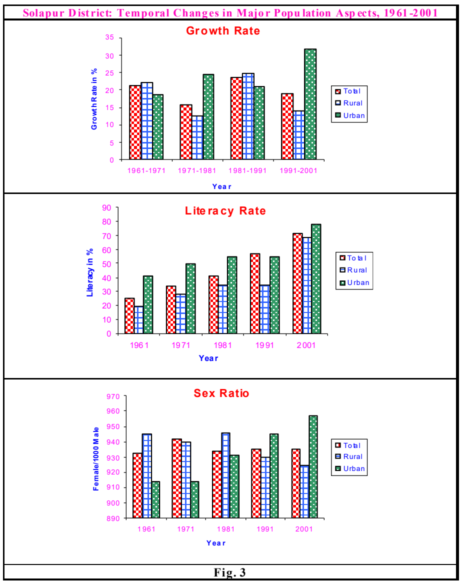


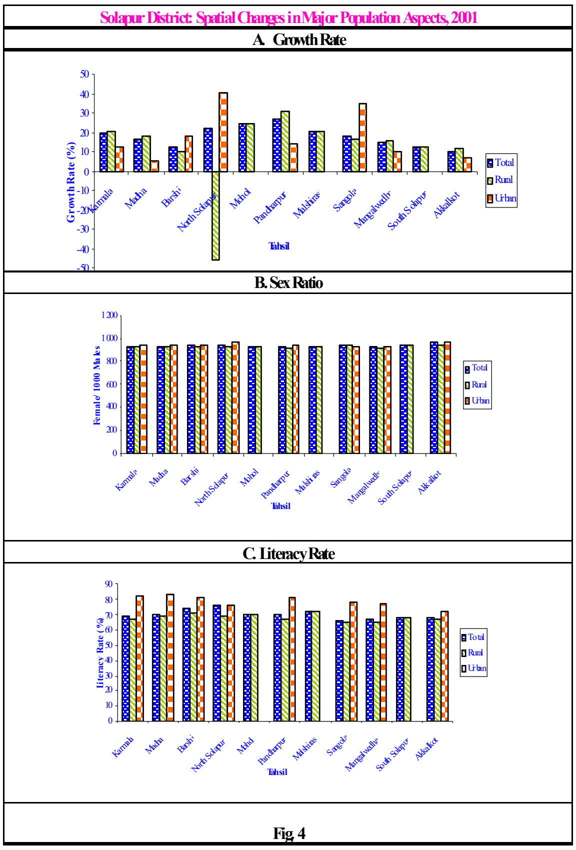
Fig. 3

Sex Ratio

Sex ratio is a useful indicator to understand women's health and position in any society (Mankari, et.al. 2011). The sex ratio of the study area is 935 in 2001. The number of female per 1000 male population has different form tahsil to tahsil in the study area. The sex ratio of the study area was 933 in 1961, which increased by only 2 up to 2001 and become 935. In the study area sex ratio found high in Akkalkot (961) and low in Mohol (920) tahsil. Population of Mohol tahsil is migrating from out of the tahsils. Interestingly found high sex ratio urban area than the rural (Table 2 and Fig 4 B).

Literacy

Literacy is reliable index of socio-economic development (Ramotra, 2008), but it has both spatial and social exclusion which needs to be study (Pore and Mote, 2010). In 1961 the literacy rate of study area was 25.15 per cent which constantly increased and become 71.25 per cent in 2001. Study area has 71.25 per cent literacy rate (2001) which is low than state (76.90%). North Solapur tahsil has high literacy in the study area i.e. 76.09 per cent. Barshi (74.09%) Malshiras (71.67%) have literacy rate above the average literacy rate. In Karmala, Madha, Mohol, Sangola, Mangalvedha, South Solapur and Akkalkot tahsils low literacy has been observed. (Table 2 and Fig 4 C).


Solapur District: Spatial Changes in Major Population Aspects, 2001

A. Growth Rate

B. Sex Ratio

C. Literacy Rate

Fig 4

CONCLUSION

Different demographic variables experiences both spatial and temporal changes due to the various factors. The growth rate of population, generally decreasing from last four decades, where sex ratio slightly increased and the literacy rate of the study area experiences steady increase. High density of population and literacy observed in developed tahsils where as low density and found in the tahsils like Karmala, Sangola and South Solapur. The rural-urban difference in the population characteristics of the study area is also considerable.

REFERENCES

Akhilesh Kumar Mishra, Prabuddh Kumar Mishra. (2018): "Spatio-temporal Analysis of Demographic Characteristics: A Case Study of Samastipur District, India. American Research Journal Of Humanities and Social Sciences, vol 4, no. 1, pp. 1-14.

Census of India (1961-2001): Maharashtra Solapur District Census Handbook.

Government of Maharashtra (1984): Maharashtra State Gazeteers, Solapur District.

Mankari, M. P, Rathod, H. B, Kulkarni, M. J and Kankure, K. B. (2011): "A Demographical Over-View of Latur District in Maharashtra," Maharashtra Bhugolshtra Sanshodhan Patrica, Vol. XXVIII, No. 2, pp. 75-80.

Pore, A. V. and Mote, Y. S. (2010): "A Study of Hierarchical Exclusion in terms of Literacy in Kolhapur District", The Goa Geographer, Vol. VII, No. I, pp. 59-65.

Ramotra, K. C. (2008): "Development Processes and the Scheduled Castes", Rawat Publication, Jaipur.

Socio-economic Review and District Stastical Abstract, Solapur District, 2010

❑❑❑

29

STUDY OFONLINE EXAMINATION AND IMPACT OF WEB CAMERA ON STUDENTS

DR. RAVINDRA S. NETAWATE
HEAD DEPARTMENT OF COMMERCE,
D.G.RUPAREL COLLEGE OF ARTS, SCIENCE &
COMMERCE COLLEGE MAHIM, MUMBAI

****

ABSTRACTS –The technology has given the birth of new inventions, in this covid situation , the communication and its means was going at a meager, we must agree here, that the covid has stopped the space of development but it has not vanished the business process, the human being overcome on it by using the technology, the colleges and schools have adopted the online examinations of the students through the technology, the means were available and the colleges have implemented it without causing any harmful effects on students and teachers. The students have saved their educational development only due to Computer technology. In online examination web cameras control the cybercrime. It monitors the student's examination but the authenticity of this web camera is unanswered.

Introduction-

The digital technology has played an important role in the Corona Virus situation, India is the most victim country in this pandemic more than three lacks people have lost, many of them find difficulty after curing from the diseases, but the pandemic has taught the big lesson to the whole world and man has found the different solutions for living life. As before this the exams were taking physically in the classes where the Peon, teachers, students, were required but in this situation , many schools, colleges and the universities have taken its exams through the digital technology.

In this exam process , the monitoring to the students was challenging job , but the web camera has solved this problem , before starting the camera , the students cannot start its exam, he couldn't have the chance to make the malpractices, such as copy, using extra internet sources, or taking assistance of any other, The question is remained that the passing ratio,and percentage of marks have been increased tremendously , hoe its happened, therefore we ask some questions to the students of P.G.

Review of Literature-

According to V.Chingath A.Jamina(2021 Feb.) Pointed out that the cybercrimes occurred in commercial sector, 60% cybercrimes happen in commerce which is dangerous to business community, hence the businessman should use the cyber security instruments.

According to Annamals Laxmanan (2015) The cyber criminals attack to exploits less develop country due to weak security control &then use this exploitationto target more developed country.

Objectives of the Study-

1. To study the role of digital technology in online examination

2. To find out the Problem of Digital technology.

3. To study the Merits of Digital technology.

4. To give the suggestions to the problem of online examination.

Origin of the Problem-

When colleges find difficulty in Classroom examination, then they find the need of web camera. when online exams started, for the smooth flow of exams, to monitor to the students was a herculean tasks for the college authority, but web camera has made it easy, that's why, many colleges have adopted the web camera technology in online examination.

Research Methodology-

Research Methodology- Descriptive research methodology has been used to check the validity of the problem.

Data Collection-

a. The Primary data collected from the post graduates students of Commerce and the arts students of IDOL. We have selected hundred students and through, mobile calling we have asked them questions about role of web camera, during online examinations.

b. The secondary data is collected from the journal, newspapers, and Research thesis on digital technology.

c. Sampling Techniques- Random sampling technique has been used to collect the, original information of given problem.

d. Tools & Techniques- To analyze the data Chi-square technique has been used, The tables, diagram has been used to aware the exact research problem. F-test has been used.

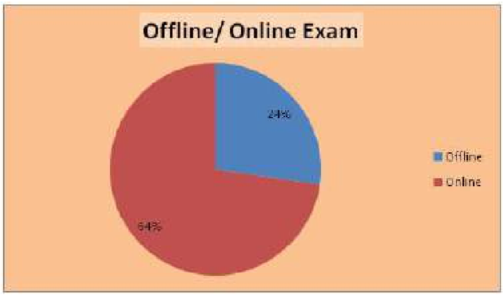
Interpretations of Data –

To find the validity of the given problem, we have made the survey on telephone and asked questions to the students.

1. Do you like online / offline examination?

Sr.No.	Offline	Online
1.	24%	64%

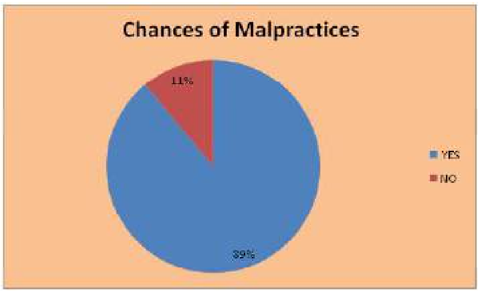
The above table is indicated that 64% percent students like the online examination during Pandemic situation.



2. Is there anychances of Malpractices

Sr. No.	YES	NO
1.	89 %	11%

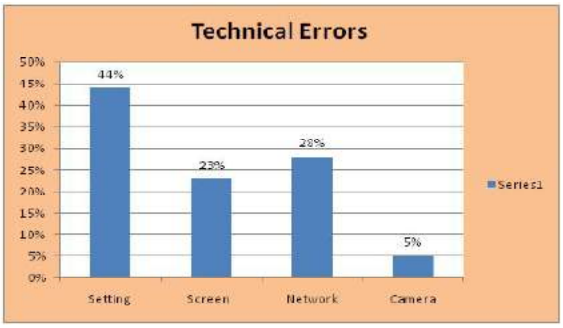
When students asked about chances of malpractices 89% students saidthat there is a chances of malpractices.



3. Do you find technical errors during examination?

Sr. No.	Setting	Screen	Network	Camera
1.	44%	23%	28%	05%

The above table indicated that there are numbers of technical errors, 44% students facing the problem of Device setting, 23% get the problem of Screen , which is not visible or bluer, 28% students get the problem of network issue like power supply, range etc. and 05% students face camera adjusting problem.



Findings-

1. The online exam is useful in this pandemic situation.

2. There is more chances of malpractices, students can search the answers from Google.

3. They can keep someone else back or horizontal directions of the cameras.

4. The only images can be captured hence, more chances of malpractices.

5. Irregular class students like these examination.

6. Easy source of passing to the students.

7. Web camera's couldn't function effec-

tively.

8. If power supply went out , difficulty face by the students.

9. No chances of revaluation / verification.

10. Helpdesk facilities is very poor , no one response immediately.

11. Many private agencies have been conducted online examination, no confidentiality is maintained.

Suggestions-;

1. In pandemic, online examination is good for the safety of the students..

2. This is a temporary solution but in future offline examinations should have been conducted.

3. No private agencies should have been involved in online examination only college authority should conduct such examination.

4. Powerful internet facilities require.

5. Students financial condition need to be verified before conducting such examination.

6. If technical errors would have been occurred, student must get a chance of reexamination.

7. This styles of examination could adverse effects on the employment of the teachers and the intellectual development of the students, hence it should not continue for the longer period.

Conclusion-

The above study indicated that, during Pandemic, such examination is required from the point of view students safety, The technology has more improved ,as it has prose at the same time there is a cons, we cannot judge the knowledge of students properly. The above discussion indicates us that for long terms and from the future of the students, examinations should be conducted by not online but offline.

Bibliography-:

1.Abdullah H.(2013) The Role of ICT In teaching Science education in Schools, Journal of Education & Social Science.

2. Gartica D. &Mcnair (2015) Students perception in to teaching Learning Process. American journal of Information System Vol.3, issue no.2 Pg. 40-44.

4. WWW.Legal service of India.com/legal

5. WWW.financial express.com.

6. S.R.. Bhansali, The information Technology Act. Publisher, University Law building 2016.

❑❑❑

30

Science Technology And Cyber Security

Ms. Dr. S. M. Sayyad
Lecturer, Head Of Department,
Department of Hindi, B.C. Vita

****

ABSTRACT:

Cyber Security plays an important role in the field of information technology.

Securing the information have become one of the biggest challenges in the present day. When ever we think about the cyber security the first thing that comes to our mind is ‘cyber crimes’ which are increasing immensely day by day. Various Governments and companies are taking many measures in order to prevent these cyber crimes. Besides various measures cyber security is still a very big concern to many. This paper mainly focuses on challenges faced by cyber security on the latest technologies .It also focuses on latest about the cyber security techniques, ethics and the trends changing the face of cyber security.

INTRODUCTION:

Today man is able to send and receive any form of data may be an e-mail or an audio or video just by the click of a button but did he ever think how securely his data id being transmitted or sent to the other person safely without any leakage of information?? The answer lies in cyber security. Today Internet is the fastest growing infrastructure in every day life. In today’s technical environment many latest technologies are changing the face of the man kind. But due to these emerging technologies we are unable to safeguard our private information in a very effective way and hence these days cyber crimes are increasing day by day. Hence cyber security has become a latest issue. The scope of cyber security is not just limited to securing the information in IT industry but also to various other fields like cyber space etc.

What is Cybercrime or e-crime?

Cybercrime or e-crimes are offenses that are committed against individuals or groups with a criminal motive of intentionally harming the reputation of the victim, causing physical or mental harm, and cause loss of money or information directly or indirectly by using the Internet and electronic devices

Beginning and growth of e-crimes:

This section indicatesseveral general trends, since 1960s, about how e-crimes began and grew. The summary is as follows:

- In the early decades of modern information technology (IT), computer crimes were largely committed by unsatisfied individuals and dishonest employees.
- Physical damage to computer systems was a prominent threat until the 1980s (Sterling, 1992).
- Criminals often used authorized access to subvert security systems as they modified data for financial gain or destroyed data for revenge (Louw C., Von Solms S., 2014).
- Early attacks on telecommunications systems in the 1960s led to sabotage of the long distance phone systems for amusement and for theft of services (Kabay, 2008).
- As telecommunications technology spread throughout the IT world, people with criminal tendencies learned to penetrate systems and networks for amusement (Kenefick, 2008).
- Programmers in the 1980s began writing malicious software, including selfreplicating programs, to interfere with personal computers (Kabay, 2008).
- As the Internet increased access to increasing numbers of systems worldwide, criminals used unauthorized access to poorly protected systems for sabotage, political action and

financial gain (Erbschloe, 2004).

- As the 1990s progressed, financial crime using penetration and destabilization of computer systems increased (Sterling, 1992).
- The types of malware shifted during the 1990s, taking advantage of new vulnerabilities as operating systems were strengthened, only to give way to new attack routes (Kenefick, 2008).
- Illegal applications of e-mail grew rapidly from the mid-1990s onward, generating plenty of unwanted commercial and fraudulent emails (Hussainat M., 2013).
- Social networking has become an increasingly important tool for cyber criminals to recruit people to assist their money laundering operations around the globe (Erbschloe, 2004).
- Global mobile devices' penetration—from smart phones to tablet PCs—accessing the Internet by 2013 surpassed 1 billion, creating more opportunities for cybercrime.

Cyber Stalking :

Cyber stalking is defined as using the internet or other electronic means with a view to harass or threaten any individual, group of individuals, or an organization. It includes monitoring, false accusations, identity theft, making threats, damage to data or equipment, the request of minors for sex, or gathering information that may be used to threaten or harass (Bhatt S. & Pant D., 2011).Three ways of cyber stalking. Cyber stalking categories Email Stalking Send e-mails to user for harassment and extortion. In some cases send viruses to intimidate the user.

Internet Stalking Takes on public through internet such as a chat room, social network, and Web sites by sending personal data, pictures, and video to several locations to meet their demand, which is often physical. Computer Stalking Computer-to-computer connection, the activities of stalker is working through the Internet and the Windows operating system in order to assume control over the computer of the targeted victim. The defensive option for the victim is to get disconnected and reassign their current address of internet. Lambert Royakkers (Royakkers, 2000) defined stalking crime as follows: "Any person is guilty of the stalking crime who: willfully, maliciously, trace another person with the intent of placing that person in reasonable fear of death, sexual assault, or great bodily injury to that person, any member of that person's family, or anyone with whom that person has a sexual or intimate relationship".

PUNISHMENT:

It is an unpleasant event that follows a behavior and decreases its frequency.

However, the use of punishment will have negative effects over long periods of time. It may cause undesirable emotional reactions. It leads only to short-term hide of the undesirable behavior rather than to its elimination. Educating, guiding and counseling may help in this direction and contribute effectively in minimizing crimes and frauds. We need to apply love force as against any legal or pressure techniques. We need to bring "change" in people who are already involved in such bad manners and habits using following Systems Model of Change.

It is not the strongest who survives nor the most intelligent, but the one who most responsive to change. Hellriegel, Slocum and Woodman discuss this issue in their Book "Organizational Behavior". Social media is sweet gift from western countries. Even country like USA is not able to control cyber crimes. Hence, they have started taking strict security steps. Outcome of these steps will be known only in future. The basic question is about attitude to control any kind of crimes. India could have adopted western model in this regard. But we miss that opportunity.

Conclusion :

Technology has become an integral part of our daily life in the world of the internet and cannot be dispensed with. Although there are several advantages of the technology, but it has become a threat to our lives too. It became necessary to take caution when using any technology so as not to be trapped by e-crimes. Many of the countries do not have specific laws related to ecrimes until today, so it is imperative to enact new laws to combat the worldwide scourge, which has no boundaries. Many of the studies in the current literature have focused on factors that affecting e-crimes such as demography, sexual, financial, cultural, and political.

There is a need to improve and validate these studies region vise and country vise.

Thus, as future work, it desired to do the followings:

- Build new models to measure the influence of demography and technology over the factors of e-crimes leading political, cultural, financial, and sexual aspects in societies locally and globally.
- Create hypotheses for each factor to find the influence between factors.
- Collect data from significant sample sources, on country as well as region bases, to test on the build models and created hypothesis.
- Using suitable statistical measures for data analysis.
- Discuss the study finding and objectives.
- Drawing conclusions and set recommendations for future studies.
- Making necessary and needed measures for cybersecurity around.

❑❑❑

31

Overview of Cyber Security

Dr.Rajkumar Shrihari Mare
Assistant Professor,
Shripatrao Kadam Mahavidyalya Shirwal,
Maharashtra, India

****

Abstract :

Cyber security are techniques generally set forth in published materials that attempt to safeguard the cyber Environment of a user or organization. It manages the set of techniques used to save the integrity of networks, programs And data from unauthorized access. It refers to the body of technologies, processes, and it may also be referred to as Information technology security. The field is of growing importance due to increasing reliance on computer systems, Including smart phones, televisions and the various tiny devices that constitute the Internet of Things.

Keywords: IT security, Internet of things (IOT)

I. INTRODUCTION

The internet has made the world smaller in many ways but it has also opened us up to influences that have never before Been so varied and so challenging. As fast as security grew, the hacking world grew faster. There are two ways of Looking at the issue of cyber security. One is that the companies that provide cloud computing do that and only that so These companies will be extremely well secured with the latest in cutting edge encryption technology.

II. WHAT IS CYBER SECURITY ?

Its being protected by internet-connected systems, including hardware, software and data, from cyber attacks. In a Computing context, security comprises cyber security and physical security both are used by enterprises to safe against

Unauthorized access to data centre and other computerized systems. The security, which is designed to maintain the Confidentiality, integrity and availability of data, is a subset of cyber security.

III. WHY DO WE NEED CYBER SECURITY ?

The range of operations of cyber security involves protecting information and systems from major cyber Threats. These threats take many forms. As a result, keeping pace with cyber security strategy and operations can Be a challenge, particularly in government and enterprise networks where, in their most innovative form, cyber Threats often take aim at secret, political and military assets of a nation, or its people. Some of the common threats Are :

Cyber terrorism It is the innovative use of information technology by terrorist groups to further their Political agenda. It took the form of attacks on networks, computer systems and telecommuni cation Infrastructures.

Cyber warfare It involves nation-states using information technology to go through something another Nations networks to cause damage. In the U.S. and many other people live in a society, cyber warfare has Been acknowledged as the fifth domain of warfare. Cyber warfare attacks are primarily executed by hackers Who are well-trained in use of benefit the quality of details computer networks, and operate under the Favourable and support of nation-states. Rather than closing a targets key networks, a cyber-warfare attack May forced to put into a situation into networks to compromise valuable data, degrade communications, Impair such infrastructural services as transportation and medical services, or interrupt commerce.

Cyber spionage It is the practice of using information technology to obtain secret information without Permission from its owners or holders. It is the most often used to gain strategic, economic, military Advantage, and is conducted using cracking techniques and malware.

Who are Cyber Criminals ?

It involves such activities as child printed sexual organs or activity; credit card fraud; cyber stalking; defaming Another online; gaining unauthorized access to computer systems; ignoring copyright, software licensing and Trademark safe to protect; overriding encryption to make illegal copies; software piracy and stealing anothers Identity to perform criminal acts. Cybercriminals are those who conduct such acts. They can be categorized into Three groups that reflect their motivation.

Type 1: Cybercriminals – hungry for recognition:
Hobby hackers;
IT professionals (social engineering is one of the biggest threat);
Politically motivated hackers;
Terrorist organizations.

Type 2: Cybercriminals – not interested in recognition:
Psychological prevents;
Financially motivated hackers (corporate espionage);
State – sponsored hacking (national espionage, sabotage);
Organized criminals.

Type 3: Cybercriminals – the insiders:
former employees seeking revenge;
Competing companies using employees to gain economic advantage through damage and/or theft.

How To Maintain Efffective Cyber Security

Historically, organizations and governments have taken a reactive, "point product" approach to combating cyber Threats, produce something together individual security technologies – one on top of another to safe their Networks and the valuable data within them. Not only is this method expensive and complex, but news of Damaging cyber breaches continues to dominate headlines, rendering this method ineffective. In fact, given the Area of group of people of data breaches, the topic of cyber security has launched to the top of the priority list for Boards of directors, which they seeked as far as less risky way. Instead, organizations can consider a natively Integrated, automated Next-Generation Security Platform that is specifically designed to provide consistent, Prevention-based protection – on the endpoint, in the data centre, on the network, in public and private clouds, and Across Saabs environments. By focusing on prevention, organizations can prevent cyber threats from impacting The network in the first place, and less overall cyber security risk to a manageable degree.

What Cyber Security Can Prevent

The use of cyber security can help prevent cyber-attacks, data breaches and identity theft and can aid in risk Management. When an organization has a strong sense of network security and an effective incident response plan, it is Better able to prevent and serious of these attacks. For example, end user protection defends information and guards Against loss or theft while also scanning computers for malicious code.

Types of Cyber Security Threats : The use of keeping up with new technologies, security trends and threat Intelligence is a challenging their task. However, it should be in order to protect information and other assets from cyber Threats, which take many forms.

Ransom ware is a type of malware that involves an attacker locking the victim's computer system files typically Through encryption and demanding a payment to decrypt and unlock them.

Malware is any file or program used to harm a computer user, such as worms, computer viruses, Trojan horses And spyware.

Social engineering is an attack that relies on human interaction to trick users into breaking security procedures In order to gain sensitive information that is typically protected.

Phishing is a form of fraud where fraudulent emails are sent that resemble emails from reputable sources;

However, the intention of these emails is to steal sensitive data, such as credit card or login information.

What does a security analyst do ?

An information security analysts protects to safe the company s systems and networks by planning and carrying out Measures of security. They create disruptive solutions to prevent critical information from being stolen, damaged, or Compromised. Their primary responsibility is to keep a business or organizations data, clients, employees, and any Virtual stored information safe from cyber attacks or hacking of any sort.

What are the consequences of cyber attack ?

Cyber-attacks will cause more damage financially and reputational even to the most withstand organisation. The Organisation which suffers cyber-attack, have to face the losing assets, business reputation and potentially the Organisation have to face regulatory fines and taking legal action and the costs of remediation. A survey taken by UK Government about cyber security in 2017, found that the average cost for a large business is £19,600 and for a small to Medium-sized business is £1,570.

IV. HACKING TOOLS

There are various tools are the modes of attack. And the malware are used for the totality of these tools. Examples are Viruses and worms. Computer programs that reproduce the functional copies of themselves with varying effects ranging From emphasize and inconvenience to compromise of the confidentiality or integrity of information, and Trojan horses, Destructive programs that pretence as benign applications but set up a back door so that the hacker can return later and Enter the system. Often system intrusion is the main goal of system intrusion is more advanced attacks. If the intruder Gains full system control, or, root access, he has unrestricted access to the inner workings of the system .Due to the Characteristics of digitally stored information the person with criminal intent will delay, disrupt, corrupt, exploit, Destroy, steal, and modify information. The value of the information or the importance of the application will be Depended, which the information are required and that such actions will have different effect with varying degrees of Gravity.

V. THE LEVEL OF CYBER RISK

There are some additional reasons for that threat is overrated. First, as combating cyber-threats has become a highly Politicized issue, official statements about the level of threat must also be seen in the context of different bureaucratic Entities that compete against each other for resources and influence. This is usually done by stating an urgent need for Action (which they should take) and describing the overall threat as big and rising. Second, psychological research has Shown that risk perception is highly dependent on intuition and emotions, as well as the perceptions of experts (Gregory And Mendelsohn 1993). Cyber-risks, especially in their more extreme form, fit the risk profile of socalled, dread risks, Which appear uncontrollable, catastrophic, fatal, and unknown. There is an inclination to be afraid of low probability Risks, which translates into pressure for serving an action with all sorts of willingness to bear high costs of uncertain Benefit. Only the system attacks sufficiently destructive or disruptive need the attention of the traditional national Security apparatus. Attacks that interrupt the services or that cost mainly a nuisance to the computer.

VI. REDUCING CYBER – IN – SECURITY

The three different debates have been taken over the many concepts and counter measures have been produced with Their focus. The computer network which owns a entities have a common practice to take a responsible for protecting It. However, there are some assets considered so crucial in the private sector to the functioning of society and Governments have to take additional measures to ensure the level of protection. These efforts are usually included under The label of critical (information). Information assurance is guide for the infrastructure protection and to the Management of risk, which is essentially about accepting that one is (or remains) insecure: the level of risk can never be Reduced to zero. This means that minor and probably also major cyber-incidents are bound to happen because they Simply cannot be avoided even with perfect risk management.

CONCLUSION

Depending on their (potential) severity, however, disruptive incidents in the future will continue to fuel the military Discourse, and with it fears of strategic cyber-war. Certainly, thinking about (and planning for) worstcase scenarios is a Legitimate task of the national security apparatus. However, for the favour of more plausible and more likely problems They should not to get more attention Therefore, there is no way to study the, actual level of cyberrisk in any sound Way because it only exists in and through the representations of various actors in the political domain.

REFERENCES

[1]. Daniel, Schatz,; Julie, Wall, (2017). "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law. 12 (2). ISSN 1558-7215. Archived from the original on 28 December 2017.

[2]. Rouse, Margaret. "Social engineering definition". Tech Target. Archived from the original on 5 January 2018. Retrieved 6 September 2015.

[3]. Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017)."Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law. 12 (2). ISSN 1558-7215.

[4]. "Reliance spells end of road for ICT amateurs", 7 May 2013, The Australian

[5]. Stevens, Tim. "Global Cyber security: New Directions in Theory and Methods". Politics and Governance. 6 (2). Doi:10.17645 /pag.v 6i2.1569.

[6]. "Computer Security and Mobile Security Challenges". Researchgate.net. Archived from the original on 12 October 2016. Retrieved 4 August 2016.

[7]. "Distributed Denial of Service Attack". Csa.gov.sg. Archived from the original on 6 August 2016. Retrieved 12 November 2014.

[8]. Wireless mouse leave billions at risk of computer hack: cyber security firm Archived 3 April 2016 at the Way back Machine.

[9]. "Multi-Vector Attacks Demand Multi-Vector Protection". MSSP Alert. July 24, 2018.

[10]. Millman, Renee (December 15, 2017). "New polymorphic malware evades three quarters of AV scanners". SC Magazine UK.

[11]. Turner, Rik (May 22, 2018). "Thinking about cyber attacks in generations can help focus enterprise security plans". Informa PLC. Ovum.

[12]. "Identifying Phishing Attempts". Case. Archived from the original on 13 September 2015.

[13]. Arcos Sergio. "Social Engineering" (PDF). Archived (PDF) from the original on 3 December 2013. [14]. Scannell, Kara (24 February 2016). "CEO email scam costs companies $2bn". Financial Times (25 Feb 2016). Archived from the original on 23
June 2016. Retrieved 7 May 2016.

[15]. "Bucks leak tax info of players, employees as result of email scam". Associated Press. 20 May 2016. Archived from the original on 20 May 2016. Retrieved 20 May 2016.

[16]. "What is Spoofing? – Definition from Techopedia". Archived from the original on 30 June 2016.

[17]. "spoofing". Oxford Reference. Retrieved 8 October 2017.

[18]. Marcel, Sébastien; Nixon, Mark; Li, Stan, eds. (2014). Handbook of Biometric Anti-Spoofing: Trusted Biometrics under Spoofing Attacks (PDF). London: Springer. Doi:10.1007/ 978-1-4471-6524-8. ISBN 978-1-4471-6524-8. ISSN 21916594. LCCN 2014942635. Retrieved 8 October 2017 – via Penn State University Libraries.

❑❑❑

32

A Case Study of Cyber Crime in Banking Sector

Prof. Navnath Nathrao Ipper
Assistant Professor in Economics,
Chatrapati Shivaji College Satara

****

Abstract:

The Indian Banking industry is old and many changes are brought in this industry since liberalization. The banking system is well regulated and supervised, it involves moral practice, financial distress and company governance. The call for development has given this unit monstrous probabilities and so, banks are presently among the best recipients of the IT insurgence. The on-line exchanges mounting on advancements like NEFT (National Electronic Store Exchange), RTGS (Constant Gross Settlement), ECS (Electronic Clearing Administration) and transportable exchanges has provided aid in saving cash and fund problems.Consequently, with the development of computers and net innovation, new forms of overall violations referred to as 'Digital Wrongdoings' has advanced within the scene.

Over some years, the character and example of Digital Wrongdoing occurrences have progressively fashionable and complicated. Banks and funds connected Foundations stay the intense focuses of digital culprits within the most up-to-date decade. conspicuously financial profit is till now the important inspiration driving most cybercriminal exercises and there's token shot of this ever-changing shortly.

1. Introduction

Until mid-1990s, managing an account segment in many parts of the world was basic and dependable; anyway since the coming of innovation, the keeping money division saw a change in perspective in the wonder. Banks so as to upgrade their client base presented numerous stages through which exchanges should be possible absent much exertion. These advancements empowered the client to get to their bank funds 24*7 and year around through, ATMs and Web based managing an account methods. With the pace in innovation, the money cheating cases have increased. Cyber criminals are using different techniques to collect bank data and last their cash. Various specialized techniques have been used by the banks to safeguard these crimes, but this issue still holds on. The explanation for this is the resistance measures right now accessible with banks are accessible in the open market or area which can be used by a digital criminal, who can easily cross the safety standards. One of the techniques to relieve the issue of digital wrongdoings in keeping money segment is to distinguish the variables by banks and the issue of digital wrongdoings. Banks which are the most part focusses of digital wrongdoings experience the I'll effects of different online assaults like phishing, keystroke logging malwares, wholesale fraud etc.

2. Objectives

1.A Study of the nature of cyber security challenges because of rapid digitization.

2.Banks can deal with cyber threats by focusing on afew suggested possible solutions.

3.Examine how the banking industry is the pandemic result in rapid digitization of banks unlike in the past.

4. Cyber Crime in Banking Sector

Digital violations can be comprehensively be arranged into classification such as digital harassing, programming robbery, wholesale fraud, Email spam, online robbery

The online wrongdoings can be classified as:

Hacking: It is an unlawful access to a system to degenerate or to see any misguidedly information.

Phishing: It includes a procedure to collect private data like username, password, one time password etc.

Vishing: A criminal act for social designing via phone to access an individual and budgetary data from population with the goal to attain monetary benefits.

Spamming: spontaneous messages sent to a mass population trying to constrain the message in individuals who might not get it.

ATM Skimming and Purpose Offer Wrongdoings: It is the most developed method of trading off ATM machine or POS by introducing a gadget on the keypad which copies the same thing. Effective execution of skimmers through ATM machines gather the card numbers and personal information that are later repeated to do fake transactions

5. Internet Banking in India

Electronic Keeping money or e-managing an account alludes where saving money exercises are completely utilizing instructive and PC innovation over human asset. In contrast to the traditional method in e-managing there is no physical association with the banks and their customers.

E-managing is the conveyance of banks data and administration to clients by means of various conveyance stages which can be utilized through PC and mobile phones or advanced TV.[3]

A working gathering on managing was established by RBI. For the management and administration, the gatherings partitioned money into 3 categories:

Enlightening Framework: This category gives data about credit plans, branch areas, financing costs to the clients. The client can download different utilities according to their personal needs. There is no sensible possibility of any unapproved individual getting into the creation arrangement of the bank.[4]

Open Framework: This gives data to client about his record balance. The data can be checked by clients after confirmation and signing through passwords.[5]

Value Based Framework: In this category the clients can do changes through it's framework and they are directly transferred to the clients record. A bi directional change takes place between the bank and client and between client and the outsider. This framework is used trough instruments like http and https. E keeping money incorporates Web Saving money, Portable Managing an account, RTGS, ATM's, Master Cards, Charge Cards and keen cards and so forth.[6]

Reasons for Cyber Crime

Hart in his work, the idea of law has said 'people are helpless so standard of law is required to ensure them'. After applying this we may state that PC's are powerless so standard of law is required to secure and protect them against digital wrongdoing. Following are some reasons.

Loss of proof

Negligence

Complex

Easy to access

Capacity to store information in little place.

6. Impact of Cyber Crime on Banking Sector

The main cases have been identified because of the violent upsurge in cell phones with internet. Mobile phones are used for a number of online services like web saving money, paying service charges, web based shopping and is according to the criminals to acquire access to criminal data.

In the cases, where the hackers are not able to get significant data, the destroy the bank's site as a measure to render against their endeavors.

Other than monetary benefits from digital assaults, the illicit business generally termed as the Darkweb[7] adds to the cybercrime as a tool for trading individual data. Touchy data including stolen Card Numbers, web based managing account, therapeutic records and authoritative access to servers are exchanged for cash in this online network

Material and Method Used

The information is gathered from different sources like magazines, government report. Measures of optional information is accessible in articles, magazines, journals and beforehand directed analysts on the comparative theme. The gathered information will help in differentiating the key parameters for further investigation and in this manner will help in characterizing the destinations of examination

Case Study

Case under the Study: Official Website of Maharashtra Government (Hacked Mumbai)

On 20th September 2007 IT specialists were attempting to re-control the official website of the Maharashtra government which was hacked. http:/www.maharashtragovernment .in, stayed blocked. Vice President Pastor and home priest R.R Patil confirmed that that the Maharashtra government site has been hacked. He affirmed that the state government will look into this matter and asked the Digital wrong doing Branch to examine the hacking. Patil said if there would be need them the state would hire private IT officials for this matter.

While, reestablishing the site disclosed to the Middle Easterner News that that programmers may have decimated majority of sit's substance. IT officials said that the hackers were recognized as, Program Cool Al- Jazeera and added that they were in Saudi Arabia. Senior authority from government IT decision said that the official site has been influenced by infections on a few events before, however was never hacked.

Three individuals were held liable for on line Visa trick, as people were abused through online methods for booking air tickets. These parties were helped by Digital Wrongdoing Examination Cell in Pune. Mr. ParveshChauhan, ICICI Prudential extra security officer gripped for one of his client. As per data given by the police, one of the client got a message for buying air tickets when the master card was held by him. He directly went to the bank when he came to know about the issue. The tickets were booked through the online methods.

Later after examination it was disclosed that the information was gotten from State Bank of India. Shaikh was working in the Visa department and he had the information about the new clients. Further, he shared the information to Kale. Kale further passed this information to his friend Lukkad, who further booked air tickets from the acquired information and sold them for equivalent amount of money. Digital Cell head DCP Sunil Pulhari was associated for eight days and lastly caught the offenders.

UTI bank was trapped in a phishing attack in February 2017 by propelling phishing assault on the website of UTI bank. A URL on geo cities landed on the client's email id's asking about the personal information such as login Id and password. Which as later discovered by the IT officials that the website admin of the page was an individual named PetrStastny whose email could be found on the webpage. Top authorities of UTI bank confirmed that they have informed about the case to the Monetary Office Wing, Delhi Police. The bank had also drawn in the administrations of Melbourne based Extortion Watch Worldwide, main organization which keeps a check on phishing and bringing down these activities.

India's First ATM Card Fraud

The Chennai police busted a gang associated with digital wrongdoing. The police caught Deepak PremManwani aged 22 years who was caught breaking into an ATM in the month of June. According to the police report when he was detained, he has with him Rs 7.5 lakh knocked from two ATMs in The Nagar and Abiramipuram in Chennai. Preceding that, he had left with Rs 50,000 from an ATM in Mumbai. Manwani was an MBA dropout from a Pune school and was filled in a Chennai based firm.

His wrongdoing started from a web bistro. He had some contacts who were sitting in Europe, they used to give him a card of a couple of American banks for 5 Dollars each. The administrator of the European site had an interesting plan to get individual ID Number of the clients.

That organization had a huge number of supporters. Evidently Manwani and other supporters went into the arrangement of this pack and bought a numerous information, on specific terms, are basically into an arrangement on a good sharing premise. Additionally, Manwani also learned how to create 30 plastic cards that contained important information to empower him to break ATMs.

After receiving huge number of complaints from the charged Visa clients and banks in the US, the FEI began an investigation and alarmed the CBI in New Delhi that universal pack has developed in India as well.

7. Finding

Maximum part of the Cybercrime consists of hacking and data fraud.

Banks are becoming more and more focus as all the people's money is held with banks.

The security of their clients is at huge risk since it has turned out to be anything but difficult to hack their own database.

The quantity of cases by cyber cell has remained low throughout the previous years, with just 20 percent achieve rate.

There is no such order that deals with these violations, especially with the saving money segments.

8. Suggestion

IT Act ought to be revised as needs be to characterize cybercrime and furthermore indicate the situations where the Demonstration will have additional regional purview. The extent of the IT Demonstration should be widened to incorporate legitimate structure identifying with digital laws in India. The obligation of the middle people is unclear and must be made progressively unmistakable and express.

1. Cyber Fraud Council in Banks

At whatever point a digital extortion is carried out the unfortunate casualty should answer to the Digital Misrepresentation Gathering that must be set up by in every single bank to audit, screen research and report about digital wrongdoing. In the event that, such Committee does not take perform or declines to play out its obligation then an arrangement to record a FIR must be made.

The issue to be brought before such gathering can be of any esteem. In any case, when the esteem is high then the Committee will act quickly. RBI in its 2011 Report expressed that when bank fakes are of short of what one Crore then it may not be important to require the consideration of the Extraordinary Advisory Group Board.[8]

2. Education to Customer

The client must be aware about different bank cheats and measures should be taken to educate them for security components with the objective that they don't fall prey as casualties of cybercrime. If a client is cognizant and reports a particular matter of cybercrime timely, then the rate of cybercrimes can be diminished. A client should be made aware of the rules and regulation of E-Managing an account. This awareness can be brought to the customers by publishing on bank's site, distributing in paper, sending messages, training and so on.

On the off chance and a bank present any new strategy or there are some other progressions which are which are required to be trailed by all banks according to RBI at that point bank must educate the client through phone.[9] The mindfulness material ought to be opportune refreshed remembering the adjustments in the enactment and rules of Reserve Bank of India.[10]

3. Training of Bank Employees

Introduction programs must be directed for the staff by banks. The staff must be made mindful about misrepresentation counteractive action measures. It can be done in a better way by distribution of pamphlets, through magazines. Center saving money arrangement programming having discussion on elements causing cybercrime and activities required to prevent them.

4.Cooperation at International Level to Curb Cybercrime

The internet is transnational in nature and requires mutual understanding between states to cooperate to turn away cybercrime. In spite of the fact that, a couple of bargains and usage estimates exist a healthy methodology characterizing legitimate and specialized measures and authoritative abilities is yet to take focal significance for India in its objective to add to the worldwide battle against cybercrime.

IT Act, 2000 having additional regional application represents an issue in examination, arraignment and removal of outside nationals. India ought to effectively connect as a feature of the worldwide cybercrime network focused on Asia, Europe and America to look for help and furthermore add to universal cybercrime issues.

1.The society should report these cases to the Digital Wrongdoing Branch rather than involving the branches for quick and strict activities.

2.Projects should be started to aware the public about the continuous situations and forthcoming situations.

3.Punishments should be practiced completely to stop these issues and punish the assailants.

4.The legislature should keep a track on the working system of Huge information banks.

5.There should be quick dispose of cases, to meet the complaints and fabricate certainty among the general public.

6.The law implementation should be strict and occasionally monitor such wrongdoings

9. Conclusion:-

In my opinion no sort of crime should be tolerated. The safety and privacy of an individual should be safeguarded. Every person has a right to live in a secure environment, no matter in real life or on internet.After doing the research on this issue, I understand the motive of the cyber-criminals. To a certain extent, I see why some choose to take their political/religious protests online.

Protestors are likely to get caught

Online protests get due attention

Support is gained quickly.

Global reach through internet.

However, I find Cyber Crime more serious offence than the real life crimes, as it effects millions of web users at once. In real life it harms only a few number of persons.

When online business activities get disrupted, it leads to great problems for customers and companies. With technology being such a big part of our lifestyle today, cybercrime has no place in it. For instance, following cybercrime on Sony, the Federal Bureau of Investigation has issued search warrants to arrest the culprits. To me, it is a massive piece of news, because it indicates strengthening commitment against these criminals.

Reference:-

1. Kharouni, L (2012) Automating Online Baking Fraud Automatic Transfer System: The Latest Cybercrime Toolkit

2. Liu, J., Hebenton B &Jou , S Handbook of Asian Criminology.

3. Daniel, E (1999), Provision of electronic banking in the UK and Republic of Ireland, International Journal of Book Marketing, Vol 17 No.2

4. Reserve Bank of India, Report on Internet Banking, available at: https://www.rbi.org.in/Scripts/PublicationReport Details. aspx?Url Page=&ID=243#ch2(Last Visited: Oct 11, 2019, 10:25 PM).

5. Dheenadhayalan V., Automation of

Banking sector in India, Yojana, February, (2010) p.32.

6. Murashbekov, ÎB. (2015). Methods for Cybercrime Fighting Improvement in Developed Countries. Journal of Internet Banking and Commerce.

7. Reserve Bank of India, Working Group on Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds, (21 Jan 2011).

8. Ibid

❑❑❑

33

A Study of Cyber Security and Cyber Crime

Dr.Sunil S. Langade
Assistant Professor in Commerce,
Annasaheb Waghire College, Otur. Tal.Junnar,
Dist.Pune

****

Abstract:

Nowadays, cybercrime is one of the major crimes done by computer expert. In this paper, need of cyber security is mentioned and some of the impacts of the cybercrime. Cyber security is to provide prevention against the cybercrime, while cybercrime is that group of activities made by the people by creating disturbance in network, stealing others important and private data, documents, hack bank details and accounts and transferring money to their own.

This paper gives detailed information regarding cyber security and cybercrime. It includes types of cyber security, need of cyber security, issues in cyber security, its advantages and disadvantages, history of cybercrime, types of cybercrime. Keywords: Cyber, cybercrime, cyber security, crime, security, network, hacking, steal data, information security, network security, operational security, communicational security, application security

1. Introduction

It is a combining form relating to information and technology, the internet, and virtual reality. The term cyber security is used to refer to the security offered through on-line services to protect your online information. It additionally refers to the technologies and tactics designed to secure computer systems, computer networks and information from unauthorized access, susceptibilities and attacks delivered though the internet. Cyber security is an all-encompassing domain of information technology it comprises the entire set of security-related technologies. Cyber security is also body of technologies, processes and practices designed to protect and secure networks, computer systems, various programs and data from cyber-attack, damage all these things or unauthorized access these. In a computing context, security includes both cyber security and physical security. Security standards which are enable organizations to practice safe security techniques to minimize the number of successful cyber security attacks and prevent their data or systems. Though, cyber security is important for network security, data security, communication security, operational security and application security [2][3]. Cyber security is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment [5]. Cyber security strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.

2. Thegeneral security objectives

1. To evaluated modifications inside the Cyber Security practices.

2. To evaluate the issues will rise up within the Cybercrime in society.

3. To assess the,Availability, Integrity, Confidentiality which mayinclude authenticity and non-repudiation

3.Elements of Cyber Security

Elements of cyber security include: Application security is the use of software, hardware, and procedural methods to protect application from external threats, viruses, malwares or attacks. At the time of software design, security is becoming a very important concern during development of applications [1]. It would become more and more accessible over networks, and as a result, there are possibilities to a wide variety of threats entered to harm software or application and its data. Security measures at the time of building applications and application security routines which minimize the unauthorized code will be able to manipulate applications to access, steal, modify, or delete sensitive data. Actions to be taken to secure applications are called counter measures. The most basic software for countermeasure is application firewall that secures files or the handling of data by specific installed programs. The most common hardware countermeasure is a router that can secure the IP addresses of an individual computer system to being directly visible on the internet. Other countermeasures include conventional firewalls, programs or algorithms for encryption or decryption processes, anti-virus programs, spyware detection or removal programs and biometric authentication systems.

1. Communication Security:

Communication security is also known as COMSEC. COMSEC is the process to secure or prevent unauthorized access to traffic will be generated from telecommunication systems, or it will also help for any written information that is transmitted or transferred to another device via any other medium. There are several COMSEC disciplines, including:

• Cryptographic security:

It encrypts data of sender side and makes it unreadable until the data is decrypted by receiver side. • Emission security: It is used to prevent the release or capture of equipment emanations to prevent information from unauthorized interception.

- **Physical security:**

It ensures by giving prevention of unauthorized access to a network's cryptographic information, documents and equipment.

- **Transmission security:**

It is used to protect unauthorized access when data is physically transferred from one side to other side or one medium to other medium to prevent issues such as service interruption, steal data by malicious person.

- **Information security:**

It is used to protect information or data and its critical elements, including the systems software and hardware that use to store or transmit that information.

Information security is also known as InfoSec. InfoSec is a set of strategies for managing the processes, tools which are used in software and policies of software that are mainly for security purpose and necessary to prevent, detect and counter threats to digital and non-digital information [4]. InfoSec responsibilities include a set of business processes that will protect information assets of how the information is formatted or whether it is transit or not, is being processed or is at rest in storage. InfoSec programs are follow the core objectives of the CIA (confidentiality, integrity and availability): it maintaining the confidentiality ensure that sensitive information is only disclosed to authorized parties, integrity stands for prevention of unauthorized modification of data and availability that guarantees the data can be accessed by authorized parties when requested of IT systems and business data.

4. Network Security:

Network security is used to protect the networking components, connection of networks and con- tent related to network. A network security system typically relies on layers of security and it consists of more than one component that including in to the network for monitoring network and security software and hardware, and it appliances. All components work together to increase the overall security and performance of the computer network. 3. Operational Security: Operational security is an analytical process that classifies information assets and determines the controls required to secure these assets. Operational security is also known as OPSEC. Operational security typically consists of a five-step iterative process: • Identify critical information: The first step is to find out which data would be particularly affect to an organization or harmful for organization if it was obtained by an adversary. This includes intellectual property, employees' and/or customers' personally information and financial statements.

5.Determine threats:

The next step is to determine which code or program represents a threat to the organization's private or sensitive information. There may be numerous adversaries that target different pieces of information, and companies must consider any competitors or hackers that may target the data.

- **Analyze vulnerabilities:**

In the vulnerability analysis stage, the organization examines potential weaknesses among the safeguards in place to protect the private information that leave it vulnerable to potential adversaries [6]. This step includes identifying any potential lapses in physical/ electronic processes designed to protect against the predetermined threats, or areas where lack of security awareness training leaves information open to attack.

- **Assess risks:**

After vulnerabilities have been determined, the next step is to find the threat level associated with each of them. Companies rank the risks according to factors such as the chances a specific attack will occur and how damaging such an attack would be to operations. The higher the risk, the more pressing it will be for the organization to implement risk management controls.

• Apply appropriate countermeasures:

The final step consists of implementing a plan to mitigate the risks beginning with those that pose the biggest threat to operations. Potential security improvements stemming from the risk mitigation plan include implementing additional hardware and training or developing new information governance policies.

6. Problematic Elements of Cyber Security

One of the most problematic elements of cyber security is thesecurity risks. The traditional approach has been focus most resources on the most crucial system components and protect against the threats, which necessitated leaving some less important system components undefended and some less dangerous risks, i.e., not protected. Such an approach is insufficient in the current environment.

1. Major Security Problems:

• Virus:

A Virus is a program that is loaded onto your computer without your knowledge and runs against your wishes. These are computer programs that attach themselves to or infect a system or files, and have a tendency to circulate to other computers on a network by clicking on it, through mail, through external devices, etc. They disrupt the computer operation and affect the data stored either by modifying it or by removing it altogether.

• Example of viruses: (1) Melissa, (2) Sasser, (3) Zeus, (4) Conficker, (5) Stuxnet, (6) Mydoom, (7) Code Red.

• Warms:

Worms unlike viruses do not need a host to cling on to. They merely replicate until they eat up all available memory in the system. The term worm is sometimes used to mean self-replicating malware (MALicioussoftWARE). It occupies some free memory of drives or external devices.

• Example of warms: (1) Badtrans, (2) Bagle, (3) Blaster, (4) ExploreZip, (5) Kak worm, (6) Netsky, (7) SQL Slammer, (8) Supernova Worm

• Hacker:

In common a hacker is a person who breaks into computers, usually by gaining access to administrative controls.

7. Types of hackers:

• Malware:

The word "malware" comes from the term "MALicioussoftWARE." Malware is any software that infects and damages a computer system without the owner's knowledge or permission. (1) Viruses, (2) Warms, (3) Root kits, (4) Trojans, (5) Spyware, (6) Crime ware, (7) Adware

• Trojan horses:

Trojan horses are email viruses that can duplicate themselves, steal information, or harm the computer system. These viruses are the most serious threats to computers.

• Password Cracking:

Password attacks are attacks by hackers that are able to determine passwords or find passwords to different protected electronic areas and social network sites.

8. Advantages of Cyber Security

1. Improved security of cyberspace
2. Increase in cyber defense
3. Increase in cyber speed
4. Protecting company data and information
5. Protects systems and computers against virus, worms, malware and spyware, etc.
6. Protects individual private information
7. Protects networks and resources
8. Fight against computer hackers and identity theft
9. Minimizes computer freezing and crashes.
10. Gives privacy to users

9. Disadvantages of Cyber Security

1. It will be costly for average users
2. Firewalls can be difficult to config-

ure correctly

3. Need to keep updating the new software in order to keep security up to date.

4. Make system slower than before.

5. Incorrectly configured firewalls may block users from performing certain actions on the Internet, until the firewall configured correctly.

10. Safety Tips for Cyber Security

1. Use antivirus software

2. Insert firewalls, pop up blocker

3. Uninstall unnecessary software

4. Maintain backup

5. Check security settings

6. Use secure connection

7. Open attachments carefully

8. Use strong passwords, (keep combination of uppercase, lowercase, special characters etc.) do not give personal information unless required

11. Issues in Cyber Security

1. Better end user education it's sort of expressing the self-evident, however most frameworks are just as secure as the propensities for the general population utilizing them. Terrible on-screen characters abuse this to exploiting powerless passwords and un patched programming and utilizing complex phishing strategies [8].

2. Security mindful programming advancement: They are sufficiently not individuals centered on security. With an expanding measure of individuals getting associated with Internet, the security dangers that reason more hazards to hurt information, programming and gadget too.

Cybercrime

Cyber security is needed when crime will be performed: The former descriptions were "computer crime", "computer related crime" or "crime by computer". With the pervasion of digital technology, some new terms like "high-technology" or "information age" crime were added to the definition. [6] Also, Internet brought other new terms, like "cybercrime" and "net" crime. Other forms include "digital", "electronic", "virtual", "IT", "high-tech" and technology enabled" crime. It will do by that people who are mostly connected to internet, online activities, social activities, etc.

History of Cybercrime

1. The first recorded cybercrime was recorded in the year 1820.

2. The first spam email took place in 1978 when it was sent over the Arpanet.

3. The first Virus was installed on an Apple Computer in 1982.

12. Types of Cybercrime

• Hacking

In simple words, hacking is an act committed by an intruder by accessing your computer system without your permission. Hackers (the people doing the hacking) are basically computer programmers, who have an advanced understanding of computers and commonly misuse this knowledge for devious reasons. a. SQL injections b. Theft of FTP passwords c. Cross site scripting

• Virus dissemination

Viruses are computer programs that attach themselves to or infect a system or files, and have a tendency to circulate to other computers on a network. They disrupt the computer operation and affect the data stored either by modifying it or by deleting it altogether

• Logic bombs

A logic bomb, also known as slag code, is a malicious piece of code which is intentionally inserted into software to execute a malicious task when triggered by a specific event.

• Denial-of-Service attack

A Denial-of-Service (DoS) attack is an explicit attempt by attackers to deny service to intended users of that service. It involves flooding a computer resource with more requests than it can handle consuming its available bandwidth which results in server overload.

• Phishing

This is a technique of extracting confidential information such as credit card numbers and username password combos by masquerading as a legitimate enterprise.

• Bombing and spamming

Email bombing is characterized by an abuser sending huge volumes of email to a target address resulting in victims email account or mail servers crashing.

• Jacking

Web jacking derives its name from hijacking. Here, the hacker takes control of a web site fraudulently. He may change the content of the original site or even redirect the user to another fake similar looking page controlled by him.

• Cyber stalking

Cyber stalking is a new form of internet crime in our society when a person is pursued or followed online a. Internet stalking, b. Computer stalking.

• Data diddling

Data Diddling is unauthorized altering of data before or during entry into a computer system, and then changing it back after processing is done.

• Theft and Credit Card

Fraud Identity theft occurs when someone steals your identity and pretends to be you to access resources such as credit cards, bank accounts and other benefits in your name.

• Slicing attack

A salami slicing attack or salami fraud is a technique by which cyber criminals steal money or resources a bit at a time so that there no noticeable difference in overall size.

• Software Piracy

Internet piracy is an integral part of our lives which knowingly or unknowingly we all contribute to. Cybercrime includes • Illegal access • Illegal interception system • Interference data • Interference misuse of devices fraud.

13. Conclusion

Any intelligent device that can pass data to one or more other devices (either through a network or not) is encompassed within the scope of Cyber Security that includes pretty much the entire foundation of modern society. All need to be aware of cyber security as well as cybercrimes and its causes. There is little seriousness about security regarding online, social and other activities through which probability of risk will be higher. It causes loss of data, modifying data, removing useful information as personal details, passwords of mail accounts, social accounts or bank accounts. People may also know about laws against cybercrimes or cyber laws and actions which will be taken and how to fight against crime.

References

1. Sergey, Melnik, Smirnov Nikolay, Erokhin Sergey. Cyber security concept for Internet of Everything (IoE). Systems of Signal Synchronization, Generating and Processing in Telecommunications. 2017. IEEE, 2017.

2. Martin, Nigel, John Rice. Cybercrime: Understanding and addressing the concerns of stakeholders. Computers and Security. 2011; 30(8): 803–814.

3. Shang H, Jiang R, Li A. A Framework to Construct Knowledge Base for Cyber Security. 2017 IEEE Second International Conference on Data Science in Cyberspace (DSC). IEEE, 2017.

4. ManmohanChaturvedi, AynurUnal, ShilpaBahl. International cooperation in cyber space to combat cyber crime and terrorism. 2014 IEEE Conference on Norbert Wiener in the 21st Century (21CW). IEEE, 2014.

5. Rayne Reid, Johan Van Niekerk. From information security to cyber security cultures. Information Security for South Africa (ISSA). 2014. IEEE, 2014.

6. R. Hewett, S. Rudrapattana, P.

Kijsanayoth. Cyber-security analysis of smart SCADA systems with game models. Proceedings of the 9th annual cyber and information security research conference, ACM, 2014, pp. 109–112.

7. Von Solms, Rossouw, Johan Van Niekerk. From information security to cyber security. Computers and Security. 2013; 38: 97–102.

8. Eric A. Fischer. (2106). Cybersecurity Issues and Challenges: In Brief. [Online]. Available from https://fas.org/sgp/crs/misc/R43831.pdf [Accessed on October 201

❑❑❑

34

An Impact of Cyber Crime Indian Economy

Dr.Rodage Kailas Dadasaheb
Assistant Professor in Economics,
Dada Patil College Karjat, Tal-Karjat,
Dist.A.Nagar

****

Abstract:

Cybercrime is relentless, undiminished, and unlikely to stop. It is just too easy and toCybercriminals at the high end are as technologically sophisticated as the most advanced information technology (IT) companies, and, like them, have moved quickly to adopt cloud computing, artificial intelligence, Software-as-a-Service, and encryption. Cybercrime remainsfar too easy, since many technology users fail to take the most basic protective measures,and many technology products lack adequate efenses, while cybercriminals use bothsimple and advanced technology to identify targets, automate software creation anddelivery, and monetization of what they steal.

The aim of the research is to examine the negative impact cybercrimespose to the society. The concepts of cybercrimes are introduced and different typesof cybercrimes are explored as examples of some of the impacts which caused bycybercrimes activities. Results from this study show that, there are many negativeimpacts which the society suffer from the cybercrimes and why the computer ornetworking are tools target for the crimes. The discussions are made from thefindings and finally the paper addresses different measures which can be taken tocombat these cybercrimes so that people still enjoy using the technology rather thanstop them to use it.

1. Introduction

As the Internet came into widespread commercial use, the nature of computercrimes began to shift. 'While in some crimes, one component of the crime may havebeen committed using an electronic instrument, in other crimes, the crime as awhole is committed in the online or electronic environment. These crimes, knownas cybercrimes, generally occur in the virtual community of the Internet or incyberspace' (Heather 2008, Newton 2008).

Viruses, worms, and Trojan horses are another serious threat. There is a variety ofCyber crime committed but these are the most prevalent and appear to be among themost troubling to computer users (Furnell, 2002 in Brett, 2008).

As it has been seen in the introductory part, there is no way any organization orcountry can avoid the uses of ICT since it needs to remain competitive in the marketplace, but the biggest issue is how to deal with cybercrimes so as to minimizeif not to reduce its threats. Therefore, the paper intends to explore the impact ofcybercrimes in the society and the security measures which can be taken to prevent these threats.

The wide range of existing estimates of the annual loss—from a few billion dollars to hundreds ofbillions—reflects several difficulties. Companies conceal their losses and some are not aware of what hasbeen taken. Intellectual property is hard to value. Some estimates relied on surveys, which provide veryimprecise results unless carefully constructed. One common problem with cybersecurity surveys is thatthose who answer the questions "self-select," introducing a possible source of distortion into the results.

Given the data collection problems, loss estimates are based on assumptions about scale and effect—change the assumption and you get very different results. These problems leave many estimates opento question.

The Components of Malicious Cyber Activity

In this initial report we start by asking what we should count in estimating losses from cybercrime and cyber espionage. We can break malicious cyber activity into six parts:

- Opportunity costs, including service and employment disruptions, and reduced trust for online activities
- The loss of sensitive business information, including possible stock market manipulation
- The additional cost of securing networks, insurance, and recovery from cyber attacks
- Cybercrime, which costs the world hundreds of millions of dollars every year
- The loss of intellectual property and business confidential information
- Reputational damage to the hacked company

2. Objective of the Study

1. To evaluate the Problems will rise up within the Cybercrime in society.

2. To assess the which may include authenticity and non-repudiation

3.To evaluate Cybercrime has been increasing in complexity and financial costs

3.Research Methodology

The method we employed in this research was the survey method while the research design used was the purposive research design technique so as to meet up with the targeted presentation date. The survey method was used because our aims are to get the awareness from users of the computer vis-a-viz the Internet and to determine the impacts of these menaces on the economy The population of this study is the Commerce , Economics, Computer Science Department of (SPPU)University of Pune in order to get the impacts from the professional while the Computer and Internet users mostly students and Lecturers. A sample size of 50 was selected using the random sampling procedure from the targeted population of 100. The method used to collect data for this study is structured questionnaire. A total of 50 copies of the questionnaire were personally administered out of which 46 copies were retrieved in usable form. This represents a response rate of 92%. [6]

4. Literature review

A. What is Cybercrime?

In the most general form crime can be de-fined as the violation of law, especially a serious one Cyber crime is an unlawful act wherein the computer is either a tool or target or both. Cyber crime consists of specific crime dealing with computer and networks and facilitation of traditional crime through the use of a computer. Cyber crime uses the unique feature of Internet namely the sending of emails, speedy publication of information through the web to any one the planet. These criminal activities can often be faster [7] A cybercrime is a crime that is committed with the help of a computer through a communication device or a transmission media called the cyberspace and global network called the Internet [2]. Cyber crime has been increasing in complexity and financial costs since corporations, government and individual or society at large started utilizing computers in the course of doing business. As technology increases between governments, corporate organizations and individuals that are involved in international and local businesses; criminals have realized that this is a cost effective method to make money. Efforts to address Internet crime include activities associated with defending networks and data, detecting criminal activities, inquiring into crime and taking legal action against criminals [3].Cyberspace security is crucial for maintaining the continuity of these vital services and for preserving the publics trust in information systems. But can this be achieved world-wide? Well, this is a topic for another day as our focal point in this paper is all about cybercrimes and its impact on the Indian economy.[6] Some examples of cyber crimes include sending spam emails (spamming), stealing personal information (identity theft), breaking into someone's computer to view or alter data (hacking) and tricking someone into revealing their personal information (phishing), making Internet services unavailable for users (Denial of service – DOS), advanced free fraud 419 (aka Yahoo-yahoo), credit card fraud (ATM), plagiarism and software piracy, pornography, stealing money bit-by-bit in a cunning way (salami attacks) and virus dissemination etc.So many crimes are committed every day in the Indian cyberspace. A recent report in the Daily Trust, (2010)by the Internet Crime Complaint Centre, which is a partnership between the Federal Bureau of Investigation (FBI) and America's National White Collar Crime Centre, revealed that India is now ranked third among the list of top ten sources of cybercrime in the world with 8% behind the US (65%) and the UK (9.9%). [5]. What Indian government, corporate organizations and the society at large do not know is that the heavy economic impact on the country, (either in financial terms or otherwise), will have an adverse consequences on unemployment rate, social services and international reputation. Therefore, a detailed introduction of cybercrime needs to be presented with the view to fully analyze the indices that make up this crime so that our government and society will be aware of this crime and its implication on the economy. In this paper, we will introduce the origins and the evolution of cybercrime, the different categories of cybercrime (target cybercrime, tool cybercrime and computer incidental).

The impact of cybercrime has been, and will be in the future, felt by all governments and economies that are connected to the Internet. Criminals will use the Internet, computers and other digital devices to facilitate their illegal activities as long as the financial gains outweigh the consequences when caught. Knowing about the quantity of Cybercrime as well as the economic impact is vital for both governments as well as businesses which could be a necessary tool to adjust the legal and regulatory frameworks as well as institutional capacities. Prosecutors and law enforcement agencies must have resources, training and equipment required to address cybercrime in order to keep current on this newest method of crime fighting. Lack of reporting this crime leads to uncertainty with regard to the extent and impact. This is especially relevant with regard to the involvement of organized crime. Available information from the crime statistics in India, if at all available, does not reflect the real extent of the crime or damages cause as a result of the crime. Different motivations of private users and businesses not to report Cybercrime is another concern for the Government [9].

What is known is that the losses caused by Cybercrime can be significant. Losses are not only related to direct financial losses but also necessary investments in Cyber security and loss of reputation when incidents happen. It is important to give guidance in this regard e.g. reporting obligation / establishment of reporting mechanisms (complaint center) [8].

5. Types of Cybercrimes most prevalence in Indian

(1) Assault by Threat – threatening a person with fear for their lives or the lives of their families or persons whose safety they are responsible for (such as employees or communities) through the use of a computer network such as email, videos, or phones.

(2) Child pornography – the use of computer networks to create, distribute, or access materials that sexually exploit underage children.

(3) Cyber laundering – electronic transfer of illegally-obtained monies with the goal of hiding its source and possibly its destination.

(4) Cyber stalking – express or implied physical threats that creates fear through the use of computer technology such as email, phones, text messages, webcams, websites or videos.[3]

(5) Cyber terrorism – premeditated, usually politically-motivated violence committed against civilians through the use of, or with the help of, computer technology. [9]

(6) Cyber theft is using a computer to steal. This includes activities related to: breaking and entering, DNS cache poisoning, embezzlement and unlawful appropriation, espionage, identity theft, fraud, malicious hacking, plagiarism, and piracy.

a. Hardware Hijacking - Researchers at Columbia University recently discovered a serious security flaw in certain printers, as well. Many printers automatically update their software when accepting a print job, connecting to the Internet to download the latest print drivers.

b. Spam - Unsolicited mass e-mail, known colloquially as ¯spam , is more than annoying: spam messages can be used to trick people into giving up sensitive personal information (known as ¯phishing), or as carriers for computer worms and viruses. [1]

c. Script kiddies-A wannabe hacker. Someone who wants to be a hacker (or thinks they are) but lacks any serious technical expertise. They are usually only able to attack very weakly secured systems.

d. Insiders-They may only be 20% of the threat, but they produce 80% of the damage. These attackers are considered to be the highest risk. To make matters worse, as the name suggests, they often reside within an organization

(7) Yahoo Attack:- Also called 419 because section 419 of the Indian criminal code has a law against such offenders. It is characterized by using e-mail addresses obtained from the Internet access points using e-mail address harvesting applications(web spiders or e-mail extractor). These tools can automatically retrieve-mail addresses from web pages. Indian fraud letters join the warning of impersonation scam with a variation of an advance fee technique in which an e-mail from Indian offers the recipient the chance to share a percentage of a huge amount of money that the author, a self-proclaimed government official, is trying to siphon out of the country

(8) Salami Attack:-Salami assaults are flamboyant economic scams or exploits against confidentiality by comprehensive data gathering.[9]

6.Analysis of Data

The responses to the questions in the questionnaire provided the basis for the following analysis. *Perceived awareness level of respondents to cybercrimes Source:

It shows clearly that cracking is a major crime in our society with the frequency of 29 and percentage of 52.7% while the least which was strongly disagree went for 1 with a percentage 1.8%. This improvement may not be too far from the fact that Internet is almost available for every user. Almost the same level of awareness goes for pornography, software piracy and ATM fraud with the frequencies of 22, 29 and 29; and percentages of 40%, 52.7%, 52.7%. It won't be out of place if we assume that the increment in all these mentioned cases are also as a result of the availability of Internet connectivity.

Another prominent cybercrime we have in our society today is the yahoo-yahoo (cyber extortion) which seem uncontrollable,

That 25 respondents strongly agreed that it is a noticeable crime with a percentage of 45.5% while only 1 respondent remained undecided with a percentage of 1.8%. Despite the high level of benefits derived from the use of the Internet, it almost seems the disadvantages are appearing to be overwhelming.

7. Conclusion

In India, there is no doubt that a good number of people have turned the ethical use of information and communication technologies into unethical activities. This problem is not peculiar to India alone, but it is a problem world-wide and that is why it becomes imperative that organizational data /information must be safeguarded especially these days that almost every business is being run on line. our investigation on cybercrimes we observed its threat to the economy of a nation and even peace and security. Therefore there is need for a holistic approach to combat these crimes in all ramifications. Our proposal therefore is the need for cyber police who are to be trained specially to handle cybercrimes in India. In addition, the police should have a Central Computer Crime Response Wing to act as an agency to advise the state and other investigative agencies to guide and coordinate computer crime investigation. We are also proposing that the country should set up National Computer Crime Resource Centre, a body, which will comprise experts and professionals to establish rules, regulations and standards of authentication of each citizen's records and the staff of establishments and recognized organization, firms, industries etc.Forensics commission should be established, which will be responsible for the training of forensics personnel/law enforcement agencies. Above all, comprehensive law to combat computer and cyber related crimes should be promulgated to fight this phenomenon ¯to a halt. Our proposal on the nature of law to combat cybercrime is not included in this paper. We recommend that before anybody enters into any kind of financial deals with anyone through the internet he/she should use any of the search engines to verify the identity of the unknown.

References

· Shinder, D.L.(2002), Scene of the Cyber crime: Computer Forensics Handbook.

Syngress Publishing Inc. 88 Hingham Street, USA

· Eric A. Fischer. (2106). Cybersecurity Issues and Challenges: In Brief. [Online]. Available from https://fas.org/sgp/crs/misc/R43831.pdf [Accessed on October 201

· Criminal Investigation Department Review, January 2 (Mis Cyber Crime Scenario In India Criminal Investigation Department Review January 19 , 2008 [4] Hawser, A. (2011). Hidden threat. Global Finance, 25(2), 44

· Manmohan Chaturvedi, AynurUnal, ShilpaBahl. International cooperation in cyber space to combat cyber crime and terrorism. 2014 IEEE Conference on Norbert Wiener in the 21st Century (21CW). IEEE, 2014.

· Milner, H. V. (1999). The political economy of international trade. Annual Review of Political Sci-ence, 2, 91–114

· Martin, Nigel, John Rice. Cybercrime: Understanding and addressing the concerns of stakeholders. Computers and Security. 2011; 30(8): 803–814.

· Conference proceedingbyYerra Shankar Rao "Cyber crimeAssement "National Conference on Current Trends in Computing (NCCTC) ISBN No. : 978-3-642-24819-6, 23rd -24th March, 2014,Page no10-14.,North Orissa University ,Baripada Orissa

· Sergey, Melnik, Smirnov Nikolay, Erokhin Sergey. Cyber security concept for Internet of Everything (IoE). Systems of Signal Synchronization, Generating and Processing in Telecommunications. 2017. IEEE, 2017.

· Shang H, Jiang R, Li A. A Framework to Construct Knowledge Base for Cyber Security. 2017 IEEE Second International Conference on Data Science in Cyberspace (DSC). IEEE, 2017.

· India emerging as major cyber crimecentre (2009), Available at: http://wegathernews.com/ 203/india-emerging-as-major-cyber-crime-centre/, Visited: 10/31/09

· Rayne Reid, Johan Van Niekerk. From information security to cyber security cultures. Information Security for South Africa (ISSA). 2014. IEEE, 2014.

· R. Hewett, S. Rudrapattana, P. Kijsanayoth. Cyber-security analysis of smart SCADA systems with game models. Proceedings of the 9th annual cyber and information security research conference, ACM, 2014, pp. 109–112.

· Types ofcyber crime, http://www.slideshare.net/ferumxxl/types-of-computer-crimes. Accessed on December 2012

· Von Solms, Rossouw, Johan Van Niekerk. From information security to cyber security. Computers and Security. 2013; 38: 97–102.

❑❑❑

35

Scope of cyber security while using Digital Banking Transactions in India

Mr. Hemant Pandharinath Patil
Asst.Prof. Dept. of Commerce,
D. G. Ruparel College Matunga, Mumbai

****

Abstract :

Banking now a days is very easy and handy to use. Who would have thought about 24 x 7 banking even 2 decade back. With evolution in technology digital banking grows very fast. Usage of digital banking through internet, mobile phone, ATM card, POS machine etc. leads to threat in cyber security. Many time cyber-crime may takes place because of lack of awareness and lack of proper education in this regard. Internet Banking user generally leak information like OTP, phishing to someone else, visiting wrong website, malware, insufficient protection to device, launching free antivirus with insufficient security in device, less security in Banking APPs etc give birth to cyber-crime. User generally keep same password for his/ her social media and banking APPs. Social media account may get hacked. It may also lead to money laundering by fraudulent which may be used for some harmful purpose to society.

Key words : OTP, malwares, RBI, antivirus, APPs, Money laundering, social media, hacked.

Introduction :

Banking is back bone of daily transactions. Almost every bottom person in a country use mobile phone. But digital banking make it happen. The Credit card was introduced in India in 1980 and in the same year payment terminal – POS machine comes into existence. POS was The first evolution in digital banking space in India. With introduction of ATM machine 24 x 7 banking was started in India. Then with technological development in mobile phone different banking APPs were innovated. Use has access to theses banking APPs 24 x 7 to process banking or financial transactions anywhere and any time. Latest technology make it possible. Now one can do banking transactions at any time. In 1995 internet services was introduced in India, but in banking space online banking was started for the first time in India by ICICI Bank in 1996 through their branches. Slowly all other banks like HDFC Bank, Indusind Bank, Citi Bank etc have started giving internet banking facilities to its customers by the year 2000. Today all most all banks are providing internet banking facility. Former RBI governor Raghuram Rajan made some drastic changes in digital banking space. He is the first one to introduce UPI (Unified Payment Interface) service in India in the year April 2016. Another evolution in digital banking space was E-wallet. First mobile wallet come in India in the year 2004by Oxigen, in 2009 Mobikwik. Later Paytm, G-pay, Amazon pay, PhonePe, Airtel Money etc come into action. With the excess use of mobile and internet banking role of cyber security plays very vital role. On one hand one can access his bank account 24 x 7 and can send money across the world, but at the same time its risk is also high. Cybercrime is one of the rapidly increasing crimes hitting the world today. It is largely driven due to the increased exposure of information on the internet via cloud services. Networks and devices managing the infrastructure can be disrupted on a wide scale. Here stopping identity theft isn't the only goal, but protecting data integrity is. As cybercriminals are becoming more sophisticated, we need to understand their change in target, how are that affecting organizations, and their methods used in targeting.

2. Research methodology

2.1 Purpose of study

The study was intended the scope of cyber security with respect to Digital Banking

2.2 Objectives of study

To study the scope the cyber security.

To aware users about safe use of Digital Banking

2.3 Method of data collection

The data was collected using secondary data sources namely journal magazines business articles websites government records etc.

2.4 Scope of study

An attempt was made by the researcher to restrict the scope of study to Digital Banking in India

3. Analyses of Findings

Digital banking is very popular among the young star. With the latest technology and smartphone young star getting attracted towards Digital world. The increase in number may be due to discount offer, ease to operate, no need to go out personally, points earned etc. Even old age people are moving towards the digital banking platform more. India ranks highest in the usage of digital payments in the current scenario. The study highlights that the usage of digital payments amongst Indian consumers in the current scenario stood highest at 75 per cent, followed by China (63 per cent) and Italy (49 per cent). The global average stood at 45 per cent.

Though these percentage are very high, but with theses high percentage the chances of crime also increases. There are different type of crimes that may take place while digital banking usage

Hacking

Hacking is basically gaining unauthorized access to your system profit, protest, information gathering, or to evaluate system weaknesses.

Denial of Service

It brings down the server (any server). It is known as the flooding machine with requests in an attempt to overload systems. It also uses bots for tasks.

Virus Dissemination

It involves direct or search unauthorized access to system by introducing malicious programs known as viruses, worms etc. Virus needs host while worms are standalone.

Credit Card Fraud

Card fraud begins either with the theft of the physical card or with the comprise of data associated with the account.

Phishing

A malicious individual or group who scam users. They do so by sending e-mails or creating web pages that are designed to collect an individual's online bank credit card, or other login information.

Cyber Stalking

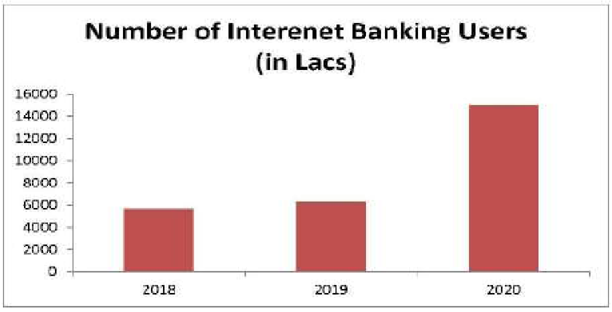
It can be defined as the use of electronic communications to harass or frighten someone, for example by sending threatening emails, messages etc

Modus Operandi

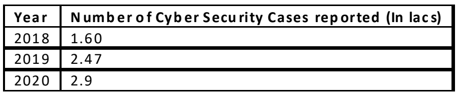
1. Sending Annoying Text Massages and Multimedia Messages
2. Making Offensive calls
3. Data theft
4. Identity theft
5. Providing attractive discount
6. Giving free offers

Number of Internet Banking users in India from 2018 to 2021

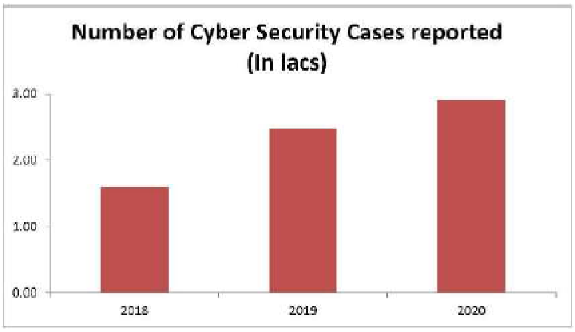
Year	Number of Users (in Lacs)
2018	5660
2019	6270
2020	15000



Number of Cyber Crimes Reported across India from 2018 to 2020



Year	Number of Cyber Security Cases reported (In lacs)
2018	1.60
2019	2.47
2020	2.9



Thought the number of cyber security cases reported are very low as compere to the number of users. This may be due to awareness by different payment bank link Airtel Payment Bank, Paytm Payment Bank, Google Pay etc. These all service providers aware their customer through advertisement to not to accept any request from unknown number. It is very important that the customers is very well aware with cyber security factors to avoid frauds and fraudulent transactions. The problem is arise when most of the young kid using their internet banking or pocket or UPI account. When we say young kind they are in age group of 18-30. Many time majority of this group is inexperience

In India there is increased in the usage of internet banking transactions as a result of Covid 19. RS 25.5 billion real-time payments transactions were processed in the country followed by 15.7 billion in China, 6 billion in South Korea, 5.2 billion in Thailand, and 2.8 billion in the UK. Among the top 10 countries, the US was ranked ninth with 1.2 billion transactions. The transaction volume share for instant payments India, among real-time transactions, was 15.6 per cent and 22.9 per cent for other electronic payments in 2020, according to a report by the US-based payments system company ACI Worldwide. Importantly, paper-based payments continued to have a considerable share of 61.4 percent in India.

Why Is Cyber Security Important In Banking?

1) Excess usage of Digital transactions, digital money. In this context, taking all the security measures is important to protect the data and privacy.

2) Data leaked by most of the organization, many time through internet or social media. E.g. birthday on face book, profile not locked on social media can be viewed by anyone.

3) Many time data given by banks to phone banking officer or any other officer by bank to sell or cross sale that particular officer may not be loyal to bank

4) Lost or stolen of card my be possible give information of yours which may be sensitive

5) Many personal and sensitive information is stored in mobile phone, like password, card details etc. Digital banking Apps are also installed. Lost or stolen of mobile phone but not blocked the phone on time may be harmful

6) Sharing details like Aadhar number, PAN number to any unknown persons. Also sharing personal information like OTP, Password to unknown person

7) Banks need to be on their guard 24/7; if not, your data with the bank can be breached.

4. How to do safe Online Banking to avoid fraud and financial loss?

1) Keep Financial data separate and do not store it in mobile phone or make it public

2) Always ask who is speaking over phone, ensure that you will not share any private and personal information to any unknown person. Bank or Non Banking financial institution never ask to share any private and personal details

3) Keep password of credit card, Debit Card and digital banking channel safe and separate. Keep on changing all the passwords in regular interval. One should avoid password such as Birthdate, Room no, Building No etc so

that fraudulent can trace the same

4) Never share the OTP received on your phone as well as on your email

5) When ATM Transactions are processed, ensure that you carry your card and cancel all the transactions visible on screen

6) Take cyber awareness training to avoid fraud

7) If debit or credit card is lost or stolen, immediately hotlist the card by contacting your bank.

5. Conclusion:

All uses must use digital banking channel with much more integrity and care. Fraud can happen anytime and by anyone. It is very important that the digital banking password even can not be shared even to relative many time. It is our social, ethical as well as personal responsibility that we must use internet banking with some extra care. It is after all over heard earned money that we are dealing with. One must remember that no body in the world will give you anything free, so please avoid to trap in such a fraud offers. Be safe and keep your finance safe. Any fraud message or emails must be identified. Phishing is one of the difficult type to identify, 50% of digital banking frauds are processed from phishing, but we must check the email sender before clicking on any financial transactions related emails. Similarly message also carry link and messages tells about free offer or heavy discount or credit of money in account. Theses are sign of frauds. We just have to think wisely and process our banking transactions.

6. Bibliography :

Braga, F.D., Isabella G and Mazzon J.A., (2013). Digital wallets as a payment method influence consumer in their buying behaviour, Available at Internet desk. (2016, Nov. 12). Recalibration of ATMs will take up to three weeks, says Jaitley. The Hindu.

Jinkook, Fahzy Abdul-Rahman, and Hyungsoo Kim. "Debit card usage: an examination of its impact on household debt." Financial Services Review. 16.1 (2007): 73.

Mercatanti, Andrea, and Fan Li. (2014). "Do debit cards increase household spending? Evidence from a semiparametric causal analysis of a survey." The Annals of Applied Statistics. 8.4: 2485-2508.

Jafar Alghazo (2017) Cyber security analysis of internet banking in emerging countries: User and bank perspectives

7. Websites :

https://www.business-standard.com/article/finance/over-290-000-cyber-security-incidents-related-to-banking-reported-in-2020-121020401220_1.html

http://www.legalserviceindia.com/legal/

https://www.thehindubusinessline.com

https://www.financialexpress.com/industry/banking-finance/digital-payments-india-pips-china-us-others-in-2020-leads-global-tally-with-this-many-transactions/2226074/

❑❑❑

36

Science Technology And Cyber Crime

Dr. S. R. Suryavanshi
Lecturer, Head of Department,
Department of Hindi,
S.K.M, Shirwal

****

Abstract

Cyber science, responding to the cyberization trend, aims to create a new collection of knowledge about these cyber-enabled worlds, and provide a way of discovering what is in the cyber-enabled worlds and how they work. Cyber science is concerned with the study of phenomena caused or generated by the cyberworld and cyber-physical, cyber-social and cyber-mental worlds, as well as the complex intertwined integration of cyber physical, social and mental worlds. It fuels advances in cyber technology, beyond the existing cyber related technologies. In this paper, after discussing the cyberization background and process, and explaining cyber science and technology, we present our visions and perspectives on new opportunities, essential issues and major challenges for cyber science and technology. We further describe cyber related technologies and closely related existing research areas, and envision future research directions, in terms of cyber physical, cyber social, cyber life, cyber intelligence and cyber security, which are five basic dimensions of cyber science and technology.

INTRODUCTION

Few things are more suspect than a claim of the birth of a new science. Yet, in the last few years, terms like “Science of Cyber,” or “Science of Cyber Security,” or “Cyber Science” have been appearing in use with growing frequency. For example, the US Department of Defense defined “Cyber Science” as a high priority for its science and technology investments (Lemnios 2011), and the National Security Agency has been exploring the nature of the “science of cybersecurity” in its publications. This interest in science of cyber is motivated by the recognition that development of cyber technologies is handicapped by the lack of scientific understanding of the cyber phenomena, particularly the fundamental laws, theories, and theoretically-grounded and empirically validated models (JASON 2010).

Lack of such fundamental knowledge – and its importance – has been highlighted by the US President’s National Science and Technology Council (NSTC 2011) using the term “cybersecurity science.” Still, even for those in the cyber security community who agree with the need for science of cyber — whether it merits an exalted title of a new science or should be seen merely as a distinct field of research within one or more of established sciences — the exact nature of the new science, its scope and boundaries remain rather unclear.

CYBER CRIME

Cybercrime encompasses a wide range of crimes including stealing people’s identity, fraud and financial crimes, pornography, selling contraband items, downloading illegal files etc. According to the laws, any crime involving a computer and Internet is called cyber crime. Some of the popular and alarming crimes in the cyber world are discussed below:

A. **Financial Crimes** : With the increasing demand of the on-line banking, the financial crimes have become very alarming. Financial crimes include credit card frauds, stealing money from on-line banks etc. The criminals of credit card fraud get information from their victims often by impersonating a Government official or people from financial organizations asking for their credit information. The victims fall prey to this without proper inquiries and give away their credit card information to these criminals. In this ways, criminals may steal their identity and the consequences are mostly financially damaging.

B. **Cyber Terrorism** : Terrorism acts which are committed in cyberspace are called cyber terrorism. Cyber terrorism may include a simple broadcast of information on the Internet about bomb attacks which may happen at a particular time in the future. Cyber terrorists are people who threaten and coerce an individual, an organization or even a government by attacking them through computers and networks for their personal, political or social benefits.

C. **Cyber Stalking** : 'Stalking' as has been defined in Oxford dictionary, means "pursuing stealthily". Cyber stalking is following an individual's or organization's whereabouts on the Internet. These may include sending threatening or nonthreatening messages on the victim's bulletin boards, which may be by social networking sites or even through e-mails. According to David Wall, one of the prevalent forms of Cybercrime is Cyber stalking.

This is basically a crime where the individual is constantly harassed by another individual example, sending constant mails to any individual with unsuitable contents and threat messages.

D. **E-mail Spoofing and Phishing Scams** : Cyber criminals often spoof e-mails of known and unknown individuals. E-mail spoofing basically means sending an e-mail from a source while it appears to have been sent from another e-mail. E-mail spoofing is a very common cause of monetary damages. The act that attempts to obtain vital information like passwords, details of credit cards by pretending to be a trustworthy entity in an electronic company is called phishing. Phishing e-mails are likely to contain hyperlinks to the sites containing malwares.

E. **Misuse of e-mail and Personal Information** : Information about user's activity on the Web is being recorded and there will be privacy losses. Many users are not aware about it. Web users leave a "data shadow" with information about what they read, where they shop, what they buy, whom they correspond with and so on. High-volume server can track significant information about a user's browsing habits. Many advertising companies share user profiles and build massive databases containing users and their data shadows. When users select set of trusted re mailers, the message recipient can not tell where the message originated. There are many such re mailers available for use. Attackers can send junk mail free of charge. If they have to pay for each thing they sent, there would be fewer attacks. It would be harder to steal people's accounts if it cost the victims money.

There are ways to keep data safe. A. D. Rubin, D. Geer and M. J. Ranum discuss about security in more detail in their Book "Web Security Source".

Few Impacts Of Cyber Crime

· **Emotional Impact of Cyber Crime** : The first study to examine the emotional impact of cybercrime, it shows that victims' strongest reactions are feeling angry (58%), annoyed (51%) and cheated (40%), and in many cases, they blame themselves for being attacked. Only 3% don't think it will happen to them, and nearly 80% do not expect cybercriminals to be brought to justice— resulting in an ironic reluctance to take action and a sense of helplessness. We accept cybercrime because of a 'learned helplessness', said Joseph LaBrie, PhD, associate professor of psychology at Loyola Marymount University. It's like getting ripped off at a garage – if you don't know enough about cars, you don't argue with the mechanic.

People just accept a situation, even if it feels bad."Despite the emotional burden, the universal threat, and incidents of cybercrime, people still aren't changing their behaviors - with only half (51%) of adults saying they would change their behavior if they became a victim

Cybercrime victim Todd Vinson of Chicago explained, I was emotionally and financially unprepared because I never thought I would be a victim of such a crime. I felt violated, as if someone had actually come inside my home to gather this information, and as if my entire family was exposed to this criminal act.

Now I can't help but wonder if other information has been illegally acquired and just sitting in the wrong people's hands, waiting for an opportunity to be used. The "human impact" aspect of the report delves further into the little crimes or white lies consumers perpetrate against friends, family, loved ones and businesses. Nearly half of respondents think it's legal to download a single music track, album or movie without paying. Twenty four percent believe it's legal or perfectly okay to secretly view someone else's e-mails or browser history. Some of these behaviors, such as downloading files, open people up to additional security threats.

· **Impact of Cyber Crime over Teenager** : These days a worst fear in teenager's eyes is Cyber Bullying. It is become common over past five years, generally from the age below eighteen are more susceptible and feared from Cyber Bullying as per inspection. It is becoming an alarming trend in our society. As per inspection of data, the worst fear of cyber crime is on teenagers female. Cyber Bullying is a fear when person receives threats, negative comments or negative pictures or comments from other person. This is all done through core technologies described above mainly via online. Cyber Bulling can be done through chatting, instant messaging etc. Where website like Facebook, Orkut, Twitter user are more affected from Cyber Bullying. In my analysis generally feared person can reach a limit of depression, humiliation and threatens. Through this analysis we come to analyze that if person Bulled online he or she may be depressed up to the level of self harming.

· **Impact of Cyber Crime over Youth** : Cyber communication is society's newest way to interact. Online social networking websites, text messages and emails provide users with an effective, quick way to communicate with people all over the world. Teens in particular spend hours online every day, on computers or personal electronic devices.

CONCLUSION

We also need latest technology and more importantly technical staff who understand and make use of this technology. Misuse of social media can be done within minutes, whereas cells are working at very slow speed. It may lead to decades to resolve the cases and by that time in some sensitive cases damage is already done. Time is now to act instead react. Sometimes there is dependency on foreign agencies. We know that laws are different in different countries. This causes further delay. There is urgent need of ethical hackers who can go to the root cause of criminals. Looking at the growth of social media in India, we require at least Fifty thousand ethical hackers. Good opportunity for such job seekers.

Some of the recent bollywood movies and TV serials broadcast criminal cases and the process of catching the criminals. But in large populated country like India, criminals are becoming smarter and get lesson from the episodes. We as member of society person should consider, think and give right directions to new generations to come.

❑❑❑

37

Analysis of Correlation between Chemical Factors of Ashti Lake, Dist. Solapur (M.S.)

A.L. Shaikh
Arts, Science and Commerce College,
Mokhada, Dist. Palghar (M.S.)

S.D. Kambale
V.G. Vaze College of Arts, Science and
Commerce, Mulund (E), Mumbai (M.S.)

S.K. Pawar
Arts, Science and Commerce College,
Mokhada, Dist. Palghar (M.S.)

A.A. Koparde
Dahiwadi College, Dahiwadi Dist. Satara (M.S.)

****

Water, being permissible to many molecules contains various elements in it. During present investigation chemical parameters of Ashti lake, Dist. Solapur (M.S.) were analyzed during March 2019 to February 2020. Ashti lake is the huge water body which supply water to the 22 nearby villages. The study reveals that these chemical parameters are correlated with each other. Further all those parameters are within standard permissible limits of water quality. Results are discussed with recent literature.

Keywords- Chemical parameters, Ashti Lake, Correlation

Introduction

Natural water contains many types of the molecules and particles either dissolved or suspended in it. Water is amongst the basic need for being alive due to the fact that almost all cellular activities need water. Hence water is the prime necessity of all living organisms including human. Natural water is source of drinking water and it is also used in agricultural farms. Potability of water is dependent on the chemical entities present in it, their amount and proportion. Hence it become necessary to study these parameters present in water. In any naturally occurring aquatic ecosystem chemical parameters are correlated with each other (Welch, 1952). Chemical factors and molecules are added into the water bodies from rock, soil, precipitation and anthropogenic activities. These chemical factors are inter-related and they have impact on one another, which eventually have its effect on suitability of water for drinking purpose. This states the importance of comparative study while analyzing chemical nature of water of an aquatic ecosystem (Wetzel, 2001). Though the water is prime necessity of life, even of the human, it is getting polluted day by day. According to Wetzel (2001), freshwaters of the world are facing rapid harmful qualitative and quantitative effects on water. Ingress of unwanted components by natural process and human activities is leading to serious water pollution issues which may end up into huge loss of potable water resources. There is tolerable range of limit regarding water quality parameters within which all living organisms can live; disturbances in these limits may pose serious effects on the liveliness of these organisms (Devenport, 1993).

Many researchers have carried out investigation of chemical parameters of water of various aquatic bodies few of them are Kate et al. (2020), Jadhav and Jadhav (2020), Roy (2018), Mulla and Bhosale (2016), Mane (2013). Present investigation is an attempt to assess the chemical nature of water of Ashti lake by analyzing few chemical parameters and correlation between them.

Material and Methods

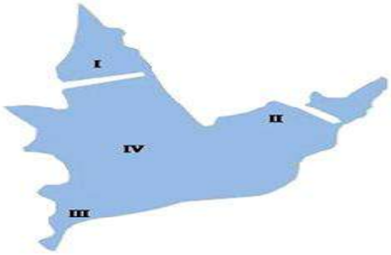
Material-

Present investigation is carried out at

Ashti Lake, Dist. Solapur (M.S.). This huge water body is located in Mohol Tahsil of Solapur District (M.S.). It is situated 22 km away from Pandharpur. Ashti lake comes under Madha subdivision of irrigation department of Maharashtra State. The lake is situated at $17^0 47'$ N to $17^0 48'$ N along latitude and $75^0 25'$ E to 75^0 to $26'$ E along longitude. It is present 458 meter above mean sea level.

The Ashti lake was built in 1881 by the British government. The lake is large and spread over an area of about 2830 acres. The lake is perennial and act as source of water for drinking and irrigation purpose. It provides water to the more than 22 villages present nearby. Water input to this lake is through the annual precipitation in that area and the lake is also connected to Ujani dam.

Present investigation was carried out during March 2019 to February 2020. Water was collected from selected sites monthly. Chemical parameters opted to study was analyzed into the laboratory except pH. The pH of water was observed at the sites itself with the help of Digital pHmeter. Rest of all chemical parameters was analyzed into the laboratory by using standard prescribed methods.



Ashti Lake Showing Study Sites

Method-

During present investigation water was collected from the selected 4 sites early in the morning. Water samples were analyzed in the laboratory by using methods prescribed by APHA (2012), Ragothaman and Trivedi (2002), Trivedi and Goel (1984) and Trivedi et al. (1998).

Correlation between parameters was analyzed by using MS EXCEL, Microsoft Office, 2007. The correlation matrix is prepared, which is the tabular representation of correlation pattern between parameters. Correlation values are shown in body of the table and various selected parameters are placed diagonally in respective caption and stub. Positive correlation values represent positive correlation between parameters while negative values represent negative correlation between parameters. Values near zero represent no correlation between parameters.

Results and Discussion

During present investigation some selected chemical parameters were analyzed, results obtained in this investigation are shown in table 1. While the correlation pattern obtained is shown with help of correlation matrix in table 2.

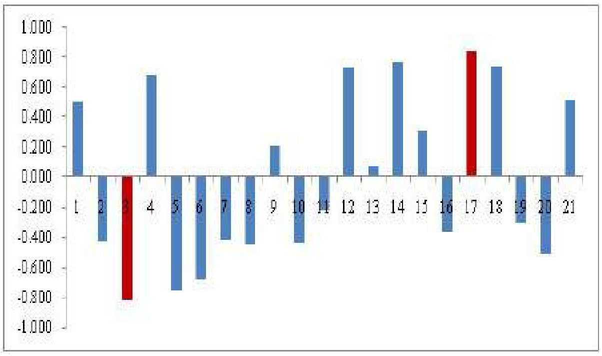
Table 1: Monthly variation in few chemical parameters of Ashti Lake during March 2019 to February 2020.

Months	Sites	Parameters						
		DO (mg/l)	Free CO_2 (mg/l)	Hardness (mg/l)	BOD (mg/l)	Phosphate (mg/l)	pH	Alkalinity (mg/l)
March 2019	I	3.3	1.8	203	9.5	5.3	8.6	125
	II	3.2	2.2	199	9.4	5.4	8.5	121
	III	2.9	2.0	219	9.2	4.9	8.6	129
	IV	3.5	1.6	201	9.0	5.2	8.3	126
April 2019	I	4.1	2.3	210	14.2	4.3	8.5	185
	II	3.2	2.2	217	14.3	4.2	8.4	188
	III	4.4	1.9	221	15.4	4.9	8.3	190
	IV	4.6	2.2	199	16.2	5.2	8.5	186
May 2019	I	2.9	3.5	219	14.7	6.9	8.9	200
	II	3.5	3.6	203	15.1	6.2	8.9	220
	III	2.8	4.2	210	14.7	6.5	8.5	202
	IV	2.7	3.4	208	15.2	7.1	8.7	199
June 2019	I	5.4	6.9	171	4.6	4.8	8.0	121
	II	5.3	6.2	179	5.2	5.2	8.1	115
	III	4.9	6.5	183	4.9	4.5	8.0	120
	IV	5.2	6.6	171	4.0	5.0	8.1	123
July 2019	I	5.4	4.3	144	4.6	9.7	7.5	129
	II	5.3	4.2	150	5.2	10.1	7.6	130
	III	6.1	4.3	146	4.2	9.8	7.5	125
	IV	5.2	4.0	149	4.4	9.5	7.9	130
August 2019	I	8.1	3.8	149	2.3	11.3	7.2	101
	II	7.5	3.9	140	1.9	11.5	7.1	99
	III	8.4	3.1	143	2.5	10.9	7.0	102
	IV	7.9	3.5	142	2.8	11.4	7.2	103
September 2019	I	8.3	10.2	160	1.5	11.4	7.2	120
	II	8.9	10.2	161	1.0	10.2	7.2	115
	III	8.2	9.1	180	0.9	11.9	7.1	117
	IV	7.6	10.0	166	1.6	12.1	7.3	118
October 2019	I	6.3	8.7	161	3.7	5.4	7.3	118
	II	6.9	8.6	163	3.2	5.3	7.5	119
	III	7.2	8.5	179	4.2	4.9	7.9	110
	IV	6.5	8.3	162	3.9	5.2	7.8	115
November 2019	I	5.8	16.6	101	4.4	5.2	7.4	136
	II	6.1	16.1	102	4.3	4.3	7.9	123
	III	5.5	15.9	110	4.0	5.2	7.5	132
	IV	5.7	15.0	119	4.2	5.1	7.6	135
December 2019	I	4.1	0.0	125	6.5	2.5	7.1	162
	II	3.7	0.0	131	6.2	2.6	7.9	159
	III	4.9	0.0	129	6.9	3.0	7.5	171
	IV	4.3	0.0	138	7.0	2.6	7.8	155
January 2020	I	4.3	0.0	138	5.7	2.4	8.3	159
	II	4.8	0.0	142	5.3	2.1	8.5	160
	III	4.0	0.0	129	6.2	2.5	8.7	148
	IV	4.1	0.0	130	5.7	2.9	7.9	152
February 2020	I	5.1	0.0	182	8.4	8.3	8.2	101
	II	5.9	0.0	175	8.3	8.2	7.8	115
	III	4.8	0.0	183	9.0	7.9	8.2	109
	IV	5.1	0.0	173	7.9	8.0	8.1	114

Table 2: Coefficient of correlation (r) and coefficient of determination (r^2) between water parameters of Ashti Lake during March 2019 to February 2020.

Sr. No.	First parameter (X)	Second parameter (Y)	r	r^2
1	DO	Free CO2	0.503	0.253
2	DO	Hardness	-0.431	0.186
3	DO	BOD	-0.817	0.668
4	DO	Phosphate	0.676	0.457
5	DO	pH	-0.754	0.569
6	DO	Alkalinity	-0.679	0.461
7	Free CO2	Hardness	-0.417	0.174
8	Free CO2	BOD	-0.449	0.202
9	Free CO2	Phosphate	0.209	0.044
10	Free CO2	pH	-0.436	0.190
11	Free CO2	Alkalinity	-0.224	0.050
12	Hardness	BOD	0.734	0.539
13	Hardness	Phosphate	0.072	0.005
14	Hardness	pH	0.768	0.590
15	Hardness	Alkalinity	0.306	0.094
16	BOD	Phosphate	-0.358	0.128
17	BOD	pH	0.833	0.695
18	BOD	Alkalinity	0.736	0.541
19	Phosphate	pH	-0.305	0.093
20	Phosphate	Alkalinity	-0.511	0.261
21	pH	Alkalinity	0.506	0.256

Graph 1: Bar diagram showing correlation coefficients



The results obtained from the present investigation reveal that all the chemical parameters under study are well within prescribed limits of WHO (Table 1). Dissolved Oxygen is in the range from 2.7 to 8.9 mg/l, Free CO_2 is maximum 16.6 mg/l while CO_2 is absent in free form in few months during investigation. Total hardness of the water of lake is found to be in the range 101 to 221 mg/l. Maximum Biochemical Oxygen Demand (BOD) found was 16.2 mg/l while minimum BOD was 0.9 mg/l. Phosphates in the water of Ashti lake were in the range from 2.1 to 12.1 mg/l. pH of the water of Ashti lake was found to be alkaline and in the range from 7 to 8.9. Alkalinity of the water is 99 to 220 mg/l.

During present investigation it is observed that all selected chemical parameters are correlated with each other. The pattern of correlation is shown in Table 2, where correlation is represented by r values. Dissolved oxygen is positively correlated with free CO_2 and Phosphates while it negatively correlated with hardness, BOD, pH of the water and alkalinity. Free CO_2 is positively correlated with the phosphate and negatively correlated with the hardness, BOD, pH and alkalinity. Hardness is positively correlated with the BOD, Phosphate, pH and alkalinity. Phosphate is negatively correlated with pH and alkalinity while pH is positively correlated with alkalinity. Further all the values of coefficient of determination indicate the impact of parameters on one another, which further reveals interdependency of all the selected parameters. The results obtained in the present investigation are in corroboration with the results of Bhandari and Nayal (2008), Alam et. al., (2015), Kothari et.al., (2021) and Shroff et. al., (2015).

Conclusion:

During present investigation the water sample of the Ashti lake is analyzed from March 2019 to February 2020. Some of the chemical parameters are selected for analysis. All the chemical parameters selected for this investigation are well within permissible limit prescribed by WHO. Hence the water of Ashti lake is fit for potability and agricultural uses. Further all the chemical parameters are correlated with each other and drop or raise in one parameter may lead to drop or rise in another. Though all the parameters are well within limit yet continuous monitoring and surveillance is needed for maintenance of water quality of Ashti lake.

References

Alam M.T., S. Sultana, S.K. Das and S.K.

Mazumder (2015). Water quality parameters and their correlation matrix: A case study in two important wetland beels of Bangladesh. Ciencia e tecnica Vitivinicola, Vol. 20 (40): 1-27.

APHA (2012). Standard methods for the examination of water and waste water. 22nd Ed. American Public Health Association, American Water Works Association and Water Environment Federation, Washington D.C. pp. 1-1 to 10-175.

Bhandari and Nayal (2008). Correlation Study on Physico-Chemical Parameters and Quality Assessment of Kosi River Water, Uttarakhand, e journal of chemistry. Vol. 5(2): 342-346.

Davenport, Y. (1993). Responses of the Blenniuspholis to Fluctuating Salinities, Mar. Eco. Progress Series 1: 101-107.

Jadhav and Jadhav (2020). Study of water quality parameters of Mula-Mutha River at Pune, Maharashtra (India). Int. J. of Lakes and rivers. Vol. 13 (1): 95-103.

Kate S., S. Kumbhar and P. Jamawle (2020). Water quality analysis of Urun Islampur City, Maharashtra, India. Applied Water Sciences. Vol. 10:95 pp. 1-8.

Kothari V., S. Vij, S.S. Sharma and N. Gupta (2021). Correlation of various water quality parameters and water quality index of districts of Uttarakhand. Environmental and Sustainability Indicators. Vol 9 (100093) pp 1-8.

Mane A. V.(2013). Water quality and sediment analysis at selected locations of Pavana River of Pune district, Maharashtra. J. of Pharma. Res. Vol. 5 (8): 91-102.

Mulla R.K. and S.M. Bhosale (2016). Water quality analysis and simulation of Panchaganga river using Matlab. Int. J. Eng., Sci., & Res. Tech. Vol 5(8): 613-620.

Ragothaman and Trivedi (2002). "Aqautic Ecology" Agrobios, Jodhpur. pp.1-247.

Roy R. (2018). An Introduction to water analysis. Int. J. for Env. Rehab. & Cons.Vol. 9(2): 94-100.

Shroff P., R.T. Vashi, V.A. Champaneri and K.K. Patel (2015). Correlation study among water quality parameters of groundwater of Valsad District of South Gujrat, India. J. of Fundam. & Appl. Sci. Vol. 7(3): 340-349.

Trivedy R. K. and P. K. Goel (1984). "Handbook of Chemical and Biological Method for Water Pollution Studies." Environmental publications, Karad pp. 1-247.

Trivedi, R.K., P.K. Goyal and C.L. Trishal (1998). "Practical Methods in Ecology and Environmental Science." Enviro. Media Publications, Karad.

Welch, P. 1952. "Limnology", 2nd Ed., McGraw- Hill Book Company, Inc., London pp. 1-538.

Wetzel, R.G. (2001). "Limnology- Lake and River Ecosystems" 3rd Ed., Academic Press, Elsevier Inc., London.

❑❑❑

38

Social Media and Cyber Security

Dr. Manjiri Karekar
Dept. of Politics,
S. P. College, Pune

****

Introduction- 17th and 18th centuries are referred as age of enlightenment while 20th century referred to as the age of Information and Technology. The past decade has witnessed as a boom in Information Technology as well as internet related technology. This has changed our society and our way of life. The internet has come a long way with even entire business being set up online to meet the need of modern day consumer. This development in the field of technology is a boon for humankind. But it can also be misused i.e. one's personal data and privacy are under constant threat in cyberspace. Now computers are unavoidable in our all aspects of life. There is misconception that all information posted by individuals remains private. But the information posted online can be accessed through a number of ways of data collection services and other techniques without consent of users. On this background we have to see cyber security.

Cyber security- Cyber security is important because it protects all types of data from theft and damage. This includes sensitive data, personally identifying information, protected health information, personal information, and intellectual property data, and government and industry information systems.

Cyber security is a necessary investment for government agencies. Technology has provided new ways for government agencies to work, interact with citizens and improve overall operations. Cyber security and attitudes towards it have undergone a significant change. Political motivation is the main driver behind cyber terrorism. The caliber of cyber terrorism attacks is significantly more harmful than average virus. This is because they are unforgiving and have more sinister intentions. As a result governing bodies have to create and continually rethink mitigation strategy.

Social networking sites are a popular medium of interaction and communication. Social networking sites provide the ability to run applications and games to test users' knowledge. The popularity of social networks makes it an ideal tool through which awareness can be created on existing and emerging security threats. Normally all people use face book, messenger, what's app, Twitter, Blogs, Linked in etc.

Presently social engineering is very famous threats for cyber criminals. It allows attacker to find out personal information of any individual. Attackers are making this information available online or from company database by using fake accounts or create trust over time, after getting trust from user, attacker start to collect personal impression of individual. Information includes name of the project, name of the server and go through website which drop a backdoor to their computer. Especially for stealing money and confidential information is carried out. Using system vulnerability, attacker develop fright and unease instead of, to get users to take part with their money and this is very specific and targeted attack and its chances are more to get success.

The most grave social media threats get emphasized when fake or bogus accounts have successful connection with so many people of various institutes, corporate and especially military and government and security firms.

Exploitation of celebrity names is the most popular way today. By using this method rumour is created and misinformation as well as to attack followers which can spam. There have been various examples where hacker is creating the account by using name of celebrity. Attacker is extracting individual's personal information to misuse it. There is no real authentication or identity check to protect against such kind of threats.

Apart from above mentioned things there are conciliation of websites, dissemination of spams, malware and reveal of confidential information also part of topmost social media attack.

Classification of Threats and Attacks on social media-

General Web attacks- Web is a very popular and inevitable part of human life now-a-days. In this context social media plays very pivotal role. There are seven threats on social media website.

1. Drive by downloads from mainstream websites are increasing. 2. Attacks are heavily obfuscated and dynamically changing making traditional antivirus solutions ineffective.3. Attacks are targeting browser plug-ins instead of only the browser itself. 3. Misleading applications infecting users are increasing. 4. SQL injection attacks are being used to infect mainstream websites. 5. Mal advertisements are redirecting users to malicious websites.6. It is observed explosive growth in unique and targeted malware samples.

Malware- Malware is any kind of software which is used to disturb operations performed by computer. It also gathers sensitive information or gaining access to private system. It can be in various forms including script, active content, executable code and other software. According to survey 70% malware are in software.

Vulnerabilities- It is a kind of weakness which gives a way to attacker to reduce performance of a computer system. There are various types of risks on social media sites due to vulnerability. Various tactics includes bating, click jacking, cross site scripting, Doxing, elicitation, Phraming, Phishing, Phreaking, scams and spoofing.

Malicious URL- These URLs are created for malicious purposes. It can be used to download any kind of malware which is affecting to the computer. It also contains other messages includes spam, phishing. It also improves its (URLs) position in search engines using blackhat technique of SEO.

Online interaction of people is creating more knotted life of them. In this case social media is the best option. It also opens opportunities of criminals of cyber as well as online threats. Criminal of cyber with various purposes try to contact with social media users to targets for scams, spam and other various types of attacks. With content updates, status online and sharing links, images and videos as well as sending secret messages or direct messages create possibility to exploit information of legitimate users.

Initiative of attacks- Millions of users is available on popular social media sites, including face book, twitter. It is the best destination for criminals to execute their criminal activities. When user is getting log on into website, he encounters various kinds of social media threats. Whenever they try to download any page, URLs, images it triggers spamming routine. All above things are uploaded by criminals who are already having their account on those websites. However it not only social media wall or anything on which attacks are taking place, but it also possible to send spam messages supposedly legitimate site of social media.

Users come across attacks- As all users are having various options to post on sites, same as those various options used by attackers to create different types of threats on social media.

Facebook- This is very simple in which criminals can post which acts as an attack. This includes celebrity talks and disasters. Users, who are clicking on this type of post it leads to repost malicious scripts, links, images, videos on user's wall. Some survey sites are also getting open when users like some post available on others wall which leads to profile making of cyber criminals. Another application leads users to play games, to add features of profiles and allow more stuff. Anyone can develop this kind of applications and submit which can be accessed by users. Hence criminals of cyber can also use this kind of opportunities to create spam or phishing attacks. The other types of attacks by facebook are done by chat features available in that. Messages coming in chat are used to spread application like phishing and malware spreading.

Twitter- It has limitations 140 characters for twitting any kind of massage. It is a short message. Criminals of cyber are using this limitation of short message to post links or short posts. For ex. To recharge vouchers, advertisement of jobs and products and many more. In Twitter individual user can upload link related to malware. It tricks to promote fake applications and backdoor applications. Fake U Tube links are also available.

Malware, spam, phishing and other attacks are very challenging foe social media in which they have to keep secret of user's profile and information. The final goal of social media is to enable another user to access information of one user and provide communication among different users as well. Some of the users are having such kind of perception that cyber criminal will not get benefits from their information. Cyber criminals can easily find out the way to explore more information to access anyone's accounts. The same things are related to corporate accounting systems. Linked can be the best example.

To keep your privacy and to defend from attacks and social media is not easy task. Individual can limit certain attacks. At the time of sign in automatically attacks and threats are taking place. There are various ways to defend and prevent various attacks on social media.

Some basic measures of precautions are there to avoid becoming victim of threats to social media. User should identify a bogus notification which takes the appearance about legitimate prompts from the exacting website of social media.

When individual user is trying to browse profile online that time user should keep in mind that everything which is available on the page is not at all safe. Cyber criminals are constantly waiting for opportunities to attack on any legitimate user of social media and their information.

Further, individual user should be enough experts to protect his data and its privacy as well. It would be best to accept and make mindset that information which is posted online is publically available. Along with this carefulness an individual must be aware about sensitivity and confidentiality of data and information. One must not share sensitive business information as well via private chat messages also. It is just because of when account is going to hacked by hacker they can collect all information about individuals business.

In addition to prevent this, user must be aware about security settings available in any social media websites.

Right to Privacy- Ultimately the issue of cyber security is related to right to privacy. In 2012 the UN human Rights Council affirmed the freedom of expression on internet is a basic human right which implies that the rights of individual existing offline must also be protected online. As per Article 21 of the Constitution of India, "No person shall be deprived of his life or personal liberty except according to procedure established by law." In India, right to privacy has not been mentioned expressly in the fundamental rights, but it has been carved out by the Supreme Court through an interpretation of right to life under Article 21 of the Constitution. Hence by theft of private data is affecting right to privacy. The most comprehensive provisions about privacy on internet can be found in Information and Technology Act (ITA) 2000. The ITA contains a number of provisions that can safeguard online privacy or dilute online privacy. Provisions, that clearly protects user privacy include: penalizing, hacking and fraud and defining data protection standards for body corporate.

Since 2010 there is increasing recognition by both the government and public that India needs privacy legislation specifically one that addresses the collection, processing, and use of personal data. In 2011 the Guidelines for Cyber Café rules were notified under Information Technology Act. These rules require Cyber Café to retain details of every user for a period of one year. Cyber Café must also retain history of Websites accessed and logs of proxy servers installed at Cyber Café for a period of one year. In October 2012 a report of the group of experts on privacy was published. The report provided recommendations for a privacy framework and legislation in India. The report recognizes privacy as a fundamental right and defines and defines nine National Privacy Principles that would apply to all data controllers both in private sector and the public sector. Thus privacy is an emerging and increasingly important field in India's society.

Cyber security laws and policies have a direct impact of human rights, particularly right to privacy, freedom of expression and the free flow of information. Policy makers have created several national policies with the intentions of protecting internet and other information communication technology systems against malicious actors. However many of the policies are broad and ill defined and lack clear checks and balances and other accountability mechanisms, which can lead to human rights abuses can stifle innovation.

Cyber security around the world- In 2014 erosion of cyber security was identifies as an emerging global trend. This can partially be attributed to increase in data breaches and cyber attacks against companies, governments and consumers, which have became more sophisticated in recent years. Cyber attacks went on increasing and y 2020 it became a key area of concern of digital economy.

Repressive laws, increased surveillance and regulatory control from governments such as China, Egypt, UK, Canada and France have also increased. These varied policies and practices are changing the nature of internet and creating challenges regarding its technical and legal fragmentation.

In underdeveloped countries like Latin America, Caribbean online users' lack of concern and awareness about the dangers of cyber crime and hacking has been feeding the high levels of cyber crime in the region. Efforts to solve this problem from a governmental level are often restricted by a lack of resources to build capacity and shortage of knowledge to implement cyber security policy.

In support of a governmental cyber security agenda and strategy development in Latin America, public knowledge is working with local civil society groups and experts for strategic development support, helping their coordination and local engagement in relevant local and global policy cyber security policymaking debates.

Role of Civil Society- It is critical for the civil society actors to deepen their knowledge and develop skills, including technical skills and understanding, to actively engage in policy discussions and measure appropriate responses. Civil society is uniquely positioned to advocate for cyber security policies based on human rights approach and can play an important role in monitoring and documenting government and business practices, identifying knowledge gaps and providing analysis to inform policies and relevant discussions.

References-

Ghosh Shantanu, 'Top Seven Social Media Threats", in article on http://searchsecurity.techtarget.in,2011

Gohel Hardik, 'Looking back at evolution of the internet', in article in CSI Communications-Knowledge Digest for IT Community, 2014

Cluley Graham, 'Malware and spam rise 70% on social networks, security reports revealed' at Sophon press release http;//www.sophos.com, 2010

http://forbesindia.com/article/checkin/indias-internet-privacy-woes/35971/1

http://planningcommission.nic.in/reports/genrep/rep_privacy.pdf (Report of the Group of Experts on Privacy)

www. Right to Privacy and Cyber security

www. Right to Privacy on internet on India

❑❑❑

39

Concept of Cyber Security

Dr.Wahida Shaikh
Head, Department of Political Science,
Abeda Inamdar Sr. College of Arts, Science &
Commerce, Pune

****

Abstract:

Cyber security is technique. Generally, it is set forth in published materials. It attempts to safeguard the cyber environment of a user or organization. It is used to save the integrity of networks, programs and data from unauthorized access at global level. It refers information technology security, and technologies, processes. The concept of cyber security is of growing importance due to increasing reliance on computer and network systems, including television smart and android phones, and the various tiny devices that is connected with the Internet.

Keywords: IT security, Internet of things (IOT), Terms—Computer hacking, Computer security, Reverse engineering, Software protection

Research Methods:

A qualitative and library-based research method used to analyze the background of the Cyber Security and how the Cyber security threats to the common citizen, society, and Government.

Data Collection-

The following sources of data used in writing this research paper.

1) Primary Sources:

The report on Cyber Security.

2) Secondary Sources:

Relevant reference books and research articles.

Note on Reference:

The researcher has used the 'in-text'

method for citation, mentioning the surname of the author, year of publication and page number at the end of the sentence. At the end of the research paper, full bibliographical reference was given in the following manner: Author, Year of publication, Title of the work in (Italicized), Place of publication, and Publisher.

Introduction:

The internet network has made the world smaller in many ways in contemporary world. But it has also opened us information at global level. It influences all aspects of life that have never before been so varied and so challenging. As fast as internet network, and security grew, the hacking system world grew faster. There may be two ways of looking at the issue of cyber security. One is that the companies that provide cloud computing do. Only these companies will be extremely well secured with the latest in cutting edge encryption technology.

Concept of Cyber Security:

Cyber security is being protected by internet-connected systems. It includes hardware, software and data. It protects from cyber attacks. In a computing context, and security comprises cyber, and physical security both are used by enterprises to safe data against unauthorized access. It is also protected data centre and other computerized systems. The security, which is designed to maintain the integrity, availability and confidentiality of data. It is a subset matter of cyber security.

Definition of Cyber Security:

Cyber security is a complex subject. It has a number of definitions.

The National Initiative for Cyber Security Careers and Studies (NICCS) defines:

'The activity, ability, capability, and state whereby information and communications network. The information contained therein are protected from defended against damage, unauthorized use or modification, and exploitation (https://niccs.us-cert.gov/glossary)'.

According to report on Cyber security of University of Maryland, on Cyber security referrers to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction (https://merrill.umd.edu).

According to Oxford Dictionary, the state is being protected against the criminal and unauthorized use of electronic data.

According to kaspersky, Cyber security is the practice of defending mobiles devices and computers, servers, electronic systems, data and networks from malicious attacks. It is also known as IT security and electronic information security. The term applies in many contexts, from mobile computing to business. It can be divided into a few common categories (https://www.kaspersky.co.in).

According to digital guardian, Cyber security refers to the set of technologies, practices, and processes. It is designed to protect networks, data and devices, programs, from damage, attack, and unauthorized access. It may also be referred to as information technology network and security (https://digitalguardian.com/).

Source: www.google.com, last accessed on 03/06/2021.

It is the collection of policies, tools, security concepts, guidelines, security safeguards, actions, risk management approaches, training, assurance and best practices that can be used to protect the cyber environment. Organization assets include connected computing and mobile devices, personnel, applications, services, and telecommunications systems. It is totally transmitted and stored information in the cyber environment.

Need of Cyber Security:

The cyber security protects information and systems from major cyber threats at global level. These threats take in many forms. As a result, cyber security strategy and operations can be a challenge in government and enterprise networks because where most innovative form, cyber threats often takes place. It aims at secret information about financial and military installment.

There are some of the common threats as follow.

· **Cyber terrorism:** Terrorist organization needs secret information of state actors. These types of information used by terrorist groups to further their political, financial and religious agenda. Terrorist used this types of information to attack on Indian Parliament and United State of America. Cyber terrorism took the form of attacks on networks, computer systems and telecommunication infrastructures.

· **Cyber warfare:** It involves nation-states. It uses information technology to go through something another nation's networks to cause damage. In the United State, cyber warfare has been acknowledged as the fifth domain of warfare. Cyber warfare attacks are primarily executed by hackers. Hackers who are well-trained in getting information from computer networks. They work, and operate under the support of nation-states. A cyber-warfare attack may force to get compromise valuable data, and degrade communications. It includes infrastructural services as transportation, commerce and medical services.

· **Cyber spionage:** It is a bad practice of getting information technology to obtain secret information without permission from its owners. It is the most often used to gain military strategy, and economic advantage. It is conducted using cracking techniques and malware.

Cyber Criminals: It involves all such fraud activities as credit card fraud, child printed sexual organs, cyber stalking, gaining unauthorized access to computer systems, defaming another online, ignoring copyright trademark safe to protect, software licensing, software piracy and stealing another's identity to perform criminal acts and overriding encryption to make illegal copies.

Cybercriminals are those who conduct all such above mentioned activities. They can be categorized into three groups according to their motivation.

Cybercriminals – hungry for recognition: This is first type. They are as follow:

· IT professionals (social engineering is one of the biggest threat)

· Hobby hackers

· Terrorist organizations.

· Politically motivated hackers.

Cybercriminals – not interested in recognition: This is second type. They are as follow:

· Psychological prevents.

· State – sponsored hacking (national espionage, sabotage).

· Financially motivated hackers (corporate espionage).

· Organized criminals.

Cybercriminals – the insiders: This is third type. They are as follow:

· former employees seeking revenge.

· Competing companies using employees to gain economic advantage through damage and/or theft.

Reasons of Cyber Crimes:

There are many reasons which perform as a medium in the growth of cyber crime in contemporary world. Some of the prominent reasons are:

· **Money:** People are interested and motivated towards committing cyber crime at any risk is to make quick and easy money.

· **Revenge:** Some people try to take revenge with other person or organization or society or caste or religion by defaming its reputation. It brings economical or physical loss. This comes under the category of cyber terrorism.

· **Fun:** The professional do cyber crime for fun. They just want to test the latest tool they have encountered.

· **Recognition:** It is considered to be pride or honor if someone hack the highly secured information or networks like military sites.

· **Anonymity:** Many times the secrecy provide motivates the person to commit cyber crime. Because, it is too much easy to commit a cyber crime at Global level. It is too much easier to get away with criminal activity in a contemporary cyber world.

· **Cyber Espionage**: Many times the government itself is involved in cyber trespassing to keep eye on other country. The reason could be militarily economically, socially and politically motivated.

Features of Cyber Security: There are main three features of cyber security.

Confidentiality: It is roughly equivalent to privacy. Measures should be undertaken to ensure confidentiality. It is designed to prevent sensitive and important information from reaching the wrong and dangerous people. It should be assured that the information is shared only with authorized persons or organizations.

Integrity: It is assured that the information is complete and authentic. In cyber security, data integrity and security means maintaining the accuracy data over its entire life-cycle.

Availability: It should be assured that the system is responsible for storing, delivering, and processing information. It should be accessible when information is needed. Availability of information refers to ensuring that authorized parties are able to access the information when needed.

Maintain Effective Cyber Security:

Organizations and governments have to take a reactive to combating cyber threats. They have to produce security technologies. Steps have to take to safe networks and the valuable data within time. It is not expensive and complex. In fact, top of the priority has been given to cyber security. Instead, organizations can consider a natively integrated and automated Next-Generation Security Platform. It is designed to provide consistent and prevention-based protection. By focusing on prevention, organizations and government can prevent cyber threats from impacting the network in the first place.

Conclusion:

The international harmonization of cyber security has not yet been achieved. But the literature on cyber security shows a degree of coherence for high-level concepts. It displays evidence of commonality in principles, and concepts. It attributes describing various aspects of policy, and technology space. This commonality provides a tank of fundamental concepts and principles. It can help government, industry and academia.

Modern industry has developed a set of best practices in cyber security. It includes best practices for privacy and data protection, technology and governance standards, and secure technology development. It is based on high-level principles developed by the global community.

Reference:

1) https://digitalguardian.com.

2) https://merrill.umd.edu.

3) https://www.kaspersky.co.in.

4) https://www.kaspersky.co.in/resource-center/definitions/what-is-cyber-security

5) NICCS, 'Explore Terms: A Glossary of Common Cybersecurity Terminology,' https://niccs.us-cert.gov/glossary.

6) www.google.com.

❑❑❑

40

A Challenges of Cyber Security and New Technologies

Prof.Pund Vandas Pandurang
Assistant Professor in Economics,
Dada Patil College Karjat, Tal-Karjat,
Dist.A.Nagar

****

Abstract

Cyber Security plays an important role in the field of information technology .Securing the information have become one of the biggest challenges in the present day. Whenever we think about the cyber security the first thing that comes to our mind is 'cyber crimes' which are increasing immensely day by day. Various Governments and companies are taking many measures in order to prevent these cybercrimes. Besides various measures cyber security is still a very big concern to many.

This paper mainly focuses on challenges faced by cyber security on the latest technologies .It also focuses on latest about the cyber security techniques, ethics and the trends changing the face of cyber security. Keywords: cyber security, cybercrime, cyber ethics, social media, cloud computing, android apps.

1. Introduction

Today man is able to send and receive any form of data may be an e-mail or an audio or video just by the click of a button but did he ever think how securely his data id being transmitted or sent to the other person safely without any leakage of information?? The answer lies in cyber security. Today Internet is the fastest growing infrastructure in everyday life. In today's technical environment many latest technologies are changing the face of the mankind. But due to these emerging technologies we are unable to safeguard our private information in a very effective way and hence these days cybercrimes are increasing day by day. Today more than 60 percent of total commercial transactions are done online, so this field required a high quality of security for transparent and best transactions. Hence cyber security has become a latest issue. The scope of cyber security is not just limited to securing the information in IT industry but also to various other fields like cyber space etc. Even the latest technologies like cloud computing, mobile computing, E-commerce, net banking etc also needs high level of security. Since these technologies hold some important information regarding a person their security has become a must thing. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic wellbeing. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as governmental policy. The fight againstcyber-crime needs a comprehensive and a safer approach. Given that technical measures alone cannot prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cybercrime effectively. Today many nations and governments are imposing strict laws on cyber securities in order to prevent the loss of some important information. Every individual must also be trained on this cyber security and save themselves from these increasing cyber crimes

2. What is Cyber Crime

Cybercrime is a term for any illegal activity that uses a computer as its primary means of commission and theft. The U.S. Department of Justice expands the definition of cybercrime to include any illegal activity that uses a computer for the storage of evidence. The growing list of cybercrimes includes crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying and terrorism which have become as major problem to people and nations. Usually in common man's language cybercrime may be defined as crime committed using a computer and the internet to steel a person's identity or sell contraband or stalk victims or disrupt operations with malevolent programs. As day by day technology is playing in major role in a person's life the cybercrimes also will increase along with the technological advances.

3. Cyber Security

Privacy and security of the data will always be top security measures that any organization takes care. We are presently living in a world where all the information is maintained in a digital or a cyber-form. Social networking sites provide a space where users feel safe as they interact with friends and family. In the case of home users, cyber-criminals would continue to target social media sites to steal personal data. Not only social networking but also during bank transactions a person must take all the required security measures.

As crime is increasing even the security measures are also increasing. According to the survey of U.S. technology and healthcare executives nationwide, Silicon Valley Bank found that companies believe cyber-attacks are a serious threat to both their data and their business continuity.

1. 98% of companies are maintaining or increasing their cyber security resources and of those, half are increasing resources devoted to online attacks this year

2.The majority of companies are preparing for when, not if, cyber-attacks occur

3. Only one-third are completely confident in the security of their information and even less confident about the security measures of their business partners.

There will be new attacks on Android operating system based devices, but it will not be on massive scale. The fact tablets share the same operating system as smart phones means they will be soon targeted by the same malware as those platforms. The number of malware specimens for Macs would continue to grow, though much less than in the case of PCs. Windows 8 will allow users to develop applications for virtually any device (PCs, tablets and smart phones) running Windows 8, so it will be possible to develop malicious applications like those for Android, hence these are some of the predicted trends in cyber security.

4. Trends Changing CyberSecurity

4.1 Web servers:

The threat of attacks on web applications to extract data or to distribute malicious code persists. Cyber criminals distribute their malicious code via legitimate web servers they've compromised. But data-stealing attacks, many of which get the attention of media, are also a big threat. Now, we need a greater emphasis on protecting web servers and web applications. Web servers are especially the best platform for these cyber criminals to steal the data. Hence one must always use a safer browser especially during important transactions in order not to fall as a prey for these crimes.

4.2 Cloud computing and its services

These days all small, medium and large companies are slowly adopting cloud services. In other words the world is slowly moving towards the clouds. This latest trend presents a big challenge for cyber security, as traffic can go around traditional points of inspection. Additionally, as the number of applications available in the cloud grows, policy controls for web applications and cloud services will also need to evolve in order to prevent the loss of valuable information. Though cloud services are developing their own models still a lot of issues are being brought up about their security. Cloud may provide immense opportunities but it should always be noted that as the cloud evolves so as its security concerns increase.

4.3 APT's and targeted attacks APT (Advanced Persistent Threat)

This is a whole new level of cybercrime ware. For years network security capabilities such as web filtering or IPS have played a key part in identifying such targeted attacks (mostly after the initial compromise). As attackers grow bolder and employ more vague techniques, network security must integrate with other security services in order to detect attacks. Hence one must improve our security techniques in order to prevent more threats coming in the future.

4.4 Mobile Networks

Today we are able to connect to anyone in any part of the world. But for these mobile networks security is a very big concern. These days firewalls and other security measures are becoming porous as people are using devices such as tablets, phones, PC's etc all of which again require extra securities apart from those present in the applications used. We must always think about the security issues of these mobile networks. Further mobile networks are highly prone to these cybercrimes a lot of care must be taken in case of their security issues.

4.5 IPv6: New internet protocol

IPv6 is the new Internet protocol which is replacing IPv4 (the older version), which has been a backbone of our networks in general and the Internet at large. Protecting IPv6 is not just a question of porting IPv4 capabilities. While IPv6 is a wholesale replacement in making more IP addresses available, there are some very fundamental changes to the protocol which need to be considered in security policy. Hence it is always better to switch to IPv6 as soon as possible in order to reduce the risks regarding cybercrime.

4.6 Encryption of the code

Encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it.. In an encryption scheme, the message or information is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Encryption at a very beginning level protects data privacy and its integrity. But more use of encryption brings more challenges in cyber security. Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet, e-commerce), mobile telephones, wireless microphones, wireless intercoms etc. Hence by encrypting the code one can know if there is any leakage of information. Hence the above are some of the trends changing the face of cyber security in the world.

5.Role of Social Media in Cyber Security

As we become more social in an increasingly connected world, companies must find new ways to protect personal information. Social media plays a huge role in cyber security and will contribute a lot to personal cyber threats. Social media adoption among personnel is skyrocketing and so is the threat of attack. Since social media or social networking sites are almost used by most of them every day it has become a huge platform for the cyber criminals for hacking private information and stealing valuable data. In a world where we're quick to give up our personal information, companies have to ensure they're just as quick in identifying threats, responding in real time, and avoiding a breach of any kind. Since people are easily attracted by these social media the hackers use them as a bait to get the information and the data they require. Hence people must take appropriate measures especially in dealing with social media in order to prevent the loss of their information. The ability of individuals to share information with an audience of millions is at the heart of the particular challenge that social media presents to businesses. In addition to giving anyone the power to disseminate commercially sensitive information, social media also gives the same power to spread false information, which can be just being as damaging. The rapid spread of false information through social media is among the emerging risks identified in Global Risks 2013 report. Though social media can be used for cybercrimes these companies cannot afford to stop using social media as it plays an important role in publicity of a company. Instead, they must have solutions that will notify them of the threat in order to fix it before any real damage is done. However companies should understand this and recognise the importance of analysing the information especially in social conversations and provide appropriate security solutions in order to stay away from risks. One must handle social media by using certain policies and right technologies.

6. Cyber Security Techniques

6.1 Access control and password security

The concept of user name and password has been fundamental way of protecting our information. This may be one of the first measures regarding cyber security.

6.2 Authentication of data

The documents that we receive must always be authenticated be before downloading that is it should be checked if it has originated from a trusted and a reliable source and that they are not altered. Authenticating of these documents is usually done by the antivirus software present in the devices. Thus a goodanti-virus software is also essential to protect the devices from viruses.

6.3 Malware scanners

This is software that usually scans all the files and documents present in the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware.

6.4 Firewalls

A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. All messages entering or leaving the internet pass through the firewall present, which examines each message and blocks those that do not meet the specified security criteria. Hence firewalls play an important role in detecting the malware.

6.5 Anti-virus software

Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered. An anti virus software is a must and basic necessity for every system.

7.Cyber Ethics

Cyber ethics are nothing but the code of the internet. When we practice these cyber ethics there are good chances of us using the internet in a proper and safer way. The below are a few of them:

1.DO use the Internet to communicate and interact with other people. Email and instant messaging make it easy to stay in touch with friends and family members, communicate with work colleagues, and share ideas and information with people across town or halfway around the world

2. Don't be a bully on the Internet. Do not call people names, lie about them, send embarrassing pictures of them, or do anything else to try to hurt them.

3. Internet is considered as world's larg-

est library with information on any topic in any subject area, so using this information in a correct and legal way is always essential. ? Do not operate others accounts using their passwords.

4. Never try to send any kind of malware to other's systems and make them corrupt. ? Never share your personal information to anyone as there is a good chance of others misusing it and finally you would end up in a trouble.

5. When you're online never pretend to the other person, and never try to create fake accounts on someone else as it would land you as well as the other person into trouble.

5.Always adhere to copyrighted information and download games or videos only if they are permissible. The above are a few cyber ethics one must follow while using the internet. We are always thought proper rules from out very early stages the same here we apply in cyber space.

8. Conclusion

Computer security is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. Cybercrime continues to diverge down different paths with each New Year that passes and so does the security of the information. The latest and disruptive technologies, along with the new cyber tools and threats that come to light each day, are challenging organizations with not only how they secure their infrastructure, but how they require new platforms and intelligence to do so. There is no perfect solution for cybercrimes but we should try our level best to minimize them in order to have a safe and secure future in cyber space.

References

1. A Sophos Article 04.12v1.dNA, eight trends changing network security by James Lyne.

2. Cyber Security: Understanding Cyber Crimes- SunitBelapure Nina Godbole

3. Computer Security Practices in Non Profit Organizations – A NetAction Report by Audrie Krause.

4. A Look back on Cyber Security 2012 by Luis corrons – Panda Labs.

5. International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 Page nos.68 – 71 ISSN 2229-5518, "Study of Cloud Computing in HealthCare Industry " by G.Nikhita Reddy, G.J.Ugander Reddy

6. IEEE Securityand Privacy Magazine – IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2013.

7. CIO Asia, September 3rd, H1 2013: Cyber security in malasia by AvanthiKuma

❑❑❑

41

E-COMMERCE AND CYBER SECURITY

Prof. Vetal Mohan Sukhadeo
Associate Professor,
New Arts Commerce And Science College,
Shevgaon, Dist.Ahmednagar

****

Abstract :

The term e-commerce refers to the exchange of goods and services by online. E-commerce is the latest revolution changing the traditional way of business. The use of internet as way to build electronic commerce the process of e-commerce system network while computer network.

Basically equal my security is helpful of industry it helps to industry for cyber criminal which affect on business transaction in way of red and business practices. In the year 2020 approximately 30th percent business related issues attack on online transactions. Through the process of effective e-commerce security the security related that cars may be safe as possible to customer interest.

Keywords: E-commerce .e-commerce security. security issues in e-commerce. e-commerce website. securities, viruses

Objectives of study:

1) Understand the scope of e-commerce security problems.

2) Understand the space between security and values towards online transactions

3) Identify the key security treats

4) To identify tools used to establish secure internet communication channels.

Introduction:

The cyber crime is trying to break the protocols and reputations of business. e-commerce security is ensure the safety transactions with internet with consists to maintain the protocol in online transactions through the e-commerce security. it will possible to control the faith of customers and success of business.

Contents of e-commerce security-

1) Transaction privacy

It includes the protection of consumers data from the authorized parties. Apart from the online distributors that customer has to select the access for their personal accounts. online business must keep secure the customers that are antivirus protections it is help to control one customer's credit card and bank related information.

2) Integrity in online security

E commerce security is always affected by crucial term of integrity. And she was the doctor of customer has share online. The main object of integrity is to utilize the customers information without the corrections to make any certain changes in customers data probably lost the confidence of integrity on online transactions.

3) Legal authentication

The e-commerce security always focus on legal authentication between the seller and buyer of the real level of business principles and ethics. The sale always protect the interest of customers deal and requirements as per promise.

The customer also closed with the transaction according to faith of online transactions. Disney to be based on authentication and identification. The appropriate method translation is based on client's login data and private identification number.

4) Non reputation

Protect the denial of order of payment center always keep the privacy of message it will not be denied as well as the recipient of message accept the message of sender and follow the appropriate response in the regards of business transaction implementation

5) Auditability of recognization

The rectification of transaction is fine importance in online transactions. The conversation related business transactions should be recorded and verified for the future purpose.

6) Encryption

The encryption is the process of converting information of data into code especially to prevent unauthorized access. The online business related authority should encrypt the data by ways secret code and security code for the future transactions as well as it is using to the same a different security code for protection of business interest.

7) Digital signature

Those variability of the online transactions depends upon authentication by the competent authority. Digital signature is a process that generates the content of message how not to be altered in transist. The user will be generate online signature and alter is verified the signature and signature will be use specific password.

8) Security certificate

Cybersecurity certificate issued for one year. It is focused on principle cyber security skills and unpack knowledge.

The following are the major security certificates

1. Certified ethical hacker (CEH)
2. Comp TIA security
3. Certified information system
4. Certified cloud security professionals

This security certificates helps to protect the effects of business and its protocol.

E-commerce related issues:

1) The Cyber security create different issues regarding intellectual property right. And this will possibly to break the protocols of business privacy.

2) The online floors maybe cost you to the financial fraud celebration markets etc from where this is perfect on security matters and spread of data. You think affected on love data process it is data or corrupt data.

3) Though I could stream the fake version of websites and damage the reputation of company. Therefore it is need to take special prevention against the hikers to control the business deleted properties.

4) It is possible to change the website but online fraud

5) There are maximum possibility to theft of customers and use it for different and unethical business transactions like financial frauds or loss of integrity.

24/7 e-commerce website security:

1) Use multi-users security

The multi uses security control different authentication when the user login the information the instant SMS or mail receive for transaction update and further implementation. The hackers are not allowed to operate multi-uses and passwords to access the account

2) Security security level certificate

The security level certificate allows multiple domain to the secure with SSL certificate the protocol for web browsers and service are allowed for authentication. This certificate control the security of data. The highest take wrong benefits of passwords usernames and create cards if you secure the server on protection code it is possible to control it.

3) Use ultimate firewalls

You can also stop spam which affect on website. It helps to e-commerce to stop consists to real users.

4) Anti malware software

The electronic devices or computers is needed to use proper web system or software for detect and block the software. Then protecting software is called anti Malware software. It's scanned with system forward Malician software.

Conclusion:

Every business should be adopted different e-commerce security procedure and software to keep security treats. As well as it is need to be focused on usernames password multi-factor authentification. It is important that regularly access mail downloading attachments protect therapy passwords and regularly reviewing 3rd party transaction.

References-

1) Information security and cyber laws published by Agarwal Sharma

2) Cyber security Publishers John Wilay, Nemalodbale, Sunit Belapure

3) Information technology law of protection

4) Cyber security in Corvette 19 how to set up cyber secure home office.

42

Security Threats In E-commerce

Dr.Archana Anil Vikhe
Vice-principal,
A.C.S.College, Kolhar, Ta.-Rahata,
Dist.- Ahmednagar

Asst.Prof.Amol Yamaji Jadhav
Department Of Commerce,
Mula Education Society's Shri Dnyaneshwar
Mahavidyalaya Newasa, Ta.- Newasa,
Dist.-Ahmednagar

****

Abstract:

Ecommerce also known as electronic commerce or internet commerce, refers to the buying and selling of goods or services using the internet.in short e-commerce means doing business through the internet. or the transmitting of funds and data, over the Internet. This type of transactions happens either as B to B (Business to Business), B to C (Business to Customer) and C to C (Customer to Customer). With the help of various recent advanced technology tools are, Laptops, Computers, Mobiles, Telephones, Barcode readers, , ATM cards, Credit Cards and other various electronic appliances without the exchange of paper based documents or physically moving to a shopping Centre.

Now days the field of e-commerce has been covered all type of goods and services from various home groceries to large electronic goods even vehicle. Rapid development of mobile, internet and Computer technology is making to E- commerce as more popular and wider reachable.but this growing popularity of e-commerce and its ability to reach far and wide has given birth to a new field of crime called cybercrime.There are many types of cybercrime such as cyber fraud & identity theft,Phishing and other much more threats. now days these all creates many complicated issues of security infront of government , society & E-commerce users. Even then, with the help of the proper knowledge about the handling of E-commerce technology, various security measures and precautions to handle ecommerce technology, we can protect ourselves from cyber threats. This research paper is about these all things.

Keywords: E-Commerce, Security, Threats, Viruses.,Security, Cyber crime, Technology, Rapid.

Introduction:

For the last five to seven years, the concept of e-commerce has been widely used for buying & selling of various types of goods and services as well as for various types of financial transactions.now days it became very populer among young generation .E-commerce has not any time limit and geographycal boundaries limit. it works across the world 24×7 hours of the day and 365 days of the year.it provides global market platform alongwith very fast services to users .it provides many different options of choice of goods to customers as well as saves purchasing time thatswhy many people use the way of online shopping and online banking.Any kind of items or goods can be buy through virtual shopping stores. There are many various ecommecre sites ,some popular of them are Amazon, Flipkart, Myantra, eBay, Aliexpress ,snapdeal etc. are focusing on high availability of quality goodes and services & its fast delivery to ensuring the customers trust. Thus even though e-commerce technology may seem advantageous,but there are many different types of threats involved in its use. Out of which some E-commerce threat are purposeful, some are accidental, some of them are due to human error. The most of common threats are phishing attacks money threats, hacking, data misuse, Credit card frauds or unprotected service.this research work has been focused on some major e-commerce threats & its solutions.

Objective of the study:

- To know the concept of cyber security and the concept of Cyber threats.
- To study the cyber security in E-commerce.
- To study the various cyber threat in E-commerce .
- To know how to protect from various cyber attacks.
- to know how to overcome To various cyber threats.

Methodology:-

For this research, Various secondary data have been collected from various articles, magazins, news papers, websites, TV channels, Internet, Reference books, as well as taken consultancy of some research expert regarding this particular field.

Cyber Security In E-Commerce:

Cyber security means providing an protected environment over the internet for E-commerce. Cyber securities are responsible for defending against the cyber threats. The main motivator of cyber threats is money. The attacker may take the business offline and demand for money in return. The personal information on mobile phones can be hacked for the cyber-attacks.

What Is a Cyber Security Threat..?

"Threats are acts of intentionally harassing, harming or injuring someone". It may be created by person or other entity.The cyber security threat refers to unothentic or unlawfully access of personal information available on internet .cyber threats include stealing, manipulating, altering or misusing information on the Internet.The cyber threats can originate from various sources like terrorist groups, criminal organization, lone hacker etc.

In the last few years, many companies have exposed cyber threats ,for example-

1) in 2017 Equifax breach compromised the personal data of roughly 143 million consumers, including birth dates, addresses and Social Security numbers.

2) In 2018, Marriott International disclosed that hackers accessed its servers and stole the data of roughly 500 million customers.

3) one of the biggest cyber attacks happened on 11th August 2018 in Indian Bank. within 7 hours several cloned debit card of Cosmos Bank were used for thousands ATM transaction from India and 28 other country and stolen about 94 crores These examples shows that,how cyber threats are dangerous & harmful.

Types of Cyber Security Threats :

Technology is a very dynamic concept. With the development of technology, the threats in it are also changing.Now days there are many types of cyber security threats. some major of them are as under.

1) Financial frauds -

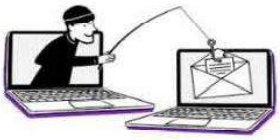
Cybercriminals have got really creative; they use credit card data to purchase goods and services on e-commerce stores.

Besides stealing bank cards and account details, cybercriminals have got really creative. Ever since the first online businesses entered the world, villains now target apps and websites. The fraudsters also file complains for fake return policies.

Financial fraud (image source -google.com)

2) Phishing -

Phishing is cyber-crime where the aim to steal personal information such as login ID and password. This can be done by personal messages or by e-mail marketing process. A fake website is created by the criminals which looks exactly like real one and it makes sure that customer enters ID and password and the bank accounts could be hacked.



Phishing

(Image source- google.com)

3)Spam -

The comments left on the blog which is infected links are the ways to harm you. This links are send via mail or messages, they wait for you to click link so they can hack your information. This can damages your blog speed.

Spam(Image source google.com)

4) Bots

Bots are automated software application programmed to perform specific task. They are responsible for ranking the websites. Yet the criminals use this technique to manipulate the pricing of your product which results in decline of sales and revenue.

5)DDoS Attacks -

Distributed Denial of Service (DDoS) and DOS (Denial of Service) attacks can harm your website or app by generating a large number of requests which eventually can crash the whole system and make it unavailable for the end-user. This eventually disrupts your site and affects sales.

6) Trojan horses –

Trojan horse is a programming code which can perform destructive functions. They normally attacks your computer when you downloading something. Malware, a program usually downloaded by customers as legitimate software, is called a Trojan horse. To this category belong programs that can gather data about credit or debit cards, transfer this information to the hacker, as well as crash users' computers or use PC resources for hacker's goals without permission of the user. These programs get any sensitive data with ease and may also infect your website.

Trojan horrse virus icon

(Image source google.com)

7) In accurate management

The main reason of e-commerce threat is poor management. Securities threats are occur when there are no proper budget are allocated for purchase of anti-virus software licenses.

E-commerce security solutions

Experts have found some solutions to prevent various threats/risks in e-commerce usage as well as suggested some precautionary measures.are as under:,

A) HTTPS security

The HTTP protocol makes vulnerable attacks. Every security advices to use HTTPS which displays the trustee green lock. The "S" stands for secure URL bar.HTTPS protects the information of customer and the websites itself. The main factor of HTTPS is that it makes higher ranking on Google's search page, as Google support the secure websites. HTTPS is a safer version of HTTP. The SSL protocol activates after SSL certificate is set and encrypts personal data before submission of information transfers to e-commerce website. The protection is necessary because when customer does online transaction the information of credit card is stolen by hacker and can be used later on.

B) Anti-malware -

Anti-malware is software that detects and deletes computer viruses, as well as other undesirable or harmful programs. Anti-malware also reestablishes files that have already been harmed by viruses and prevent further file or software modification that can be done by malicious code. Anti-malware is used against worms, viruses, and Trojan horses.

C) Secure server and the admin panel -

Another good practice is restricting user access and defining user roles. Using passwords that contain different characters and are hard to guess is a key. Making the panel notify you if a foreign IP tries to access it is an extra step for your security. You should also change them frequently. Let everyone perform only what they have to on the admin panel. 4. Secure payment gateway.

D) Additional e-commerce security measures-

The resource which are familiar please use them. Use the official bank websites and check the messages path. Make scanning your website from malware your constant routine. Use security for websites. Back up your data every day. Use security plug-ins.

E) Payment gateway security

The storage of credit or debit card information on online sites is an open invitation for hacker to disclose your personal information. If you fall victim to the security breach the hacker get their hands on the card and your business is on the edge. This might force you into bankruptcy.If you want to have a safe transaction then be cautious about the payment gateway security is not at risk. You can carry out the process off site by taking help of third party. The popular option is PayPal.

Conclusion

E-commerce is a magic wand in the hands of today's people but it should be used very carefully.because With the rapid development and growing popularity of e-commerce technology, the cyber threats associated with it are becoming a serious problem for its users.Many times these threats are deliberately created by the hackers and Sometimes such threats are occurred due to inadequate knowledge of about the e-commerce technology , negligence in use or inadequate or weak security system in the e-commerce tools. Criminals in this area who are called cyber criminals can be from anywhere in the country or anywhere in the world.Therefore, detection of such crimes and criminals is becoming a global problem and challenge. Nevertheless, with a thorough proper knowledge of the use of e-commerce tools, careful use of these tools, use of modern security mechanisms in the e-commerce system and awareness about it, We can prevent threats and cybercrime in e-commerce, and stay safe from it.

References:

https://www.the-future-of-commerce.com

https://cybersecurity.att.com

https://www.itgovernance.co.

https://www.google.com

https://www.timesofindia.com

https://www.webroot.com

https://www.itg.ias.edu

https://www.centralbank.net

https://www.indiatoday.in

https://www.getastra.com

https://www.cloudways.com

i)Whiteley.(2017).E-Commerce strategy, Technologies and applications.India: Mc graw Hill education.

ii) V.Rajaraman.(2018) Introduction to information technology. Delhi, India : PHI Publications.

iii) Daily Times of India Newspaper 11th August 2018

iv) Magazine- Digital commerce 360

v) Magazine- Practical eCommerce

vi) Magazine-eMarketer

vii) Magazine- Business India

43

Study of Cyber Security infrastructure in India

Dr. Mangesh Bhople
Asst. Professor, Dept. of BBA & BBA IB,
MIT ACS College, Alandi, Pune, Maharashtra

****

Abstract:

The Cyber Attacks has become usual nowadays. According to, Indian Computer Emergency Response Team (CERT-In), Nearly 1.16 million cases of cyberattacks were reported in 2020, up nearly three times from 2019 and more than 20 times compared to 2016, according to government data presented in the Parliament on Tuesday. On an average, 3,137 cyber security-related issues were reported every day during the year.

The increased usage of internet and mobile handsets has been increasing from ordering online food to the online banking transactions. It has increased the chances of more cyber-attacks by different hackers and drudgers. Government of India has taken initiatives to establish the required infrastructure to minimize the online vulnerability.

Formation of a trustworthy cyber security infrastructure is a need of the day. This infrastructure will enable all the users for doing safe transactions without falling victims to such cyber-attacks.In this paper, the attempt is made to study the available legal and physical infrastructure. The government has also taken some initiatives for E-governance and E- commerce activities such as IT Act 2000.

Attempt is being made in this paper to present a current scenario of this infrastructure, likely trends and imperatives that emerge from this study in Indian Commerce and Management.

Key Words: Cyber Attacks, CERT-In, E-Governance, E- Commerce, IoT.

Introduction:

The concept of cyber security is getting very much importance in the field of commerce and management today because of the present situation and the changing form of businesses from traditional to IoT based. The commerce is a vast concept which covers all the commercial activities in all the industries from agriculture to travel and tourism sectors. The concept of cyber security has more highlighted in this Covid 19 pandemic. All the monetary and non-monetary transactions have shifted from physical to virtual mode in businesses and individual areas. The information technology (IT) industry has progressed greatly over the last half century. This growth has made processes powerful, transparent, fast, cheaper and convenient. IT industry enabled many sub services and combined with other industries such fintech, communication technology etc. The IT has integrated with many other sectors and has also changed the societal norms. The act of protecting this ICT systems and their componentsare known as cybersecurity altogether. This cybersecurity can be an important tool in protecting privacy, information and preventing unauthorized surveillance and information sharing and intelligence gathering in all the terms of businesses. The management of this risks to information systems is considered fundamental prerequisite for effective cybersecurity infrastructure. The risks associated with any attack depend on three factors:

1. Threats i.ewho is attacking,
2. Vulnerabilitiesie. the weaknesses of system they are attacking,
3. Impacts ie. what the attack doesaffect on system and entire economy?

Most cyberattacks have limited impacts but a successful and large attacks on some components of critical infrastructure could affect significantly on national security, the economy, the livelihood and safety of individual citizens. Reducing such risks usually involves removing threat sources, addressing vulnerabilities and lessening the overall impacts. The central role in cybersecurity involves both securing central systems and assisting in protecting all other systems. Today organisations have their own budget also for spending on the issues related cybersecurity.

Objectives of the Paper:

1. To study the Cyber Security Infrastructure in India.

2. To study the current scenario and India's future potential.

3. To study the need of Cyber Security Infrastructure development

4. To study the vulnerable sectors in commerce and Management from Cyber Security perspectives

Research Methodology:

It is a qualitative and descriptive research where;the secondary datahas been used. Researcher has referred different reports from government and other agencies and also the research articles of different researchers. Secondary data was collected through newspapers, journals; websites and reports form related national bodies like TRAI, COAI, NASSCOM, Ministry of Information Technology etc.

Cybersecurity infrastructure in India:

Government of India has taken following steps in order to control the Cyber Attacks and make the system stronger:

1. Personnel Policy for Below Group 'A' S&T employees of MeitY and its organizations - 1983

2. National Cyber Security Policy-2013 (NCSP-2013): According to this policy, Cyberspace is vulnerable to a wide variety of incidents, whether intentional or accidental, manmade or natural, and the data exchanged in the cyberspace can be exploited for nefarious purposes by both nation- states and non-state actors. Cyber-attacks that target the infrastructure or underlying economic well-being of a nation state can effectively reduce available state resources and undermine confidence in their supporting structures. A cyber related incident of national significance may take any form; an organized cyber-attack, an uncontrolled exploit such as computer virus or worms or any malicious software code, a national disaster with significant cyber consequences or other related incidents capable of causing extensive damage to the information infrastructure or key assets. Large-scale cyber incidents may overwhelm the government, public and private sector resources and services by disrupting functioning of critical information systems. Complications from disruptions of such a magnitude may threaten lives, economy and national security. Rapid identification, information exchange, investigation and coordinated response and remediation can mitigate the damage caused by malicious cyberspace activity. Some of the examples of cyber threats to individuals, businesses and government are identity theft, phishing, social engineering, hacktivism, cyber terrorism, compound threats targeting mobile devices and smart phone, compromised digital certificates, advanced persistent threats, denial of service, bot nets, supply chain attacks, data leakage, etc. The protection of information infrastructure and preservation of the confidentiality, integrity and availability of information in cyberspace is the essence of a secure cyber space.

3. National Policy on Software Products - 2019 – According to this, The Information Technology and Information Technology Enabled Services (IT-ITES) industry of the country is a critical pillar in India's economic growth. The industry has potential to be a driving force for enabling India to develop capabilities for harnessing new technologies cutting across all the sectors, namely, agriculture, health, education, manufacturing etc, thereby creating significant employment and entrepreneurial opportunities. According to NASSCOM the sector at present is

generating an estimated revenue of around USD 168 billion, including export of USD 126 billion on an annual basis, which is around 8% contribution to India's GDP. The industry is also one of the largest organised sector employers, generating nearly 14 million direct and indirect jobs. It is further estimated that the industry can contribute up to 350 billion USD accounting to 10 percent of India's GDP by 2025.

4. Notification on National Policy on Electronics 2019 (NPE 2019) – According to this policy, Electronics industry is the world's largest and fastest growing industry and is increasingly finding applications in all sectors of the economy. The Government attaches high priority to electronics hardware manufacturing and it is one of the important pillars of both "Make in India" and "Digital India" programmes of Government of India. Besides the economic imperative, focus on electronics hardware manufacturing up to the integrated circuit or chip level is required due to the growing security concerns. The ESDM industry is of strategic importance as well.

5. Personnel Policy for Group "A" S&T Officers of Ministry of Electronics and Information Technology (MeitY) and its organizations-Instructions for Autonomous Bodies

6. Updation and Usage Policy for the SamparkDatabase (IT Platform for Messages)

7. Policy on Adoption of Open-Source Software for Government of India

8. Email Policy 2014 – in this policy government has given some important directions through following sub policies for operating on Cyberspace. These are given below:

a) E-mail Policy of Government of India

b) Guidelines for E-mail Account Management and Effective E-mail Usage

c) Email Services and Usage Policy

d) NIC Policy on format of e-mail Address

e) Password Policy

f) Security Policy for User

g) Service Level Agreement

Government has also formulated some other policies to cover the aspects

9. Policy on Use of IT Resources

10. National Policy on Universal Electronic Accessibility

11. Notification on National Cyber Security Policy-2013

12. Policy for .IN Internet Domain Registration

13..IN Internet Domain Name-Policy Framework and Implementation

Results and discussions:

India encountered almost seven lakh cyber-attacks by August 2020, as per the report by the Ministry of Electronics and Information Technology. Increased malware and ransomware have exhibited a greater threat to the cybersecurity, sovereignty and integrity of the country. A report by Subex indicates a surge of 86% cyberattack cases between April and March 2020. The Internet of Things (IoT) has become the fastest adopted technology in the industry. Internet of Things connects various sources and thus instigates sharing and generating of exponential data. From oil and energy sector to the automotive industry, the Internet of Things is making operations durable and accurate. With its sustainable mechanism, the technology is also fueling the country's ambitious project of integrating the 5G network. Apart from being used as a technology, IoT has also become a commodity. For example, the smart thermostat and the smart cable network, which embellishes smart homes, leverage IoT as a commodity. However, despite all the pros that the technology indicates, connecting different sources without any upgraded security grants easier access to cyber attackers and hackers. The existing COVID-19 outbreak has already exposed the urgency to have an upgraded cybersecurity infrastructure. Since these cyber-attacks are not confined to only healthcare infrastructure but also pervades other industry such as defense, it demands a comprehensive strategy to protect systems while leveraging the existing technology. Unfortunately, the lack of a regulatory framework for any technology becomes a major barrier to thwart cyber-attacks, ransomware and malware. Without any regulation, technologies like artificial intelligence and IoT often become exploitative. Lack of knowledge by the IoT vendors and users also advances the security challenges with IoT. In order to control the cyber-attacks, it becomes imperative to formulate a regulatory framework which monitors the IoT usage and the incidents of cyber-attacks. For this, India can observe the steps taken to maintain IoT standards from its allies. For example, European body ETSI (European Telecommunications Standards Institute) has released certain guidelines for the adoption and utilization of IoT. It's ETSI EN 303 645, a standard for cybersecurity in the Internet of Things, establishes a security baseline for internet-connected consumer products and provides a basis for future IoT certification schemes. The European Cybersecurity body states that the EN is designed to prevent large-scale, prevalent attacks against smart devices that cybersecurity experts see every day. By complying with the standards, EN will restrict the ability of attackers to control devices across the globe known as botnets which launch DDoS attacks, mine cryptocurrency and spy on users in their own homes. By preventing these attacks, the EN represents a huge uplift in baseline security and privacy. A similar regulatory framework can be deployed by the Indian cybersecurity organization so that vendors and consumers comply with the IoT standards. By installing a regulatory body, the discrepancies in the security network can be identified.Another solution to preventcyber-attacks, ransomware and malware, is educating the consumers about upgraded security network and the possible implications of disrupted IoT network. By acquainting the consumers about the basic concept such as having a separate network for IoT devices, having strong and unique passwords of IoT devices and building a firewall will make the consumers more cautious about their IoT devices and the network security, which will in turn aid in mitigating the cyberattacks.

Today, we are using numerous apps for ecommerce transactions. Google Pay, Phone Pay, Airtel Money, BHIM app, SBI Pay and many more. The number of users is increasing day by day and so the use of cyberspace. Along with the finance sector other sectors are also facing the issues of cyber-attacks. Following are some of the sectors to prevent the cyberattacks and provide more cyber security:

1. The Energy and allied Sectors like generation, distribution, billing etc.

2. The Dam related Sectors such as water maintenance and controls, hydroelectric power, city and industrial water supplies, agricultural water systems, silt and surge control, stream route for inland mass transportation, modern waste administration, and recreation services.

3. The Financial Services Sector which includes savings accounts, stock market, insurance, payment gateways and other platforms.

4. The Nuclear Reactors, Materials, and Waste Sector which includes very critical infrastructure from electricity to nuclear power. The control of such critical sectors can be hijacked by hackers and can result in more serious attacks.

5. The Food and Agriculture Sector is also following to implement critical infrastructure in the area of food processing, manufacturing, storage and selling facilities.

5. The Water supply systems to cities and industries is being managed with the help of cyberspace today. Creation of cybersecurity infrastructure in important for controlling of the administration of this essential component to the citizens in country.

6. The Healthcare and Public Health Sector is also very important sector and ensures health and wellbeing for Indians. The Covid 19

pandemic has highlighted the need of sufficient and sophisticated physical and critical infrastructure to ensure uninterrupted health services.

8. The education Sector has witnessed a paradigm shift in India and the winds of online education have already started to flow. The entire pedagogy is supposed to adapt the internet of things from admissions to examinations. Therefore, here also it is important to look after the proper set up of all required infrastructure.

9. The Transportation sector including roads, marine, rail ways and air are being manged through the IT systems today. It is essential to develop a fool proof framework of rules and safety and other infrastructure.

10. The Chemical Sector is also an important sector which is a base for many other sectors ranging from agriculture to defense and health.

11. The Communications sector is the fundamental part of Indian economy. The communication sector provides different services from individuals to governments and therefore the cyber security infrastructure is important in this sector also.

12. The Information Technology Sector has become the key sector in the economic operations of the country. It has covered all the departments and other sectors with its services including education, banking and finance. This sector itself requires such kind of strong infrastructural support and other norms for cyber security.

13. The Critical Manufacturing Sector has gained the momentum in the economic operations today. An immediate cyber-attack can affect any critical manufacturing process and the productive capacities of companies and nation. It includes metals, critical machineries, auto components, electrical appliances etc.

14. The Government schemes today from agriculture to import and exchanges are being implemented through cyber cloud mechanism. Such kind of operations are highlighting the strong supporting cyber security infrastructure. This sector has also getting affected by such internal and external threats.

Conclusion:

Our country is also following the footprints of the other developed nation to strengthen the cybersecurity infrastructure. The cybersecurity is a critical component from many aspects. These aspects are from formation of ne laws and acts to the cyber literacy amongst its users. The government cannot alone fight against this challenge. Some private sector players can also play an important role in this. Already government has given green signal for privatization of many sectors. It is also the duty of users to be educated and cautious while implementing the e-transactions and using the cyber infrastructure. Today the commerce field and entire sectors are being operated within the available infrastructure and several cases of cyber attacks are coming at front.

There are several security strategies to prevent cyber-attacks for the critical infrastructure sectors discussed above. For strengthening the infrastructure some measures such as proper configuration, patch management, reducing the attack surface areas and vulnerability, whitelisting of software, building a controlled network,authentication management, secure remote access for users, strong monitoring mechanism for attack penetration and response to such attacks.

References:

1. http://money.cnn.com/2017/09/26/technology/india-mobile-congress-market-numbers/index.html. (n.d.). Retrieved 12 09 @ 5.00 pm, 2017, from http://money.cnn.com/2017/09/26/technology/india-mobile-congress-market-numbers/index.html

2. http://www.iamwire.com/2016/11/list-of-mobile-wallets-upi-payment-apps-in-india/145172. (n.d.). Retrieved 11 23@10.00 pm,

2017

3. http://www.mospi.gov.in/147-information-technology-indian-statistical-system. (n.d.). Retrieved 12 5 @ 5.00 pm, 2017

4. http://www.mospi.gov.in/83-strengthening-infrastructure-statistics. (n.d.). Retrieved 12 8 @ 3.30 pm, 2017, from http://www.mospi.gov.in/83-strengthening-infrastructure-statistics

5. http://www.mospi.gov.in/statistical-year-book-india/2015. (n.d.). Retrieved 12 8, 2017

6. https://cipher.com/blog/the-16-sectors-of-critical-infrastructure-cybersecurity/. (n.d.).

7. https://corp.ezetap.com/blogs/ezetap-is-disrupting-the-indian-payment-industry. (n.d.).

8. https://newsroom.mastercard.com/press-releases/citibank-india-and-mastercard-launch-citi-masterpass-the-first-global-wallet-in-india/. (n.d.).

9. https://topandroidtips.com/best-online-payment-apps-india/#1_BHIM_App. (n.d.). Retrieved 11 21@10.00pm, 2017, from https://topandroidtips.com/best-online-payment-apps-india/#1_BHIM_App

10.https://www.analyticsinsight.net/how-the-internet-of-things-security-infrastructure-in-india-can-be-improved/. (n.d.).

11.https://www.etsi.org/newsroom/press-releases/1789-2020-06-etsi-releases-world-leading-consumer-iot-security-standard. (n.d.).

12. https://www.livemint.com/industry/banking/airtel-payments-bank-raises-rs-225-crore-from-parent-11580353566892.html. (2021, May 30).

13. https://www.meity.gov.in/content/policies-0. (2021, 06 04).

14. https://www.sumhr.com/digital-wallets-india-list-online-payment-gateway/. (n.d.). Retrieved 12 08@ 4.26 pm, 2017, from https://www.sumhr.com/digital-wallets-india-list-online-payment-gateway/

15. https://www.teleanalysis.com/analysis/india-87-mn-4g-subscribers-jio-alone-72-mn-25771. (n.d.). Retrieved 12 9@7.00 pm, 2017

16. INDIA, T. R. (7th April, 2017). "Indian Telecom Services Performance Indicator Report" for the Quarter ending December, 2016. New Delhi: TELECOM REGULATORY AUTHORITY OF INDIA .

17. PANNEERSELVAM, M. M. (Vol.2 (7), July (2013)). MOBILE COMMERCE – A MODE OF MODERN BUSINESS . Asia Pacific Journal of Marketing & Management Review, ISSN 2319-2836, 141-149.

18. Singh, R. K. (Vol. 4, Issue 3, March 2016). Mobile Commerce: Indian Perspectives . International Journal of Innovative Research in Computer and Communication Engineering , 4320-4326.

19. http://money.cnn.com/2017/09/26/technology/india-mobile-congress-market-numbers/index.html. (n.d.). Retrieved 12 09 @ 5.00 pm, 2017, from http://money.cnn.com/2017/09/26/technology/india-mobile-congress-market-numbers/index.html

20. http://www.iamwire.com/2016/11/list-of-mobile-wallets-upi-payment-apps-in-india/145172. (n.d.). Retrieved 11 23@10.00 pm, 2017

21. http://www.mospi.gov.in/147-information-technology-indian-statistical-system. (n.d.). Retrieved 12 5 @ 5.00 pm, 2017

22.http://www.mospi.gov.in/83-strengthening-infrastructure-statistics. (n.d.). Retrieved 12 8 @ 3.30 pm, 2017, from http://www.mospi.gov.in/83-strengthening-infrastructure-statistics

23. http://www.mospi.gov.in/statistical-year-book-india/2015. (n.d.). Retrieved 12 8, 2017

24. https://topandroidtips.com/best-online-payment-apps-india/#1_BHIM_App. (n.d.). Retrieved 11 21@10.00pm, 2017, from https://topandroidtips.com/best-online-payment-apps-india/#1_BHIM_App

25. https://www.sumhr.com/digital-wallets-india-list-online-payment-gateway/. (n.d.). Retrieved 12 08@ 4.26 pm, 2017, from https://www.sumhr.com/digital-wallets-india-list-online-payment-gateway/

26. https://www.teleanalysis.com/analysis/india-87-mn-4g-subscribers-jio-alone-72-mn-25771. (n.d.). Retrieved 12 9@7.00 pm, 2017

27. INDIA, T. R. (7th April, 2017). "Indian Telecom Services Performance Indicator Report" for the Quarter ending December, 2016. New Delhi: TELECOM REGULATORY AUTHORITY OF INDIA .

28. PANNEERSELVAM, M. M. (Vol.2 (7), July (2013)). MOBILE COMMERCE – A MODE OF MODERN BUSINESS . Asia Pacific Journal of Marketing & Management Review, ISSN 2319-2836 , 141-149.

29. Singh, R. K. (Vol. 4, Issue 3, March 2016). Mobile Commerce: Indian Perspectives . International Journal of Innovative Research in Computer and Communication Engineering , 4320-4326.

❑❑❑

44

An Effect of Cyber Crime Indian Economy

Prof.Shivannd Bhandare
Assistant Professor in Economics,
Sou.M.R.Jagtap Mahila College Umraj

****

Abstract:

Governments needs reliable data on crime in order to both devise adequate policies, and allocate the correct revenues so that the measures are cost-effective, i.e., The money spent in prevention, detection, and handling of security incidents is balanced with a decrease in losses from offences. The analysis of the actual scenario of government actions in cyber security shows that the availability of multiple contrasting figures on the impact of cyber-attacks is holding back the adoption of policies for cyber space as their cost-effectiveness cannot be clearly assessed. The most relevant literature on the topic is reviewed to highlight the research gaps and to determine the related future research issues that need addressing to provide a solid ground for future legislative and regulatory actions at national and international levels.

I.Introduction

A crime is an offense that maybe prosecuted by the state and punishable by law. A cyber-crime is a type of crime which uses computers and networks as target or weapon. Today's necessity is to minimize the cyber-crimesoccurring in various parts of the world. Cyber-crimes in India are increasing at an alarming rate. It will be better if the rate of occurrence of cyber-crime patterns is predicted for various parts of the country Cyber-crime began with disgruntled employees causing physical damage to the computers they worked with, with the aim to get back at their superiors. As the ability to have personal computers at home became more accessible and popular, cyber criminals began to focus their efforts on home users[1]. Further research on this reveals that history of cybercrime was further established that the first published report of cybercrime occurred in the 1960s, when computers were large mainframe systems. Since mainframes were not connected with other ones and only few people can access them, the cybercrimes were always "insider" cybercrimes, which means employment, allowed them to access into mainframe computers, and then refers to as computer crime rather than cybercrime. Actually, in the 1960s and 1970s, the cybercrime, which was "computer crime" in fact, was different from the cybercrime we faced with today, because availability of Internet was restricted within some sections (e.g. US military) in that era. In the following decades, the increasing of computer network and personal computers transformed "computer crime" into real cybercrime. In fact, the former descriptions were "computer crime", "computer-related crime" or "crime by computer". With the pervasion of digital technology, some new terms like "high-technology" or "information-age" crime were added to the definition. Since Internet was invented, other new terms, like "cybercrime" and "net" crime became the order of the day as people began to exchange information based on networks of computers, also keep data in computer rather than paper. At the same time, the cybercrime was not only restricted in target cybercrime, but expanded into tool cybercrime and computer incidental. We therefore come to terms with a conclusion on the meaning that cybercrime is an evil having its origin in the growing dependence on computers in modern life. A simple yet sturdy definition of cybercrime would be unlawful acts wherein the computer is either a tool or a target or both. Defining cybercrimes as illegalbehavior directed by means of electronic operations that targets the security of computer systems and the data processed by them. Cybercrime in a broader sense computer-related crime: any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.[5]

2. Objectives

1.The cost of cybercrime will continue to increase as more business functions move online and as more companies and consumers around the world connect to the Internet.

2. Losses from the theft of intellectual property will also increase as acquiring countries improve their ability to make use of it to manufacture competing goods.

3.Cybercrime is a tax on innovation and slows the pace of global innovation by reducing the rate of return to innovators and investors.

4. Governments need to begin serious, systematic effort to collect and publish data on cybercrime to help countries and companies make better choices about risk and polic

3. Research Methodology

Survey 1 was prepared using specialist online software and designed along the lines of the Delphi method. The questions for this survey were of a generic nature as the intention was for Surveys 2 & 3 to explore resultant themes at a deeper level. To exploit the Cyber ROAD Cybercrime Survey a number of distribution methods were employed by project partners. These included the project website, a dedicated website, announcements via social media, and prompting by email to interested parties. The surveys were split into two versions: one for English speakers worldwide and the other translated into Polish and aimed at Polish users This research is descriptive in nature. The Secondary sources of knowledge are used for this Secondary data has been collected from different published sources like books, , Bulletin, news journals, newspapers and magazines, and internet sites etc

4. Types of Cybercrimes most prevalence in Indian

(1)Assault by Threat – threatening a person with fear for their lives or the lives of their families or persons whose safety they are responsible for (such as employees or communities) through the use of a computer network such as email, videos, or phones.

(2) Child pornography – the use of computer networks to create, distribute, or access materials that sexually exploit underage children.

(3) Cyber laundering – electronic transfer of illegally-obtained monies with the goal of hiding its source and possibly its destination.

(4) Cyber stalking – express or implied physical threats that creates fear through the use of computer technology such as email, phones, text messages, webcams, websites or videos.[3]

(5) Cyber terrorism – premeditated, usually politically-motivated violence committed against civilians through the use of, or with the help of, computer technology. [9]

(6) Cyber theft is using a computer to steal. This includes activities related to: breaking and entering, DNS cache poisoning, embezzlement and unlawful appropriation, espionage, identity theft, fraud, malicious hacking, plagiarism, and piracy. -

Hardware Hijacking - Researchers at Columbia University recently discovered a serious security flaw in certain printers, as well. Many printers automatically update their software when accepting a print job, connecting to the Internet to download the latest print drivers.

-Spam - Unsolicited mass e-mail, known colloquially as ¯spam í⍰d í⬆; is more than annoying: spam messages can be use to trick people into giving up sensitive personal information (known as ¯phishing d or as carriers for computer worms and viruses.[1]

-Script kiddies-A wannabe hacker. Someone who wants to be a hacker (or thinks they are) but lacks any serious technical expertise. They are usually only able to attack very weakly secured systems.

-Insiders- They may only be 20% of the threat, but they produce 80% of the damage. These attackers are considered to be the highest risk. To make matters worse, as the name suggests, they often reside within an organization

(7)Yahoo Attack:- Also called 419 because section 419 of the Indian criminal code has a law against such offenders. It is characterized by using e-mail addresses obtained from the Internet access points using e-mail address harvesting applications(web spiders or e-mail extractor). These tools can automatically retrieve-mail addresses from web pages. Indian fraud letters join the warning of impersonation scam with a variation of an advance fee technique in which an e-mail from Indian offers the recipient the chance to share a percentage of a huge amount of money that the author, a self-proclaimed government official, is trying to siphon out of the country

(8) Salami Attack:-Salami assaults are flamboyant economic scams or exploits against confidentiality by comprehensive data gathering.[9]

5. Conclusion

Reliable data is a fundamental on which revenues and budgets rely from the top at government level down to board level and individual stakeholders. To understand a problem, to know what is and how to tackle it, is a task that presents greater challenges when size and extent of that problem remains very much shrouded in mystery. The CyberROAD project is working towards a roadmap for cybercrime and cyberterrorism to reveal the research gaps that can help policy makers make more informed decision on where money should be directed to return the best possible outcomes.

Cybercrime as a subject of study is still in its infancy and much can be learned from the evolutionary development of other recently established sciences. To begin, a clear taxonomy is an essential element from which a framework for further study can be developed. Our investigation of current and future scenarios via focused surveys and comparison of the cost of cybercrime reports reveals a number of research gaps that require attention if the scenarios outlined are to be achieved by 2020. Fundamental to the issue is the ability to quantify what we have and where we want to go. Currently, there is a mis-match between the experiences of stakeholders and the information to hand which can be improved with quantification of the issues and a reliable model for costing. Central to this information is the issue of trust, as without it there will be no confidence in the way forward with more time and money being wasted. Indeed, it is not an exaggeration to say that without quantification and measurement there will be no solution to the problem of cybercrime by 2020 or beyon Reliable data is a fundamental on which revenues and budgets rely from the top at government level down to board level and individual stakeholders. To understand a problem, to know what is and how to tackle it, is a task that presents greater challenges when size and extent of that problem remains very much shrouded in mystery. The CyberROAD project is working towards a roadmap for cybercrime and cyberterrorism to reveal the research gaps that can help policy makers make more informed decision on where money should be directed to return the best possible outcomes.

Cybercrime as a subject of study is still in its infancy and much can be learned from the evolutionary development of other recently established sciences. To begin, a clear taxonomy is an essential element from which a framework for further study can be developed. Our investigation of current and future scenarios via focused surveys and comparison of the cost of cybercrime reports reveals a number of research gaps that require attention if the scenarios outlined are to be achieved by 2020. Fundamental to the issue is the ability to quantify what we have and where we want to go. Currently, there is a mis-match between the experiences of stakeholders and the information to hand which can be improved with quantification of the issues and a reliable model for costing. Central to this information is the issue of trust, as without it there will be no confidence in the way forward with more time and money being wasted. Indeed, it is not an exaggeration to say that without quantification and measurement there will be no solution to the problem of cybercrime by 2020 or beyon Reliable data is a fundamental on which revenues and budgets rely from the top at government level down to board level and individual stakeholders. To understand a problem, to know what is and how to tackle it, is a task that presents greater challenges when size and extent of that problem remains very much shrouded in mystery. The CyberROAD project is working towards a roadmap for cybercrime and cyberterrorism to reveal the research gaps that can help policy makers make more informed decision on where money should be directed to return the best possible outcomes.

Cybercrime as a subject of study is still in its infancy and much can be learned from the evolutionary development of other recently established sciences. To begin, a clear taxonomy is an essential element from which a framework for further study can be developed. Our investigation of current and future scenarios via focused surveys and comparison of the cost of cybercrime reports reveals a number of research gaps that require attention if the scenarios outlined are to be achieved by 2020. Fundamental to the issue is the ability to quantify what we have and where we want to go. Currently, there is a mis-match between the experiences of stakeholders and the information to hand which can be improved with quantification of the issues and a reliable model for costing. Central to this information is the issue of trust, as without it there will be no confidence in the way forward with more time and money being wasted. Indeed, it is not an exaggeration to say that without quantification and measurement there will be no solution to the problem of cybercrime by 2020 or beyond. In India, there is no doubt that a good number of people have turned the ethical use of information and communication technologies into unethical activities. This problem is not peculiar to India alone, but it is a problem worldwide and that is why it becomes imperative that organizational data /information must be safeguarded especially these days that almost every business is being run on line. our investigation on cybercrimes we observed its threat to the economy of a nation and even peace and security. Therefore there is need for a holistic approach to combat these crimes in all ramifications. Our proposal therefore is the need for cyber police who are to be trained specially to handle cybercrimes in India. In addition, the police should have a Central Computer Crime Response Wing to act as an agency to advise the state and other Investigative agencies to guide and coordinate computer crime investigation. We are also proposing that the country should set up National Computer Crime Resource Centre, a body, which will comprise experts and professionals to establish rules, regulations and standards of authentication of each citizen’s records and the staff of establishments and recognized organization, firms, industries etc.. Above all, comprehensive law to combat computer and cyber related crimes should be promulgated to fight this phenomenon ¯to a halt. Our proposal on the nature of law to combat cybercrime is not included in this paper. We recommend that before anybody enters into any kind of financial deals with anyone through the internet he/she should use any of the search engines to verify the identity of the unknown.

References

[1] Milner, H. V. (1999). The political economy of international trade. Annual Review of Political Sci-ence, 2, 91–114

[2] Conference proceedingbyYerra Shankar Rao “Cybercrime Assement “National Conference on Current Trends in Computing (NCCTC) ISBN No. : 978-3-642-24819-6, 23rd - 24th March, 2014,Page no10-14.,North Orissa University,Baripada Orissa

[3] India emerging as major cyber-crime centre (2009), Available at: http://wegather news.com/ 203/india-emerging-as-major-cyber-crime-centre/, Visited: 10/31/09

[4] By Jessica Stanicon (2009), Available at: http://www.dynamicbusiness.com/articles/articles-news/one-in-five-victims-of-cybercrime3907.html, Visited: 28/01/2012

[5.] Computer Hope (2012), Data Theft, Available at: http://www.computerhope.com/jargon/d/ datathef.htm, Visited: 28/01/2012.

[6.] DSL Reports (2011), Network Sabotage, Available at: http://www.dslreports.com/ forum/r26182468- Network-Sabotage-or-incompetent-managers-trying-to-, Visited: 28/01/2012.

[7.] PTI Contents (2009), India: A major hub for cybercrime, Available at: http://business. rediff.com/ slideshow/2009/aug/20/slide-show-1-india-major-hub-for-cybercrim

[8.] Virus Glossary (2006), Virus Dissemination, Available at: http://www.virtual pune.com/citizencentre/html/cyber_crime _glossary.shtml, Visited: 28/01/2012

[9.] Legal Info (2009), Crime Overview aiding and abetting or Accessory, Available at:

http://www.legalinfo.com/content/criminal-law/crime-overview-aiding-and-abetting-or-accessory. html, Visited: 28/01/2012

[10.] Shantosh Rout (2008), Network Interferences, Available at: http://www.santosh raut.com/ forensic/ cybercrime.htm, Visited: 28/ 01/2012

[11]Criminal Investigation Department Review, January 2 (Mis Cyber Crime Scenario In India Criminal Investigation Department Review January 19, 2008

[12.] PrasunSonwalkar (2009), India emerging as centre for cybercrime: UK study, Available at: http://www.livemint.com/2009/08/ 20000730/India-emerging-as-centre-for-c.html, Visited: 10/31/09 [13.] India emerging as major cyber crimecentre (2009), Available at: http:// wegathernews.com/ 203/indiaemerging-as-major-cyber-crime-centre/, Visited: 10/31/09

❑❑❑

45

The Role of cyber security in post globalization world

Prof. Dr. Vilas Sadaphal
Shripadrao Kadam Mahavidyalaya, Shirval

****

A Need for closer cooperation at a global level to improve security standards, improve information, and promote a common global approach to network and information security issues …

Introduction

The phenomenon of globalization is a historic process that extends over millennia beginning with tribal migrations, trade, and military conquest. However, the pace of globalization has intensified over the past 100 years as transportation, industrial, and communications technologies revolutionized commerce around the globel.

The Shipping and travel times for goods and people, once required weeks or months, reduced to hours. Communication times compressed from days to seconds. This current epoch of globalization brought new challenges for strategic intelligence as the virtual compression of time along with new weapons technologies created short warning times and potentially cataclysmic threat.The most recent dimension to the globalization process is the digital revolution, which is changing every form of life including commerce, warfare, and culture. As online military colleges focus on security issues, the roles of globalization and new technologies become integral to intelligence, counter terrorism, and strategic security matters.[1]

But before we get into the core of the subject, since cybersecurity is related to the internet and securing the data it carries stores and transmits, we first need to examine the importance of the internet's data flows and its effect on the global economy.Data flows are the foundation of the global economy. With the present acceleration of digitization of global enterprises, supported by the quick adoption of evolving technologies like that of cloud computing and data analytics, the importance of data as an input to industries has increased, and this is not only for information industries, but also for other manufacturing and traditional industries. According to McKinsey Report, 75 percent of the value created by the internet is in traditional industries.[2]Internet adoption is highly correlated with economic development. The fact that higher internet penetration is highly correlated with a host of measures of economic success suggests that achieving universal access requires not only reforms to the telecommunications sector, but also policies for helping individuals and firms to make the most out of the internet.The environment which influences the security of states undergoes dynamic changes. Its foresee ability decreases due to the increasing interconnection of security trends and factors. The threats, their sources and bearers are of both state and more and more non-state and supranational character. Internal and external security threats mingle and the differences between them are being removed. The importance of a complex approach is increasing; it combines military and civilian tools including diplomatic and economic resources to prevent threats and to mitigate their adverse effects. The requirements for readiness to respond to sudden threats in time and effectively are also increasing.

Information Security:

Information, supporting processes, systems and networks are important assets of an organization. Defining, implementing, supporting and improving information security may be essential for maintaining capability of an organization. Organizations and their information systems are threatened when they are subject to security threats from different sources including computer frauds, espionage, sabotage, vandalism and fires.

The sources of damages, such as computer bugs, hacker attacks and denial-of-service attacks, are more frequent and their hazardousness and sophistication are increasing. Information security is important from the viewpoint of critical infrastructure protection in both the private and the public sector. In both sectors information security is important for service availability and, at the same time, for avoiding or minimizing risks.

Cyber Security and Digital Trade:

Trade and cyber security are increasingly intertwined. The expansion of the internet globally and use of data flows globally by businesses and consumers for communication, e-commerce, and as a source of access to information and innovation, is transforming international trade. As global interconnectivity grows, however, so does exposure to the risks and costs of cyber-attacks. For example, form jacking—using JavaScript to steal credit card details from e-commerce sites—or supply chains hacks which exploit third party services and software to compromise a final target, undermine business and consumer trust in using the internet for commerce.[3] Protecting trust in a digitally connected world necessarily involves collaboration across borders between the public and private sectors because global networks, organizations, and supply chains rely on the same systems and software, most of it supplied by enterprises, and they face the same threats.

Cyber security standards.

Cyber security standards can build a common approach to addressing cyber security risks based on best practice. For instance, the International Standards Organization and the International Electro technical Commission have developed a number of cybersecurity-related standards, including the jointly developed ISO/

IEC series as well as sector specific-standards for electric utilities, healthcare, and shipping. Standards are most effective when they don't proscribe a particular approach but instead are frameworks for managing risk, relying on business and government to design cyber security measures most suitable to their business practices and risk profiles. In turn, the Cyber Framework relies on international standards such as ISO as references for its cyber risk management framework, with the result that the framework is not U.S. specific and can be adopted globally.

Globalization's Security Implications

Globalization is a multidimensional phenomenon: Information technologies, along with a variety of other technologies, are developing rapidly and spreading widely. Trade is expanding globally, as is the flow of private capital and investment. Interdependencies are growing in all aspects of our lives. These developments create real possibilities to achieve economic prosperity, spread political freedom, and promote peace.[4]

Yet they are also producing powerful forces of social fragmentation, creating critical vulnerabilities, and sowing the seeds of violence and conflict. Economic crises extend across state borders and are producing global hardships. All of these are aspects of what is commonly referred to as "globalization," and all have important security implications. Most dangerously, a variety of threats have become global in scope and more serious in their effects as a result of the spread of knowledge, the dispersion of advanced technologies, and the movements of people. These same developments, combined with expanding global economic interactions, contribute to some of the problems and resentments that lie at the root of these security threats. But paradoxically, many of those same aspects of globalization offer new opportunities to achieve economic growth and democracy, thereby ameliorating the threats as well as some of their underlying causes.

Conclusion

The national security issues most impacted upon by globalization are generally found to fall into three categories: the nature of security threats in a globalised world, the effects of the phenomenon of globalization on the pursuit of national security.

Create an international cyber court or similar body. Due to the growing number of cyber attack accusations among states and the difficulty of technical attribution, it would be beneficial to create an independent, international cyber court or arbitrage method that deals only with government-level cyber conflicts and that would be recognized and respected by all parties.

These are just a few of the many possible proposals that could help increase international cooperation in cyberspace and protect the stability and resiliency of the global digital economy. Of all these proposals, it is most important that the world does not allow the establishment of cyber norms to continue at today's slow pace. There is now no universal body working to enhance global cooperation in combating cybercrime and no mechanism for developing norms for state behavior in cyberspace.

References

1. Clarke, Adele. 2005. Situational analysis: grounded theory after the postmodern turn. Thousand Oaks: SAGE.

2. Collier, Stephen, and Andrew Lakoff. 2015. Vital systems security: reflexive biopolitics and the government of emergency. Theory, Culture and Society.

3. Cooper, Melinda. 2006. Pre-empting emergence: the biological turn in the war on terror. Theory, Culture &Society .

4. Cukier, Kenneth, and Viktor Mayer-Schönberger. 2013. Big data: a revolution that Will transform how we live, work and think. Lon-

don: John Murray Publishers.

5. Dauderstädt, Michael. 2003. WeltinnenpolitikangesichtsglobalerUngleichheit: zur Dean, Mitchell. 2010. Governmentality. Power and rule in modern society. London: SAGE.

6. Deleuze, Gilles. 1990. Post-script on the societies of control. October 59:3–7.

7. Dillon, Michael. 2003. Virtual Security: A Life Science of (Dis)order. Millennium. Journal of International Studies .

8. Dunn Cavelty, Myriam. 2013. From cyber-bombs to political fallout: threat representations with an impact in the cyber-security discourse. .

Footnotes:

[1] Joshua P. Meltzer, "The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment, Brookings 2014.

[2] Symantec Internet Security Threat Report, April 2019.

[3] White House National Cyber security Strategy, September 2018

[4] NISTIR 7298, Revision 3, "Glossary of Key Information Security Terms", July 2019.

❑❑❑

46

Intelligible Communication: Crisscross for Cyber Security

Dr. Anand Uddhav Hipparkar
Associate Professor, Dept. of English,
S. M. Joshi College, Hadapsar, Pune

****

Abstract

It is a recognized fact that cyber security professionals are among the most in-demand workers everywhere in the world. It isadvisable and indispensableto have a security set-up to avert cyber-attacks in the digital age.However, communication with empathy and other soft skills has importance in cyber security. In fact, a skills transformation is continuing as business firms go back over the skills in cybersecurity they considerimportant for attaining their objectives.Thereis a growing demand for top-performing personnel in the company not only for thosewho are concerned with production but also for those having inter-disciplinary talents and those who are excellent communicators. They should be good at reading other people, and are compassionateadministrators. The technologydriven industry has the need of human resource with adequate soft skills, possessing ability to think analytically, write influentially, and stimulatecoordination. They are hard-won and rigorous.

Key words: cyber-security, data breach, business, communication,strategy, objectives, industry, plan, skills, etc.

Introduction

The present day digital age reveals that business activities have becomemore and moredefenseless to unbelievableincidents of cyber threats. There have been so many newfangledways that are being taken up.The modes such as email, cloud environments, applications, payment accesses and data centres are highly vulnerable to cyber-attacks. Almosteach business unit is now a 'digital business' in some or the other sense.It is a strange contradiction that though these digitally-enabled business units unquestionably make security more challenging, theircrucial principles remain the same. Irrespective of type of the business, safety teams are required to work to create a that considers all the technologies people use, from cloud to big data and the (rather troublesome) internet of things of our turbulent times. Moreover, the fact nowadays remains that data has become a conspicuousteamster of business importance. Hence all business units need to get acquainted with their informationsite, which is, then, shared with third parties and the way it is being secured.

The businesses have reported increasingscarcity of cyber security job aspirants who can also work well as team performers and manage teams efficiently. It is also rare to find a cyber-security candidate who knows the position's legal and ethical accountabilities. One of the majoranxietiestoday is that college students lookingat the IT industry,most of the times, do not realize what 'security' is?

Someroles likesenior security leadership positions within the cyber security field are high in-demand. Typically, these roles, of course, require a proven track record as a strong communicator who can plan and execute complex projects. These are time-consuming skills and require a solid educational foundation. As technology and business interconnect at various points across nearly all industries, it is imperative for policymaking personnel to have anoperational knowledge of cybersecurity procedures.

Therefore, it isan evident truth that cybersecurity specialistsare among the most in-demand in the world, today. These security professionals value communication, empathy, and other soft skills in cybersecurity candidates. A "skills transformation" is underway as businesses reconsider the skills in cybersecurity they deem critical for achieving their goals.The recent studies reveal that the highest-performing teams in the industryworldwide are not those havinghighly skilledprofessionals but those possessing interdisciplinary employeeshaving excellent communication skills. Moreover, they are good at reading other people and have empathizingqualities. It is also observed in tech industry that soft skills like the capacity to think analytically, write convincingly and encourage cooperation, are hard-won and rigorous.

There is agrowing scarcity of candidates for cybersecurity jobs who can work well as team players and handle teams efficiently. In this day and age, it has become scarce to find a cyber-security candidate who knows legal and ethical responsibilities of a position. The majoranxiety is that college students who look at the IT industry,every so often, donot know what security is? It is tough to catchthe candidates interested in information security as the particulars of what is actually involved are often vague from the job descriptions.

Some of the most in-demand roles within the cybersecurity field are those in senior security headship posts. Generally, these roles demand a proven profile as a strong communicator who can bring forth a blueprint and implement complex assignments. These are time-taking skills as far as learning is concerned but they necessitate a sound educational base.

It is essential for managerialheadship to haveoperationalinformation of cyber security proceduresfor the reason that technology and business interconnect at variouslevels across almost every industry sector.

Importance ofCommunication skills

It is beingargued that the employees in IT segment possessweakinterpersonal skills. Of course,it does not relate to every IT professional yet the fact remains thatweak communication in the field ofcyber security can inviteterrible consequences. It is a mandatehighly important todaythat the cyber security experts have got to communicate efficaciously with employees and business patrons at every level.

Every cyber vigilant security professional should try to develop the skills of transforming technical information produced by security teams into something important that others in the organization can comprehend is enormouslyessential skill. If the information is conveyed in the exact way, it can help in transferring the intricacies of the cyber world and the technical aspects of the dynamic nature of cyber dangers and the information setting itself.The business users of IT systems, in most occurrences, should take onto new methods and rules to improve security. But it is the most difficult to change people and their behaviour. Many security leaders have held that they are facing difficulties in this area. There is a need of creating an effective end user adoption policywhich was one of the biggest challenges.It is vital that end users need to understand their part and obligation in keeping the security of organizations. To cut a long story short, humanizing the employees is of immense importance and is a noteworthy prerequisite of upholdingarduousdatasafeguardingethics.

Need of awareness

Regardless of all the brilliantly advanced tools and methods in the security market, employees still remainat the forefront of cyber security. But so many of them may be completely unaware of the threats posed by things like social engineering. There is anecessity of educating the latest coercions and the ways to avoid or aggravate them. Theinstant the instruction saying something along the lines of “don’t open attachments” or “don’t click on links” in unwanted e-mails, people easily fall prey to such e-mails andthe message does notget through clearly. The overall worldwide scenario reveals that phishing and even whaling attacks have beenpersistentlymounting.

Therefore,more often, communication skills have beenperformingexceptionally well on security course curriculums yet the issue is wider than itseems. Many establishmentsdo not provide any education or communications related to security in place. A large number of office workers are deprived of training in cyber security awareness. Thus, the condition is so dismal that mostof them stated they could not confidently define a phishing attack.

Keeping administrators in the ring

As today’s urgent need, cyber security needs to be viewed as a matter of vitalconcern. Wemust not consider itjust as a formality. The obligation should be assigned to business owners to completelyrecognize the threats they produce for customers and take action to alleviate them. In some business firms, employees have even called for CEO pay to be linked to the success of a businesses cyber security measures. These problems are related to each level of procedure of an organization and, intrinsically, flawless communication is required with the boardroom – right to the very top.

The business firms have realized the defenselessness that digital technologies are opening them up to, and they are looking to security professionals to advise them. But their advice will only be heeded if it is clearly understood.

For a very meticulous watch on cyber harassment, one requires certain crucial work practices, including the ability to work meticulously and in a detail-oriented way. The following abilities also become very useful:—

1. Eagerness to look at technical issues and analyze them from all sides.

2. Eagerness and a high degree of adaptability.

3. Strong investigative and problem-solving skills.

4. Anup-to-date understanding of common web susceptibilities.

5. Upholding awareness and knowledge

of contemporary standards, practices, procedures and methods.

A communication strategy necessitates team work with the right roadmap and tasks that are not excessivelyunapproachable. One way can be to stimulate from an old journalism trick and use the 5W's: who, what, when, where, and why.

Who: First and foremost, it is vital to resolve who should be engaged in evolving the communication plan. It can be a firm's managing partner/director or CEO, etc. A marketing or communication director is not possibly the best choice. The input should come from the firm's executive management team and IT (CS) department/team, legal counsel, administrative leadership, HR executives, and any communications agency and software retailersas the case may be. There is a need of high-level strategic input from senior leadership and department heads to confirm that all situations are taken into account. The second mainside is in case of a cyber-attack; instantaneous decisions with potentially significant impacts will need to be made. As a result, activities drawn in the plan should be executedspeedily.

In the planning process, it is essential to decide who the key decision-makers are?How will they work when the time comes, and who is taking particular responsibilities?

In the third phase, stakeholders comprising employees, clients, and perhaps media, professional associations, law enforcement, and even government bodies should be approached.

What: The plan should consist of basic key messages and categories of information the firm will need to share with its parties in case of a cyber-attack. Information should be shortly modifiedconsistent with the situation but a basic content should be put together in advance, including statement for press, internal and external memos, a news release, and messaging for the firm's digital channels and website. The questions should be answered, specifically, if the attack was the result of an employee or software error, how much data was compromised and by whom? Some such scenarios could be written in advance and it is helpful to have all the key decision-makers involved in the development process.

When: The point at which the plan will be applied should be determined as well as how it will initiate the response team should be triggered. These issues should be stated thoroughly.One particular role has the CSPs so it is predictable that CSP's contribute to the development and use of a telephonic communication plan for a worst-case situation.Multiple communication methods and channels can be affected in case of a cyber-attack like own phone and voice mail system if they are VOIP-based, company phone system, company website (if it is hosted in-house), connections with customers, employees, the public, and the media.

Where: The company should prearrange various channels available to communicate its messages to its addressees, i.e., social media, email, phone directories, and contacting straight to the person. Depending on situation and actions needed, it will be decided which channels are preferred over another or to use them all.

Why: The main goal of the strategy is to stop the loss of clients and income. Many companies lack a disaster communication plan, namely, for a data breach, often, caused by fewer resources like time and money. Sometimes, the plan has no priority because it has no immediate or direct impact on business revenue.

In case that the core network is compromised, every computer becomes a stand-alone machine with no access to company record. Employee contact information, vendor lists, or other key phone lists could be unreachable. IT security is responsible if the organization does not have a security team. The employees must be held responsible for a response plan in case of a crisis. The legal advice is necessary if, for instance, customer credit card details have been pilfered.

Best practices of Cyber security internal communications

In case of an occurrence of acyber-attack, the cooperative efforts and communication between the departments are very essentialtobe assured that all security measures are at place. The IT section should talkto the chief information security officer (CISO)—who is an administrator in upper rank having responsibilities such as developing the company's information security design to protect its systems and resources finely.

The head of the customer has to speak to the director of development when a customer findsa security virus in their website. The head has to take quick action if the department is affected by deficiency of interdependent communication when attackoccurs and customers whose data was stolen by a hacker due to such communication disaster.

These days, it is fairly common that the poor communication culture from other companies gets thrown in the mix when employees are hired on from the outside. Bad communication could determine loosing of skill of employees than being demoralized. On the other hand, right communication involves internal meeting where the employees can talk to each other about the cyber security problems. Sometimes, in the internal meeting, other objectiveshave primacy or the CSP's have no knowledgeabout the correctapproach.

The motivated employeessee company culture and team communication as means to success and contentment. Often, the missing communication and company's weakening security, particularly cyber security are key factors.

Some methods to improve communication in Cyber Security

1. Improving communication in cybersecurity strategies through training

Cybersecurity does not refer only to locks, firewalls, and the latest technology to protect employee's sensitive data but also their susceptibility.

Employees make mistake and hackers take advantage to access to data. Many cyberattacks and destroying of data happen because of unintentional employee actions which make organization business vulnerable i.e., by clicking a phishing email that downloads malware and gives sensitive information to someone or using non-protective passwords.

One common problem is that a cybersecurity strategy and security policies in an organization require the employees who are not aware of them, i.e., to be informed about contained policy about on what to do if a cyberattack is supposed. In this case, the employees could make an error or waste time in reporting it to the right people, potentially causing more damage for the organization.

Another problem is social engineering, which is rapidly becoming a big threat against businesses of all types and sizes. In security, social engineering is a broad term used to describe an information technology attack that relies heavily on human interaction and often involves tricking other people to break normal security procedures.

Social engineering refers to the techniques used to exploit human vulnerability to bypass security systems to gather information. Social engineering attacks imply interaction with other individuals, indicating also psychological and ethical aspects. About social engineering (SE), there are many differing opinions.

2. The role of CSP's

The CS professionals (CSP's) have a special role in preventing cyber-attacks. In case of a threat to security systems, the decisions of information security professionals are very important. In case of an emergency, effective communication is crucial. If IT systems fail, a quick communication with employees is necessary as well as to coordinate an effective response. Many CSP's believe that their organizations' security controls do not provide adequate protection against advanced cyber-attacks. They affirm that executives do not put effective security controls in place and do not evaluate a data breach with financial loss. The majority of CSP's professionals fail to communicate security risks effectively to upper management.

Along with managing and developing response plans against emerging security threats, cyber-security professionals also need to inform upper management about the seriousness of security threats and convincing them to allocate adequate resources to protect against data breaches.CSP's must turn technical details of security risks into information that can be easily understood by upper management.CSP's should address these issues directly with the CEO and executive team approaching directly their attention and not be filtered out by intermediate players.

As more data moves into the cloud and across other devices, companies face a greater risk of losing sensitive information to attackers or unauthorized users. So many businesses fail to set quantitative parameters for risk (risk appetite) instead, to align the language.

Conclusion

In a nutshell, the cyber security situation is changing fast. The cyber-attacks are risingwith the use ofcutting-edge technological means and are a matter of curiosity because businesses are more technology-driven. Theswiftchanges should be made in business policies to adjust to other changes because of CS risks which change in scope and potential impact quickly. The organizations need to keep the means ready to communicate and pull quickly through in the event of anemergency. The intensity of a cyber-attack and its impact depends on these elements.

On the whole, CSP's must be set to communicate effectively in the current testing environment with the use of the best communication tools and data for the right audience at the right time. The costs of ineffectual communication, resulting in misunderstanding security risks, can be highly ruinous. But carving a design and understanding the business objectives, the stakeholders, their needs, and the risks, will help the CSP's to provide a clear and right message. It is important to be in no doubt that communication is addressed to the exact stakeholder group and then confirmed that it has been understood.

The intensity of a cyber-attack and its consequence depends on above factors. The decisive communication stages, a proper communication culture, consistent training support in case of a breach to controlstoppage and destruction are significantmattersthat can be further studied. It is possible to drawand develop a well-structured and well-practiced incident response plan that can reducedamages of cyber-attacks.

Works cited:

1. Ablon, Lillian, Martin C. Libicki and Andrea A. Golay. "Markets for Cybercrime Tools and Stolen Data." RAND Corporation. 2014.

2. Applegate, Scott D. "The Dawn of Kinetic Cyber." Presented at the 5th International Conference on Cyber Conflict, Tallinn, Estonia, June 4-7, 2013.

3. Arquilla, John. "Cyberwar Is Already Upon Us." Foreign Policy, February 27, 2012.

4.Cartin, Josh M. "Don't Forget the Humans: Toward a 21st Century Offensive Cyber Strategy." Global Security Studies 5, no. 2 (2014): 12-26.

5. Jacobson, R. V. Risk Assessment and Risk Management. In Bosworth, et al., (Eds.), Computer security handbook. New York, NY: John Wiley & Sons, 2009.

6. Kahn, David. The Code Breakers: The Story of Secret Writing, Macmillan, New York, 1967.

7.MuraliTalasila (2010), "Emerging Technologies in Combating Fraud" Proceedings from Conference on Cyber Security. "Emerging Cyber Threats & Challenges," CII, Confederation of Indian Industry, Chennai, 2010.

47

A study of dropout rate in Institution's in Higher Education in India

Prof.Mrs. Alka Gadakh
Assistant Professor in Computer Science,
St.Mira's College for Girls, Pune

****

Abstract

In order to defeat the COVID-19, Pandemic, Indian Government announced complete lockdown in the country starting on March 24, 2020 and the same was extended to 3rd May, 2020 in the second phase. Though the lockdown was necessary and inevitable so as to prevent the faster spread of Novel Coronavirus (Covid-19) and to save lives of people of the country, it is going to affect the various sectors of our economy severely. The Banking and Non-banking finance companies (NBFCs) which are backbone of India's economy are not exception to the above. This article is an attempt to assess the impact of this pandemic on Banks and NBFCs due to lockdown which has resulted into closure of all commercial organisations, educational institutions, public and private offices, suspension of means of transportation, etc. The conclusion in this regard is based on the views expressed by several groups including economists, financial institutions like IMF, World Bank and consulting firms. Secondary sources of information are used to collect the required information. The article has indicated a very severe effect of lockdown on banks and NBFCs in case it prolongs beyond July 2020.

Key words: Covid-19, India's economy, Indian Banks, NBFCs, NPAs, Lockdown

1. Introduction

In India the most problem of upper education modernization is that the balance between inputs and relevant outputs, specifically the correct balance of enrolled and graduated students. The university students' dropout rates result the waste of taxpayers' money, a lower proportion of the undergraduate s college students and, consequently, very lower employment opportunities in highly qualified positions. the varied universities in India dropouts was a crucial topic in many countries, also because it isn't only the waste of taxpayers' money but now it's also one amongst the standards for assessing and evaluating teaching learning institutions. Unfortunately, the strategic policy of upper education institutions may increase the amount but not necessarily the standard of the undergraduates. Several studies indicate that one among the important factors of students' dropout rate is that the subject studied at university.

The dropout rate is higher among students in under graduate disciplines, and among students with relatively low levels of prior qualifications. In India research in indicate that there are various others factors which are related to the faculty students' dropout rate in educational activity institutions including individual characteristics, qualities interactions within colleges, and institutional .The purpose of this research paper is to analyses ad explanation of the causes of the primary year students' dropout rates in education institutions using the 000 data of Under Graduate faculties in various University in India.

2. Review of Literature

A literature review could be a piece of educational writing demonstrating knowledge and understanding of the tutorial literature on a particular topic placed in context. A literature review also includes a critical evaluation of the material; this can be why it's called a literature review instead of a literature report.

a. to grasp, analyses so find the difference between different prediction techniques of Machine learning.

b. to spot and understand different student attributes which are mainly used for the predicting the coed performance.

c. to spot and understand the various prediction techniques which are mainly used for predicting the coed performance.

3. Objectives of the Study

1. To get a classification educational model and implement them on academic information provided by the university.

2. To develop educational system with the flexibility to predict students who are in danger to dropout in under graduate program.

3. The generated educational model is ready to see the foremost significant variable that affects academic performance, which are the abandoned subjects.

4. Research Methodology

This research is descriptive in nature. The Secondary sources of knowledge are used for this Secondary data has been collected from different published sources like books, , Bulletin, news journals, newspapers and magazines, and internet sites etc

5. The most causes and problem of dropout rate in Institution's in Higher Learning

a. A fashionable Tuition Fee

There was the primary and extremely sensitive reason why students drop out. There are rocking rapidly fees increase student debts, pushing those from underprivileged backgrounds suffer further. The research survey conducted that around 40 percent of 2020-2021 young students who couldn't afford senior college, dropped out. "I can't afford my college fees"! Further, the coed Enrollment emerging Trends by high-needs Subgroup 2020-21 confirms the dropout rate because of unaffordability.

b. Some Students not prepared academically

The most of scholar's lack of readiness may be a major done something wrong in high school graduation rates and first-year students are the primary prey. "I'm simply not ready for it, chucking up the sponge of faculty doesn't relate me! "They quit educational activity because they're simply not ready for it. We make research survey by Education Trust shows that about 40% of Under Graduate from drop-out of without completing senior college and career-ready courses of study program.

c. The scholars are Unhappy with the school

The case is worse when their senior colleges don't take them from the method of job recruitment through placement appropriately. the amount of program communications, orientations, and events to create student show up for the course goes futile when most institutions forget to stay up the identical effort. a recurring worry roommates, overloaded with study course works may well be the subsequent main reasons for college students to drop out. there are unhappiness could also arise out of the distrust that develops out of the sensation that in spite of paying such a lot of fees, the institution forgets to stay students happier. a totally without skill at particular activity clouds around them after they feel that they're not up to the duty ahead.

d. A Discouraging environment

They feel bypassed when the senior colleges don't follow Outcome Based Education. "No one cares if I attended", replied a university student who was recently interviewed by Grad Nation.org survey for his falling by the wayside. The Motivation barrier will be seen here during this student's case. There are two styles of motivation barriers exist internal and external. The interior barrier would come with a less motivational educational learning environment, whereas external would be lack of peer collaboration online, fear of isolation and also the absence of social cues.

e. Picking / Choice the incorrect course

It is unfair to conceive to a course of study only to get later that the program isn't what they expected. Within the Course evaluation done at the first stages can become a right mentor here, where college students are exposed to select courses after much thought, by their own. “I am undecided." Problems bud out from here. Determining the proper course of study for a successful career path can always be of struggle. This might be a winding road instead of a line. it's unbelievable, but the reality is around 75% of senior college students get confused about changing their major a minimum of once by the top of their study program.

f. An instructional inadequacy

When the next education system lacks this, there's a dip within the college student’s performance, which becomes a serious reason for student pull out. the bulk Students should be routed with a solid resources learning management system that has polls, notifications, quiz, assessments, and rubrics.

g. Be incompatible with work and family commitments

A Completion of senior colleges becomes an ordeal for the above-said reasons. If not addressed adequately by campus management, these reasons might cause a big decrease in student retention. This wakes up colleges and universities to debate the faculty student retention crucially. Might appear as if a thorn on one’s side. Fret not, reading one among our blogs on a way to improve student retention in higher education? Can facilitate your gain an inspiration on a way to boost college man retention can help. The conflict of interest between home, job and study can cause a breach in education. This scene is most typical among all department of education, community colleges, and state universities.

6. Conclusion

The results of this research show that approximately 35% of school students leave the humanities, Commerce and Science faculties of under graduate during the primary study year and it depends on the faculty’s curriculum and students’ Gymnasium grades. The information from different academic years are recommended to incorporate for further investigations of faculty students dropout rate.

7. Suggestion’s

1. Basic Core Strategies

The Mentoring may be a one-to-one caring, the supportive relationship between a mentor and a mentee that's supported trust. Tutoring, also a one-to-one activity focuses on academics and is a good practice when addressing specific requirements and desires like reading, writing, or math competencies.

Within the Service-learning connects meaningful community service experiences with academic learning. This teaching/learning method to promote personal and social growth, career development, and civic, social responsibility and may be a strong vehicle for effective college reform in the least grade levels.

2. The Foundational Strategies

A continuing process of evaluating goals and objectives associated with senior college policies, practices, and organizational structures as they impact a various group of learners. When all groups in an exceedingly community provide collective support to the school, a robust infrastructure sustains a caring supportive environment where youth can thrive and achieve. A comprehensive violence prevention plan, including conflict resolution, must accommodate potential violence furthermore as crisis management. A secure learning environment provides daily experiences, in the slightest degree grade levels that enhance positive social attitudes and effective interpersonal skills all told college students.

3. Early Interventions

In this research paper consistently finds that family engagement features a direct, positive effect on college student’s achievement and is that the most accurate predictor of a student’s success in class. A Birth-to-five interventions demonstrate that providing a additional enrichment can enhance brain development. the foremost effective thanks to reduce the quantity of student s who will ultimately drop out is to supply the simplest possible classroom instruction from the start of their college experience through the first grades.

4. Managing and Improving Instruction

The Teachers who work with youth at high risk of educational failure must feel supported and have an avenue by which they will be still develop qualities and skills, techniques, and study innovative strategies.

In Active learning embraces teaching and learning strategies that engage and involve college students within the learning process. The senior college Students find new and artistic ways to resolve problems, achieve success, and become lifelong learners when educators show them that there are other ways to be told.

Reference

1. Jain, L. (2008) "Dropout of Girls- Child in Schools", Northern Book Center, NewDelhi.

2. Khasnabis, R. and Chatterjee, T. (2012) "Enrolling and Retaining Slum Children inFormal Schools A Field Survey in Eastern Slums of Kolkata", Economic and PoliticalWeekly, Vol. 42, No.22, pp. 2091-2098.

3. R. C. Tyagi (2010-14) "Monitoring and Evaluation of SSA Programme: Reports",Ministry of Human Resource Development (MHRD) New Delhi.2. The National Sample Survey Office (NSSO) 64th round (2007-08)

4. Sharma, Ruchita, Shubhangna Sharma and Shipra Nagar, (2007), "Extent of Female School Drop outs in Kangra District of Himachal Pradesh", Journal of Social Science, 15(3): 201-204.

5.Choudhury, Amit (2006), "Revisiting Dropouts: Old Issues, Fresh Perspectives", Economic and Political Weekly, December 16.

6. Desai, Uday (1991), "Determinants of Educational Performance in India: Role of Home and Family", International Review of Education, Vol. 37, No. 2 pp. 245- 265

7.Rao, Mohan, M.J. (2000). "Migration of labour and school dropouts", Social Welfare, 47(6): 26-31 8.Lall, Marie, (2005), "The Challenges for India?s Education System", Chatham House, New Delhi, 9.Pratinidhi, A.K., Warerkar S.V and S.G. Grad, (1992), "A study of school dropouts in a n urban slum community", Demography India, vol. 21 No.2 pp. 301-305

10. Khasnabis, R. and Chatterjee, T., (2007) "Enrolling and Retaining Slum Children in Formal Schools A Field Survey in Eastern Slums of. Kolkata", Economic and Political Weekly, Vol. 42, No. 22, pp. 2091- 2098.

11. Borooah, Vani K (2003): „Births, Infants and Education: An Econometric Portrait of Women and Children in India?, Development and Change, 34, pp 67-102.

12. Shariff, Abusaleh (1995): „Socio -Economic and Demographic Differentials between Hindus and Muslims in India?, Economic and Political Weekly, 18, pp 2947-53.

13. Sengupta, P and J Guha (2002): Enrolment, Dropout and Grade Completion of Girl Children in West Bengal?, Economic and Political Weekly, 37(17), pp 1621-37.

14. Bhat, P N Mari and A J Francis Zavier (2005): Role of Religion in Fertility Decline: The Case of Indian Muslims?, Economic and Political Weekly, XL, 5, pp 385-402.

15. Husain, Zakir (2005), "Analysing Demand for Primary Education Muslim Slum Dwellers of Kolkata", Economic and Political Weekly, January 8, 2005

16. Rao, Rama G and. Mohanty S.K, (2004), "School Enrolment and Dropout: Policies and Achievements", Paper presented in seminar on follow-up of the National Population Policy- 2000: Focus on EAG states, 25-27 Oct. 2004.

17. Upendranath, C. (1995). "Education of girls in India: The daunting task ahead." Journal of EducationalPlanning and Administration, 9: 81-92.

18. Compendium of Environment Statistics, 2001. Report No. 147, NSSO 49 Round, 1993.

19. Through Net, "Life in a Slum", (2010), BBC News, Retrieved 5 March 5.

20.The National Sample Survey Office (NSSO) 64th round (2007-8)

21. Through Net, https://en.wikipedia.org/wiki/Dharavi

48

Qualities of a successful manager for business in India

Dr. Sahebrao Daulat Nikam
B.Y.K.College of commerce, Nashik

****

Abstract.

Management is essential to any business or non business organisation. we can give an example of business organisation i.e Sapat Chaha Pvt. Ltd Co. Nashik . Which is manufacturing tea for the people. their main motive is to earn profit.

when we talk about non business organisation we can give an example i.e. various colleges.schools.clubs,etc.all college are non business organisations.and main motive of these colleges are to provide education at affordable cost not to earn profit . Each and every organisation should have exellent management to develop and to become world class organisation . Management is nothing but it is very essencial to any type of business either it is small, medium or larger, Management has to co ordinate ,to control,to plan and and to do perfect and accurate uses of resources in any type of busines for achieving the goal and objectives of the business and next important thing is that succes of any type of business always depends upon efficient management. Management play'svery important role in all business organisations in this modern age, the success of any business always depends upon the importent qualities of managers and Skills of managers. Management is a developing science but we can not compare to phisics, chemestry, biology etc. It is related to human being human behaviour is always changing and we cant predict it so the role manegement is very imporent to get success of any type of business

Introduction :

Many management thinkars have given us many definition to understand the meaning of management..

George R.Terry, "Management is a distinct process consisting of planning, organising, actuating and controlling performance to determine and accomplish the objectives by the use of pepole and resources".

Theo Haimann,"Management is the sum total of all processes including planning, direction, control and organisation"

from both the definitions, it is clear that.management consists of getting things done through others by directing their efforts in an integrated and co-ordinated manner for business objectives. It is a process consisting of functions such as planning, organising and controlling etc .In this way manager should play very importent role to get sucess.

Management is one of the most important activities of human life. To achieve aims that could not be achieved individually, people started forming groups. Management has become essential to ensure the coordination of individual efforts. Management applies to all kinds of organizations and to managers at all organizational levels. Principles of management are now used not only for managing business but in all walks of life viz., Government, Military, Social and Educational Institutions. Essentially, management is same process in all forms of organization. But it may vary widely in its complexity with size and level of organization. Management is the life giving element of any organization.

Keywords: Management,Business, Organisation, Goods,Development,Quality, Planning,Direction.

Objective :

1. To study the qualities of successful manager.

Methodology:

The information collected by secondary sources **Secondary source:** Newspapers, Magazines, Books etc. has been used to get information. The information was obtained through a study of published books.

Qualities of a Successful Manager:

He should have various qualities for doing his work properly:

1. Education:

without education we cant get success so each and every manager should have good education as far as education is concern..A manager must have proper educational background. These days managers are supposed to have management education, besides other education.A manager has to undertake a number of all qualifications.it also helps in understanding the things and interpreting them properly. The knowledge of business environment is also important for dealing with various problems the organization may face.

2. Intelligence

A manager has to perform more responsibilities than other persons in the organization. He should have higher level of intelligence as compared to other persons. Intelligence will help a manager in assessing the present and future possibilities for the business. He will be able to see the things in advance and take necessary decisions at appropriate time.

3. Maturity:

A manager should have mental maturity for dealing with different situations. He should have patience,and he should be good listener and quick to react to situations. He has to take many decisions. which may affect the working. if not taken properly. He should keep calm when dealing with subordinates. All these types of qualities will come with mental maturity.

4.Positive Attitude:

Positive attitude is an asset for a manager. A manager has to deal with many people from inside as well as from outside the organization. He should be positive to various suggestions and taken human decisions. He should try to develop good relations with various persons dealing with him. He should understand their problems and try to become a helping hand.

5.Foresight:

A manager has to decide not only for present. There are rapid changes in technology, marketing, consumer behaviour, financial set up etc. A manager should visualize what is going to happen in future and prepare the organization for facing the situations. The quality of manager will help in taking right decisions and face the various problems. In case the situation is not rightly assessed then the organization may faces many problems.

6. Patience :

Patience is an art and a skill that can take more time to perfect. If patience is one of the qualities of a manager that you need to improve, try taking four deep breaths when you feel yourself starting to lose your cool.

7..Communication :

To be a successful manager, you have to be a good communicator. This quality of a manager encompasses more than just the words you say. It includes:

A. Your ability to get others to listen to your ideas

B. Your ability to get along with others

C. The clarity of what you say

D. Your ability to attract others

Many managers have good communication with lengthy explanations. But effective communication is more about clarity and brevity than using a lot of words to convey what you’re trying to say.A manager who wants to communicate well will be as clear as possible in what they say and take the time to make sure that everyone understands.

8.Good Judgment :

Every manager should have good judgement Though you can improve your judgment with practice, the foundation of this quality of a manager includes:

A. How you look at the world around you

B. How you listen to what others say

C. How you learn from that information

At first, good judgment is often the byproduct of your unconscious mind. With practice, you'll be able to exercise good judgment. You'll be able to examine the situation actively and come to a conclusion.

9. Ability To Listen :

The ability to listen is one of the qualities of a manager that you should never neglect. We do, after all, have two ears but only one mouth. Whether you're in a team meeting. the bulk of your activity should be listening rather than talking.

easy way to improve this skill he should listen what your team members say without interrupting. Formulate a response based on the information they've conveyed. Then, before you speak, think about what you want to say and how you want to say it.

10. Competence :

If you want to lead effectively and have your team members follow you need to be competent in every aspect of your job.That doesn't mean you have to be an expert, but you should at least have a healthy knowledge how to be efficient and successful in everything you do and everything you ask your team members to do.When you're competent in your business and exercise as many qualities of a manager as possible, your team members will follow your example not because they have to, but because they want to.

11.Organization :

As a manager, not only do you have to keep yourself organized, but you also have to keep your team members organized and Nowhere is that more obvious than in the scheduling process. There are so many different tasks to be done .

Conclusion :

without education we cant get success. Intelligence will help a manager in assessing the present and future possibilities for the business. Positive attitude is an asset for a manager. Patience is an art and a skill that can take more time to perfect. If patience is one of the qualities of a manager that you need to improve, try taking four deep breaths when you feel yourself starting to lose your cool. A manager should have mental maturity for dealing with different situations. He should have patience,and he should be good listener and quick to react to situations..The ability to listen is one of the qualities of a manager that you should never neglect. We do, after all, have two ears but only one mouth. Whether you're in a team meeting. the bulk of your activity should be listening rather than talking.

petence :

If you want to lead effectively and have your team members follow you need to be competent in every aspect of your job.That doesn't mean you have to be an expert, but you should at least have a healthy knowledge how to be efficient and successful in everything you do and everything you ask your team members to do. As a manager, not only do you have to keep yourself organized, but you also have to keep your team members organized

References :

1.Essentials of Management, Horold Koontz and Iteinz Weibrich,McGrawhills International

2.Principles & practice of management, Dr. L.M.Parasad, Sultan Chand & Sons New Delhi

3.Management: Concept and Strategies, J. S. Chandan, Vikas Publishing .Principles of Management, Tripathi, Reddy,Tata McGraw Hill.

4. Business organization and Management, Talloo, Tata McGraw Hill.

5..Essential of Business Administration ,K.Aswathapa Himalaya Publishing House.

❑❑❑

49

Recent Trends in Cyber security

Mr.Kashinath Shivaji Gangode
Shripatrao Kadam Mahavidyalya Shirwal

****

ABSTRACT

Cyber Security plays an important role in the field of information technology.Securing the information have become one of the biggest challenges in the present day. When ever we think about the cyber security the first thing that comes to our mind is 'cyber crimes' which are increasing immensely day by day. Various Governments and companies are taking many measures in order to prevent these cyber crimes. Besides various measures cyber security is still a very big concern to many. This paper mainly focuses on challenges faced by cyber security on the latest technologies .It also focuses on latest about the cyber security techniques, ethics and the trends changing the face of cyber security.

Keywords: cyber security, cyber crime, cyber ethics, social media, cloud computing, android apps.

1. INTRODUCTION

Today man is able to send and receive any form of data may be an e-mail or an audio or video just by the click of a button but did he ever think how securely his data id being transmitted or sent to the other person safely without any leakage of information?? The answer lies in cyber security. Today Internet is the fastest growing infrastructure in every day life. In today's technical environment many latest technologies are changing the face of the man kind. But due to these emerging technologies we are unable to safeguard our private information in a very effective way and hence these days cyber crimes are increasing day by day. Today more than 60 percent of total commercial transactions are done online, so this field required a high quality of security for transparent and best transactions. Hence cyber security has become a latest issue. The scope of cyber security is not just limited to securing the information in IT industry but also to various other fields like cyber space etc.

Even the latest technologies like cloud computing, mobile computing, E-commerce, net banking etc also needs high level of security. Since these technologies hold some important information regarding a person their security has become a must thing. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic wellbeing. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as governmental policy. The fight against cyber crime needs a comprehensive and a safer approach. Given that technical measures alone cannot prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cyber crime effectively. Today many nations and governments are imposing strict laws on cyber securities in order to prevent the loss of some important information. Every individual must also be trained on this cyber security and save themselves from these increasing cyber crimes

2. CYBER CRIME

Cyber crime is a term for any illegal activity that uses a computer as its primary means of commission and theft. The U.S. Department of Justice expands the definition of cyber crime to include any illegal activity that uses a computer for the storage of evidence. The growing list of cyber crimes includes crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying and terrorism which have become as major problem to people and nations. Usually in common man's language cyber crime may be defined as crime committed using a computer and the internet to steel a person's identity or sell contraband or stalk victims or disrupt operations with malevolent programs. As day by day technology is playing in major role in a person's life the cyber crimes also will increase along with the technological advances.

3. CYBER SECURITY

Privacy and security of the data will always be top security measures that any organization takes care. We are presently living in a world where all the information is maintained in a digital or a cyber form. Social networking sites provide a space where users feel safe as they interact with friends and family. In the case of home users, cyber-criminals would continue to target social media sites to steal personal data. Not only social networking but also during bank transactions a person must take all the required security measures.

technology and healthcare executives nationwide, Silicon Valley Bank found that companies believe cyber attacks are a serious threat to both their data and their business continuity.

· 98% of companies are maintaining or increasing their cyber security resources and of those, half are increasing resources devoted to online attacks this year

· The majority of companies are preparing for when, not if, cyber attacks occur

· Only one-third are completely confident in the security of their information and even less confident about the security measures of their business partners.

There will be new attacks on Android operating system based devices, but it will not be on massive scale. The fact tablets share the same operating system as smart phones means they will be soon targeted by the same malware as those platforms. The number of malware specimens for Macs would continue to grow, though much less than in the case of PCs. Windows 8 will allow users to develop applications for virtually any device (PCs, tablets and smart phones) running Windows 8, so it will be possible to develop malicious applications like those for Android, hence these are some of the predicted trends in cyber security.

Incidents	Jan-June2012	Jan-June2013	% Increase/(decrease)
Fraud	2439	2490	2
Intrusion	2203	1726	(22)
Spam	291	614	111
Maliciouscode	353	442	25
CyberHarassment	173	233	35
Contentrelated	10	42	320
IntrusionAttempts	55	24	(56)
Denial ofservices	12	10	(17)
Vulnerabilityreports	45	11	(76)
Total	5581	5592	

Table I

The above Comparison of Cyber Security Incidents reported to Cyber999 in Malaysia from January–June 2012 and 2013 clearly exhibits the cyber security threats. As crime is increasing even the security measures are also increasing. According to the survey of U.S.

4. TRENDS CHANGING CYBER SECURITY

Here mentioned below are some of the trends that are having a huge impact on cyber security.

1. Web servers:

The threat of attacks on web applications to extract data or to distribute malicious code persists. Cyber criminals distribute their malicious code via legitimate web servers they've compromised. But data-stealing attacks, many of which get the attention of media, are also a big threat. Now, we need a greater emphasis on protecting web servers and web applications. Web servers are especially the best platform for these cyber criminals to steal the data. Hence one must always use a safer browser especially during important transactions in order not to fall as a prey for these crimes.

2. Cloud computing and its services

These days all small, medium and large companies are slowly adopting cloud services. In other words the world is slowly moving towards the clouds. This latest trend presents a big challenge for cyber security, as traffic can go around traditional points of inspection. Additionally, as the number of applications available in the cloud grows, policy controls for web applications and cloud services will also need to evolve in order to prevent the loss of valuable information. Though cloud services are developing their own models still a lot of issues are being brought up about their security. Cloud may provide immense opportunities but it should always be noted that as the cloud evolves so as its security concerns increase.

3. APT's and targeted attacks

APT (Advanced Persistent Threat) is a whole new level of cyber crime ware. For years network security capabilities such as web filtering or IPS have played a key part in identifying such targeted attacks (mostly after the initial compromise). As attackers grow bolder and employ more vague techniques, network security must integrate with other security services in order to detect attacks. Hence one must improve our security techniques in order to prevent more threats coming in the future.

4. Mobile Networks

Today we are able to connect to anyone in any part of the world. But for these mobile networks security is a very big concern. These days firewalls and other security measures are becoming porous as people are using devices such as tablets, phones, PC's etc all of which again require extra securities apart from those present in the applications used. We must always think about the security issues of these mobile networks. Further mobile networks are highly prone to these cyber crimes a lot of care must be taken in case of their security issues.

5. IPv6: New internet protocol

IPv6 is the new Internet protocol which is replacing IPv4 (the older version), which has been a backbone of our networks in general and the Internet at large. Protecting IPv6 is not just a question of porting IPv4 capabilities. While IPv6 is a wholesale replacement in making more IP addresses available, there are some very fundamental changes to the protocol which need to be considered in security policy. Hence it is always better to switch to IPv6 as soon as possible in order to reduce the risks regarding cyber crime.

6. Encryption of the code

Encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it.. In an encryption scheme, the message or information is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Encryption at a very beginning level protects data privacy and its integrity. But more use of encryption brings more challenges in cyber security. Encryption is also used to protect data in transit, for example data being transferred via networks (e.g. the Internet, e- commerce), mobile telephones, wireless microphones, wireless intercoms etc. Hence by encrypting the code one can know if there is any leakage of information.

Hence the above are some of the trends changing the face of cyber security in the world. The top network threats are mentioned in below Fig -1.

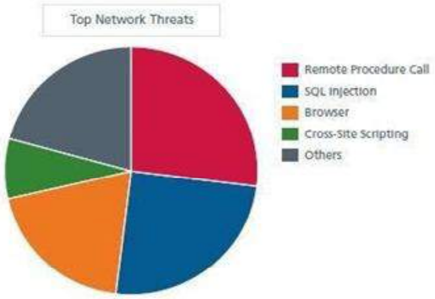


Fig -1

The above pie chart shows about the major threats for networks and cyber security.

5. ROLE OF SOCIAL MEDIA IN CYBER SECURITY

As we become more social in an increasingly connected world, companies must find new ways to protect personal information. Social media plays a huge role in cyber security and will contribute a lot to personal cyber threats. Social media adoption among personnel is skyrocketing and so is the threat of attack. Since social media or social networking sites are almost used by most of them every day it has become a huge platform for the cyber criminals for hacking private information and stealing valuable data.

In a world where we're quick to give up our personal information, companies have to ensure they're just as quick in identifying threats, responding in real time, and avoiding a breach of any kind. Since people are easily attracted by these social media the hackers use them as a bait to get the information and the data they require. Hence people must take appropriate measures especially in dealing with social media in order to prevent the loss of their information.

The ability of individuals to share information with an audience of millions is at the heart of the particular challenge that social media presents to businesses. In addition to giving anyone the power to disseminate commercially sensitive information, social media also gives the same power to spread false information, which can be just being as damaging. The rapid spread of false information through social media is among the emerging risks identified in Global Risks 2013 report.

Though social media can be used for cyber crimes these companies cannot afford to stop using social media as it plays an important role in publicity of a company. Instead, they must have solutions that will notify them of the threat in order to fix it before any real damage is done. However companies should understand this and recognise the importance of analysing the information especially in social conversations and provide appropriate security solutions in order to stay away from risks. One must handle social media by using certain policies and right technologies.

6. CYBER SECURITY TECHNIQUES

1. Access control and password security

The concept of user name and password has been fundamental way of protecting our information. This may be one of the first measures regarding cyber security.

2. Authentication of data

The documents that we receive must always be authenticated be before downloading that is it should be checked if it has originated from a trusted and a reliable source and that they are not altered. Authenticating of these documents is usually done by the anti virus software present in the devices. Thus a good anti virus software is also essential to protect the devices from viruses.

3. Malware scanners

This is software that usually scans all the files and documents present in the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware.

4. Firewalls

A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. All messages entering or leaving the internet pass through the firewall present, which examines each message and blocks those that do not meet the specified security criteria. Hence firewalls play an important role in detecting the malware.

5. Anti-virus software

Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered. An anti virus software is a must and basic necessity for every system.

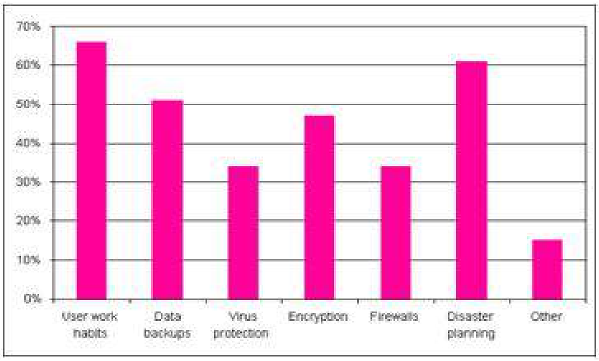


Table II: Techniques on cyber security

7 CYBER ETHICS

Cyber ethics are nothing but the code of the internet. When we practice these cyber ethics there are good chances of us using the internet in a proper and safer way. The below are a few of them:

· DO use the Internet to communicate and interact with other people**.** Email and instant messaging make it easy to stay in touch with friends and family members, communicate with work colleagues, and share ideas and information with people across town or halfway around the world

· Don't be a bully on the Internet. Do not call people names, lie about them, send embarrassing pictures of them, or do anything else to try to hurt them.

· Internet is considered as world's largest library with information on any topic in any subject area, so using this information in a correct and legal way is always essential.

· Do not operate others accounts using their passwords.

· Never try to send any kind of malware to other's systems and make them corrupt.

· Never share your personal information to anyone as there is a good chance of others misusing it and finally you would end up in a trouble.

· When you're online never pretend to the other person, and never try to create fake accounts on someone else as it would land you as well as the other person into trouble.

· Always adhere to copyrighted information and download games or videos only if they are permissible.

The above are a few cyber ethics one must follow while using the internet. We are always thought proper rules from out very early stages the same here we apply in cyber space.

8. CONCLUSION

Computer security is a vast topic that is becoming more important because the world is becoming highly interconnected, with networks being used to carry out critical transactions. Cyber crime continues to diverge down different paths with each New Year that passes and so does the security of the information. The latest and disruptive technologies, along with the new cyber tools and threats that come to light each day, are challenging organizations with not only how they secure their infrastructure, but how they require new platforms and intelligence to do so. There is no perfect solution for cyber crimes but we should try our level best to minimize them in order to have a safe and secure future in cyber space.

REFERENCES

1. A Sophos Article 04.12v1.dNA, eight trends changing network security by James Lyne.

2. Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole

3. Computer Security Practices in Non Profit Organisations – A NetAction Report by Audrie Krause.

4. A Look back on Cyber Security 2012 by Luis corrons – Panda Labs.

5. International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 Page nos.68 – 71 ISSN 2229-5518, "Study of Cloud Computing in HealthCare Industry by G.Nikhita Reddy, G.J.Ugander Reddy

6. IEEE Security and Privacy Magazine – IEEECS Safety Critical Systems – Next Generation July/ Aug 2013.

7. CIO Asia, September 3rd, H1 2013: Cyber security in malasia by Avanthi Kumar.

50

भारत के साइबर कानून और साइबर अपराध पर : एक अध्ययन

प्रा. अहिवले अनिल अर्जुन
हिन्दी विभाग,
श्रीपतराव कदम महाविद्यालय, शिरवल

****

सार –

जैसा कि हम सभी जानते हैं कि यह वह युग है जहाँ अधिकांश चीजों की शुरुआत आमतौर पर इंटरनेट पर की जाती है जैसा कि भारत में हर मिनट एक व्यक्ति अंतरजाल उपयोगकर्ता हैं ऑनलाइन व्यवहार से लेकर ऑनलाइन लेन–देन तक कार्य करता है इंटरनेट (वेब) के बाद विश्व स्तर पर कार्य किया जाता है, सामान्यत: कोई भी इसका उपयोग कर सकता है कहीं से भी इंटरनेट के संसाधन अंतरजाल प्रौद्योगिकी का उपयोग कुछ लोग अच्छे कार्य के लिए और कुछ अपराध के लिए कर रहे हैं। दूसरे के जालतंत्र तक अनधिकृत पहुंच, घोटाले जैसी गतिविधियां आदि। ये आपराधिक गतिविधियां या अपराध/अपराध से संबंधित अंतरजाल को साइबर अपराध कहा जाता है। इन अपराधोंकी रोक लगाने के लिए जो कानून बनाया, अपराधियों को सजा देना इसलिए साइबर कानून निर्माण किया। भारत, साइबर कानून सूचना प्रौद्योगिकी अधिनियम, २००० में निहित हैं। भारत में आज के तारीख तक ४४५४६ सायबर अपराध दर्ज किये गए है इन में कर्नाटक राज्य में सर्वाधिक सायबर अपराध दर्ज किये गए है (१२०२०), उत्तर प्रदेश (११४१६), महाराष्ट्र (४६६७) और सबसे कम सायबर अपराध बिहार में (१०५०) केस पाए गए है हम साइबर कानून को परिभाषित कर सकते हैं क्योंकि यह इसका हिस्सा है कानूनी प्रणालियाँ जो अंतरजाल, साइबरस्पेस और। से संबंधित हैं कानूनी मुद्दों के साथ। यह एक व्यापक क्षेत्र को सम्मिलित करता है, जिसमें शामिल हैं कई उप–विषयों के साथ–साथ अभिव्यक्ति की स्वतंत्रता, तक पहुंच और अंतरजाल का उपयोग, और ऑनलाइन सुरक्षा या ऑनलाइन गोपनीयता। सामान्य तौर पर, इसे वेब के नियम के रूप में संदर्भित किया जाता है।

संगणक के आविष्कार ने इंसान का जीवन आसान बना दिया है, यह शुरू से विभिन्न प्रयोजनों के लिए उपयोग कर रहा है दुनिया भर में बड़े संगठनों के लिए व्यक्ति। में सरल शब्द हम संगणक को मशीन के रूप में परिभाषित कर सकते हैं कि जानकारी संग्रहीत और हेरफेर ध संसाधित कर सकता है या निर्देश जो उपयोगकर्ता द्वारा निर्देशित किया जाता है। अधिकांश संगणक उपयोगकर्ता गलत तरीके से संगणक का उपयोग कर रहे हैं अपने निजी फायदे के लिए या दूसरों के लिए दशकों से लाभ इसने साइबर अपराध को जन्म दिया। इससे गतिविधियों में व्यस्तता आई थी जो हैं समाज के लिए अवैध। हम साइबर अपराध को इस प्रकार परिभाषित कर सकते हैं: संगणक या संगणक जालतंत्र का उपयोग करके किए गए अपराध और आमतौर पर साइबर स्पेस पर होते हैं, विशेष रूप से अंतरजाल अब शब्द आता है साइबर कानून। इतो इसकी कोई निश्चित परिभाषा नहीं है, लेकिन एक साधारण शब्द में हम कर सकते हैं इसे साइबरस्पेस को नियंत्रित करने वाले कानून के रूप में परिभाषित किया। साइबर कानून वो कानून हैं जो साइबर क्षेत्र को नियंत्रित करता हैं। साइबर अपराध, डिजिटल और इलेक्ट्रॉनिक हस्ताक्षर, डेटा सुरक्षा और गोपनीयता आदि साइबर कानून द्वारा समझी जाती हैं।

साइबर अपराध और साइबर कानून

हम साइबर अपराध को किसी भी पुरुष कारक या अन्य के रूप में परिभाषित कर सकते हैं अपराध जहां इलेक्ट्रॉनिक संचार या सूचना सिस्टम, जिसमें कोई डिवाइस या इंटरनेट या दोनों शामिल हैं या उनमें से अधिक शामिल हैं। हम साइबर कानून को कानूनी मुद्दों के रूप में परिभाषित कर सकते हैं: संचार प्रौद्योगिकी के उपयोग से संबंधित, संक्षेप में साइबरस्पेस, यानी इंटरनेट।

यह एक प्रयास है मानव कार्रवाई द्वारा प्रस्तुत चुनौतियों को एकीकृत करने के लिए इन पर लागू कानूनों की विरासती प्रणाली वाला इंटरनेट भौतिक संसार।

साइबर अपराध

सुस्मान और ह्युस्टन ने सबसे पहले साइबर शब्द का प्रस्ताव रखा था अपराध वर्ष १९९५ में। साइबर अपराध का वर्णन नहीं किया जा सकता है एक परिभाषा के रूप में, इसे सबसे अच्छा संग्रह के रूप में माना जाता है कार्य या आचरण करता है। ये कार्य सामग्री पर आधारित हैं अपराध वस्तु जो कंप्यूटर डेटा या सिस्टम को प्रभावित करती है। ये अवैध कार्य हैं जहां एक डिजिटल डिवाइस या सूचना प्रणाली एक उपकरण या लक्ष्य है या यह हो सकता है दोनों का संयोजन। साइबर अपराध के रूप में भी जाना जाता है इलेक्ट्रॉनिक अपराध, कंप्यूटर से संबंधित अपराध, ई—अपराध, उच्च प्रौद्योगिकी अपराध, सूचना आयु अपराध आदि। सरल शब्द में हम साइबर अपराध का वर्णन कर सकते हैं: अपराध या अपराध जो इलेक्ट्रॉनिक पर होते हैं संचार या सूचना प्रणाली। इस प्रकार के अपराध मूल रूप से अवैध गतिविधियां हैं जिनमें कंप्यूटर और एक नेटवर्क शामिल हैं। के कारण इंटरनेट का विकास, की मात्रा साइबर अपराध की गतिविधियां भी बढ़ रही हैं क्योंकि जब अपराध करने की अब आवश्यकता नहीं है अपराधी की शारीरिक उपस्थिति। साइबर अपराध की असामान्य विशेषता यह है कि पीड़ित और अपराधी कभी भी सीधे संपर्क में नहीं आ सकता है। साइबर अपराधी अक्सर देशवाले देशों से काम करने का विकल्प चुनते हैं कम करने के लिए अस्तित्वहीन या कमजोर साइबर अपराध कानून का पता लगाने और अभियोजन की संभावना। लोगों के बीच यह भ्रांति है कि साइबर अपराध कर सकते हैं केवल साइबरस्पेस या इंटरनेट पर प्रतिबद्ध हों। में तथ्य यह है कि साइबर अपराध बिना लोगों के भी किए जा सकते हैं साइबर स्पेस में भागीदारी, यह आवश्यक नहीं है कि साइबर अपराधी ऑनलाइन मौजूद रहें। सॉफ्टवेयर गोपनीयता को एक उदाहरण के रूप में लिया जा सकता है।

साइबर अपराध का वर्गीकरण : साइबर अपराध को चार प्रमुख श्रेणियों में वर्गीकृत किया जा सकता है। वे इस प्रकार हैं:

व्यक्तियों के खिलाफ साइबर अपराध में: ईमेल द्वारा दुर्भावनापूर्ण व्यवहार, धोका धड़ी, साइबर मानहानि, आईआरसीअपराध (इंटरनेट रिले चौट) और फिशिंग का इस्तेमाल होता है।

संपत्ति के खिलाफ साइबर अपराध में: सॉफ्टवेयर पायरेसी, कॉपीराइट उल्लंघन और ट्रेडमार्क उल्लंघन का इस्तेमाल होता है।

संगठन के खिलाफ साइबर अपराध में : डॉस हमला, ईमेल बमबारी और सलामी हमला शामिल हैं

समाज के खिलाफ साइबर अपराध: साइबर अपराध के खिलाफ समाज में शामिल हैं: जालसाजी और वेब जैकिंग

संसद हमले का मामला

पुलिस अनुसंधान और विकास ब्यूरो,हैदराबाद ने इस मामले को संभाला था। एक लैपटॉप बरामद किया गया संसद पर हमला करने वाले आतंकवादी से। लैपटॉप जिसे दो आतंकियों से हिरासत में लिया गया था। १३ दिसंबर २००१ को पाँच आतंकवादियों मार गिराया गया था जब संसद की घेराबंदी, कंप्यूटर पर भेजा गया था बीपीआरडी के फोरेंसिक डिवीजन। लैपटॉप में कई सबूत शामिल थे जो दो आतंकवादियों के इरादों की पुष्टि करते हैं, मुख्य रूप से गृह मंत्रालय का स्टिकर जो उन्होंने बनाया था लैपटॉप पर और उनकी एंबेसडर कार पर चिपका दिया गया। संसद भवन में प्रवेश और फर्जी पहचान पत्र हासिल करें कि दो आतंकवादियों में से एक के साथ ले जा रहा था भारत सरकार का प्रतीक और मुहर। को सावधानीपूर्वक स्कैन किया गया और इसके अतिरिक्त सील भी एक आवासीय के साथ मिलकर बनाई गई थी। जम्मू—कश्मीर का पता हालांकि सावधानी से पता लगाना साबित कर दिया कि यह सब जाली था और लैपटॉप पर बनाया गया था।

भारत में साइबर कानून: आईटी अधिनियम, २००० के तहत निम्नलिखित धाराएं हैं:

I. कंप्यूटर संसाधनों से छेड़छाड़ की कोशिश—धारा ६५

।

II. कंप्यूटर में संग्रहित डाटा के साथ छेड़छाड़ कर उसे हैक करने की कोशिश–धारा ६६।

III. संवाद सेवाओं के माध्यम से प्रतिबंधित सूचनाएं भेजने के लिए दंड का प्रावधान–धारा ६६ ए।

IV. कंप्यूटर या अन्य किसी इलेक्ट्रॉनिक गैजेट से चोरी की गई सूचनाओं को गलत तरीके से हासिल करने के लिए दंड का प्रावधान–धारा ६६ बी।

V. किसी की पहचान चोरी करने के लिए दंड का प्रावधान–धारा ६६ सी।

VI. अपनी पहचान छुपाकर कंप्यूटर की मदद से किसी के व्यक्तिगत डाटा तक पहुंच बनाने के लिए दंड का प्रावधान–धारा ६६ डी।

VII. किसी की निजता भंग करने के लिए दंड का प्रावधान–धारा ६६ इ।

VIII. साइबर आतंकवाद के लिए दंड का प्रावधान–धारा ६६ एफ।

IX. आपत्तिजनक सूचनाओं के प्रकाशन से जुड़े प्रावधान–धारा ६७।

X. इलेक्ट्रॉनिक माध्यमों से सेक्स या अश्लील सूचनाओं को प्रकाशित या प्रसारित करने के लिए दंड का प्रावधान–धारा ६७ ए।

XI. इलेक्ट्रॉनिक माध्यमों से ऐसी आपत्तिजनक सामग्री का प्रकाशन या प्रसारण, जिसमें बच्चों को अश्लील अवस्था में दिखाया गया हो–धारा ६७ बी।

XII. मध्यस्थों द्वारा सूचनाओं को बाधित करने या रोकने के लिए दंड का प्रावधान–धारा ६७ सी।

XIII. सुरक्षित कंप्यूटर तक अनाधिकार पहुंच बनाने से संबंधित प्रावधान–धारा ७०।

XIV. डाटा या आंकड़ों को गलत तरीके से पेश करना–धारा ७१।

XV. आपसी विश्वास और निजता को भंग करने से संबंधित प्रावधान–धारा ७२ ए।

XVI. कॉन्ट्रैक्ट की शर्तों का उल्लंघन कर सूचनाओं को सार्वजनिक करने से संबंधित प्रावधान–धारा ७२ ए।

XVII. फर्जी डिजिटल हस्ताक्षर का प्रकाशन–धारा ७३।
भारतीय दण्ड संहिता (आईपीसी) में साइबर अपराधों से संबंधित प्रावधान

I. ईमेल के माध्यम से धमकी भरे संदेश भेजना–आईपीसी की धारा हो–आईपीसी की धारा ४६६।

II. फर्जी इलेक्ट्रॉनिक रिकॉर्ड्स का इस्तेमाल–आईपीसी की धारा ४६३।

III. फर्जी वेबसाइट्स या साइबर फ्रॉड–आईपीसी की धारा ४२०।

IV. चोरी–छुपे किसी के ईमेल पर नजर रखना–आईपीसी की धारा ४६३।

V. वेब जैकिंग–आईपीसी की धारा ३८३।

VI. ईमेल का गलत इस्तेमाल–आईपीसी की धारा ५००।

VII. दवाओं को ऑनलाइन बेचना–एनडीपीएस एक्ट।

VIII. हथियारों की ऑनलाइन –बिक्री–आर्म्स एक्ट।
नव विकसित का उदय और प्रसार कई साइबर अपराधों को संचालित करने के लिए प्रौद्योगिकियां शुरू होती हैं हाल के वर्ष। साइबर क्राइम हमारे लिए बड़ा खतरा बन गया है। साइबर अपराध के खिलाफ सुरक्षा एक महत्वपूर्ण हिस्सा है किसी देश का सामाजिक, सांस्कृतिक और सुरक्षा पहलू। भारत सरकार ने किससे निपटने के लिए आईटी अधिनियम, २००० अधिनियमित किया है? साइबर अपराध। अधिनियम आगे IPC, १८६०, IEA को संशोधित करता है (इंडियन एविडेंस एक्ट), १८७२, द बैंकर्स बुक्स एविडेंस अधिनियम १८६१ और भारतीय रिजर्व बैंक अधिनियम, १६३४। कोई भी दुनिया का एक हिस्सा साइबर अपराध की उत्पत्ति हो सकती है इंटरनेट पर राष्ट्रीय सीमाएं दोनों बना रही हैं जांच की तकनीकी और कानूनी जटिलताओं और इन अपराधों पर मुकदमा चला रहे हैं। अंतर्राष्ट्रीय सामंजस्य विभिन्न के बीच प्रयास, समन्वय और सहयोग राष्ट्रों को साइबर की दिशा में कार्रवाई करने की आवश्यकता है अपराध। इस पत्र को लिखने का हमारा मुख्य उद्देश्य इसका प्रसार करना है आम लोगों के बीच साइबर अपराध की सामग्री। पर इस पत्र के अंत में साइबर अपराध और साइबर पर एक संक्षिप्त अध्ययन भारत के कानून हम कहना चाहते हैं कि साइबर अपराध कभी नहीं हो सकते स्वीकार किया। अगर कोई साइबर अटैक का शिकार होता है, कृपया आगे आएं और अपने नजदीकी में मामला दर्ज करें पुलिस स्टेशन SDR (विशेष आहरण अधिकार)। अगर अपराधियों को सजा नहीं मिलेगी उनके कर्म, वे कभी नहीं रुकेंगे।

51

Cyber Security in Indian Banking Sector

Dr.Devaki Nilesh Rathod
Assistant Professor in Economics,
Shripatrao Kadam Mahavidyalaya, Shirwal

****

Abstract:-Cyber security plays an important role in the field of information technology. Whenever we think about the cyber security the first thing that come to our mind is cybercrimes which are increasing immensely day by day. Various Government and companies taking many measures in order to prevent these cyber crimes. In india,the RBI red-flagged cybersecurity,issues in its financial stability report in July 2020.The report underscored the challenges due to rising cyber threats with the banking industry being primary target for such attacks. In a recent statement, the national security advisor affirmed that financial frauds increased exponentially due to greater dependence on digital payment platforms following the COVID-19 pandemic. In other news, global hackers made headlines as they attempted more than 40,000 cyber attacks on India's banking Industry. However,cybersecurity incidents are not new to the banking world. The history of the cyber threats foes back to 1971.For decades, bank across the world have been fighting countless borderless battles with faceless criminals in the cyberspace. With the rapid digitization the banking industry(and other industries)cyber threats and attacks have become more pervasive and sophisticated.

This paper mainly focus on importance of cyber security in Banking sector, biggest cyber attacks in India, types of cyber threats. As well as remedial measure of cyber attacks.

Introduction:-The onset of COVID-19 resulted in digitalization in the banking sector. Both front –end and back –end operations have now become digital. With all this growing technology, cyber-attacks persistently increase, and attackers are actively looking for their victims for the malicious cyber-attacks on sensitive data of banking and financial systems.

This new digital workforce has pushed most of the banking sectors to go online, including video conferencing that has led to privacy issues and phishing attempts, including ransomware attacks.

Since banking sectors are depending on online banking, both mobile and web services tend to have a weak security threats are becoming more prominent.Mostly,cyber criminals prefer to target the banking sector to get customer and employee information details and use them to steal bank data and money. Before moving on to cyber Security threats in the Indian Baking Sector.

Keyword:-Cyber security, cyber threats, phishing, ransomware, disaster.

Objective of the Study:-

1) To study the importance of cyber security in Banking sector.

1) To study identify the biggest cyber attacks in India

2) To study types of cyber threats.

3) To study about remedial measure of cyber attacks.

Research Methodology:-This is a conceptual Paper & study focuses on extensive study of secondary data collected from various e books ,national & International Journals and Publications from various websites, which focused on various aspects of cyber security in Indian Banking Sector.

Importance of Cyber Security in Banking Sector

Here are five reasons why cyber security is important in the banking sector:

1. Digital India has led to an increase in the usage of cashless transaction,digital money, In this context, taking all the security measures is important to protect the data and Privacy.

2. Data breaches are a serious problems in the banking sector. A weak cyber security system can cause their customer base to undergo cyber security threats.

3. When a banks data is breached, recovering from this data breach can be time-consuming and stressful. So enhancing the banking security system is a must.

4. Suppose you lost your card, given a complaint against and cards are cancelled, yet your data is sensitive and could reveal a lot of information that could be used against you and do great harm.

5. Banks need to be their guard 24/7;if not, your data with the bank can be breached.

The Biggest Cyber Attacks in India:-

Various business sectors and geographical locations are the targeted customers for the cybercriminals to perform their cyber attacks techniques. Some of the recent cyber security threats are as follows:

1.Cosmos Banks Cyber Attack in Pune:-

A recent cyber attack in India 2018 took place in Cosmos bank when hackers siphoned off Rs.94.42 crores.Below is the list of cyber attacks.

*How did they do it? Hackers hacked into the banks ATM server and took all the card details and wiped off money from 28 countries and immediately withdrew the amount as soon as they were informed.

*Prevention:-Hardening of the security system can help authorized people can be the way forward.

2.**ATM System Hacked**:-Canara Bank ATM servers were targeted in around mid-2018.According to sources, more than 300 users ATM details were hacked by attackers and wiped off 20 lakh rupees from various bank accounts.

*How did they do it? Hackers used skimming devices to steal information and stolen amounts of up to 20 lakh rupees.

*Prevention:-Enhancement of the security features in ATMs can prevent any misuse of data.

3.UIDAI Adhar Software Hacked:-

*1.1 billion Indian Adhar card details were leaked and this is one of the massive data breaches that happened in 2018.UIDAI released the official notification about this data breach and mentioned that around 210 Indian Government websites were hacked.

*Aadhar software Hacked: This data breach included Aadhar,PAN,bank account ,IFSC codes, and other personal information of the users and anonymous seller were selling Aadhar information for Rs.500 over Whatsapp.Also,one could get an Aadhar card printout for just Rs.300.

4.SIM Swap Scam:-

Two hackers from Navi Mumbai fraudulently gained SIM card information and illegally transferred money from the bank accounts of rupees 4 crore in August 2018.They carried out transaction vial online banking. Aforesaid stats and events of the latest cyber attacks in India are the wake up call for all financial sectors that are still vulnerable to cyber threats. Organizations need to implement cyber security measures and follow the below-mentioned security guidelines.

*Preventions:-Not sharing your personal information with unknown domains can help in minimizing the risk of having your personal information reaching people with malicious content.

Types of Cyber threats:

1.Large scale anti-fraud bypass: With the increase in the online transition, criminals are looking for ways to defeat anti-fraud safeguard. They try to replicate real fingerprints with existing ones stolen from someone else's PC.

2.ATM malware:- This is an interesting piece of malware, detected in financial institutions in India and is programmed to cash out ATMS.

3.Account-centric frauds: This is one of the common types of fraud, these frauds mainly concentrate on stealing and hacking sensitive details such as account ,Password,OTP etc.

4.Phishing:-Phishing is method to trick the victim into opening malicious links,leading to an installation of malware which then freezes the system. Phishing is often used to steal user data, including login credentials,etc.

5.Identity theft:-When a data breach occurs, the data of the customers are sold by cybercriminals to use in order to get credit information without his or their consent to borrow money and conduct purchase violations.

6.Threat from employees: Unhappy or dissatisfied employees contribute to the large scale of the risk, by breaching the companies policies and causing security threats to the organizations.

7.Ransomware:-These ransom ware attack will mainly hit small banks as they lack IT resources, outdated security tech,and protocols on cyber security. To protect from this ransomware,bank must adopt protection layers throughout their network which help in acting as an obstacle to block malicious software attacks.

Cyber related Challenges:-

Banks foremost agenda in board rooms has been the digitization of voluminous confidential data and banking process(not limited to payment s).This urgency has put the spotlight on digital technologies, such as cloud, Artificial Intelligence (AI)Analytical Internet of things (IOT)and machine learning(ML)with technology transformation, confidential information will be saved in remote servers and ubiquitous. Higher digitization and remote operations will lead to increased vulnerabilities and open up opportunities for cybercriminals. exposing banks to breaches or hacking. Banks need to be mindful of the following challenges while dealing with cyber threat:-

*Sophistication of Cybercrimes

*Data sharing mechanism

*Limitations associated with legacy systems

*Securing third-party services(vendors and alliance partners)

*High exposure to compromised network and devices

*Lack of skilled cyber security Professionals

*Governance and regulatory compliances.

Remedial Measures to reduce Cyber Security Threats in the Banking Sector :-

1.Assess Cloud Security:-Review your cloud infrastructure often to ensure its up to date. Assess your cloud securities current state, best practices, and compliance standards. To secure cloud platform and infrastructure one can use multifactor authentication.

2.Monitor Cloud Security:-To automate the threat detection and protect against potential threats ne can use a vulnerability management tool before they become a problem.

3.Establish Strict Access Management Policies:-Restrict your access to employees who really need this information, instead of giving access to part-time workers, contractors,etc.By providing permissions to employees who require it, you are establishing strict access management policies to protect your organization from within.

4.**Increasing Awareness** A**mong Employees**:-Bank need to adopts comprehensive training module to prepare their staff to handle cyber attacks.

5.Disaster Recovery Plan:-Having an alternate plan to protect the data, help you to minimize downtime after a disruption and avoid data loss. This can be applied only if you backup your data regularly.

6.Encrypt Your Data:-Cryptography is one of the methods to encrypt your data and ensure your most sensitive digital assets are always protected.

7.Cybersecurity training:-Cyber security training is a must for cyber security professionals to enhance their skills in relevant information and tests of their cyber-awareness by covering all aspects of data security and keeping them Up-to-date.

Conclusion:-While RBI and the Government are taking proactive steps to battle cyber-attacks, they are also evolving with newer technology trends like crytocurrencies and blockchain.This gradually increases the need for cyber security as a part of the design architecture intending to detect the stemming attacks in real time, rather than repairing the damage. Indian banks have seen steady rise in cyber threats, as they have been exploring or embracing complex technologies(such as mobile and internet banking),improving employee intranet, and more recently adopting by rid cloud technology. As a result, they have been selective in adopting digitization in the past &before the COVID-19 crisis, a majority of Indian banks focused on strategic digitization of their customer services.

References:-

1) https://www.mygreatlearning.com/blog/biggest-cyber-security-threats-indian-banking-sector

2) Cybesecurity in the Indian banking industry:Part-1,will 2020 redefine the Cyber security ecosystem?Nov.2020,https://www2.deloitte.com

3) Ashwin Manikandan, "Moody's warns banks of increased cyber risks" The Economic Times, July 08, 2020, https://economictimes.

4) Indiatimes.com/industry/banking/finance/banking/moodys-warns-banks-of-increased-cyber-risks/articleshow/76856381.

5) Reserve Bank of India, RBI releases the financial stability report, July 2020, July 24, 2020, https://www.rbi.org.in/Scripts/BS_Press ReleaseDisplay

❑❑❑