PalArch's Journal of Archaeology of Egypt / Egyptology

IMPACT OF CYBER-ATTACKS ON BANKING INSTITUTIONS IN INDIA: A STUDY OF SAFETY MECHANISMS AND PREVENTIVE MEASURES

Suman Acharya[1], *Sujata Joshi*[2]

[1,2] Symbiosis Institute of Digital and Telecom Management, Symbiosis International (Deemed University), Pune, India.

Email: [2]sjoshi@sidtm.edu.in

Suman Acharya, Sujata Joshi: 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 17(6). ISSN 1567-214x

Keywords: Cybercrime, Denial of Service, Phishing, and cyber security protocol.

ABSTRACT

This research paper aims at studying the catastrophic impact of cybercrime on banking institutions, cyber security measures attempted to curb its effect and development of a robust cyber security mechanism. In recent years banks are its direct victim. In India, a number of banks generally fall prey to the massive malware attacks; it not only leaks valuable and sensitive information but also causes heavy financial losses.

The objective of this study is to identify the business areas which are more susceptible to cyber-attacks and to ensure customization and development of cyber security protocol.

The study involves secondary data analysis from various web resources such as government websites, articles, and research papers available; it also includes case study analysis of different cyber threats and crimes that caused huge financial loss in the past.

This paper will provide insights on cyber regime which will benefit banks, financial institutions, and society at large

1. Introduction

Banking and financial sector Institution (BFSI) is huge sector with large number of customers spread across the globe. The accessibility of banking services to the weaker sections/vulnerable groups of the society has been

increasing over the years. Nearly 1.2 billon adults having accounts in banks since 2011 as per Global Findex database 2017 [1]. A study said most of the Indians switching to digital approach with 51% of them preferring online banking channels where in 26% of them access services via their bank websites and use mobile banking services. With the exceptional growth of digitization in banks, cyber risks have emerged as a major area of concern. Banking sector only accounts for 22% of the cyber-attacks that took place in India, as per the statement of Gulshan Rai [2].

There has been humongous increase of cyber intrusions and attacks over the last decade. This unprecedented growth in crime has not only caused serious damage to the critical banking processes but has also caused huge financial loss to the system.

Globally USD 114 Billion is lost nearly every year due to cybercrimes and the cost to spend in combating the crimes is amount to USD 274 billion [3]. Evolution of cyber threats happened in India majorly in 1998 post privatization of banking industry with virus attacks, followed by hacking websites, sending malicious codes, advanced worm and Trojan, identity theft (Phishing), Denial of Service (DOS) and Distributed Denial of Service (DDOS) in subsequent years and now a days with cyber espionage and cyber warfare. Some of the past cyber-attacks on Indian banking industries such as July 2016 phishing email attack on union bank of India swindling of $171 million, May 2017 Ransom ware attack causing several thousands of computers getting locked down etc. India had 42 million cyber-crime victims, 52% of whom suffered financial or some other kind of loss due to hacking, scams, frauds and thefts [4].

Major Cyber security challenges are inherent vulnerabilities in the system and software used by banks, innumerable entry points to internet, and outdated defense technologies that are highly vulnerable to advanced attack technologies used by hackers. However, mandatory cyber security preparedness is the most basic objective of banking institutions. Conscious of rising threats of the cyber infrastructure in its regulated entities, a good number of regulatory mechanisms and cyber security technologies have been evolved during these years. Therefore, recognizing the increased frequency and complexity of cyber security incidences, there is a need to conduct an ongoing review of cyber security landscape and emerging threats. Bankers' progress in strengthening cyber security resilience and response is to be monitored.

Objective of the Study:

Hence the objective of this paper is to review the threats inherent in the existing and emerging technologies, studying adoption of mechanisms to

- Conduct an ongoing review of the cyber security landscape and emerging threats.
- Analyze impact of cybercrimes on banking sector
- Intends to study the emerging technologies to meet the challenges due cyber threats.

- Suggest adoption of various security protocols/standard interfacing with stake holders and suggesting appropriate policy intervention.

2. Literature Review

The emergence of a new era in banking technology that eliminated the need of physical presence at the bank for many transactions and other banking services by accessing electronic devices has led to the spike cyber-crimes. There has been a major and exceptional contribution by e-banking for this upsurge because of the increased dependency of the consumers over the internet for simplest monetary transactions to large financial affairs. As per a survey, conducted the losses due to fraud in e banking hiked in the year 2014 by 48% as compared to 2013 [5]. The proliferation of the cyber world with the ever-growing demands of customers for convenience access from multiple devices for transaction purpose in India, play an inevitable role in attracting cyber offenders who target online banking malware. A study conducted in the year 2014 says India holds third rank after countries like Japan and the US in the list of countries most affected by online banking malware [5].

According to reports, out of the total cyber fraud occurrences worldwide, 7% of it is carried out in India[4] .Indian banks have been witnessing persistent attacks from possible state and non-state actors, organized criminals and hacktivists. The case of cyber-attack on Canara Bank in the year 2016 explains this better , where bank's e payments were attempted to be blocked by vandalizing its site through the insertion of malicious software by a hacker from Pakistan [6]. Union Bank of India also fell prey to an attack in July 2017, where close to USD 170 million was looted from its Nostro account. According to reports the offenders gained entry by using spear phishing. In a survey conducted by KPMG in 2017 on cybercrime, it has been pre-supposed that initially banks were not well equipped with adequate cyber security mechanism, because of which they were succumbed to rampant cyber threats. Cyber-crimes cases increased from 89% to 94% and the financial losses due to it had also increased from 45% to 63 % [4]. It also revealed that around 70% believed that their institution was ill equipped to fight cyber fraud[4] .

According to a report by Deloitte in 2015 on cyber-crime: 93 percent respondents suggested that there has been an increase in fraud cases in banking industry in the last two years and less than 25 percent of the fraud losses were capable of being recovered because the time lag between cyber-attacks and detection of the threat and attackers is very large. Despite warnings from fraud cases around the globe, large percentage of banks in India did not put adequate emphasis on Fraud and Risk Management solutions. Unfortunately, only 20% of all banks thought of Fraud Risk Management an effective method of fraud control and a large number of these banks only realized after those banks somehow became victims of cyber-attacks [4] .The catastrophic impact of cybercrime on the performance of banking institute and stringent effort undertaken to protect the banking industry from the clutches of cyber-attacks and growing competition among banks, have drawn the attention of researcher, policy makers and cyber experts to identify and analyze the cyber-crime zones, intentions of cyber criminals and vulnerable points susceptible to cyber-attack.

The intention of the study mostly centers on developing a robust world class cyber security mechanism to prevent loss and facilitate growth and production.
Although, a lot of studies have been carried out on cyber-crime on banking platforms still, there is a lot of debate and confusion. Some argue that excessive digitization has led to the emergence of cyber-crime platform and prescribe for a defensive safety protocol. Others encouraging digitization as a modern technology emphasizes on having an aggressive world class uniform cyber security protocol to meet the need of digitization. Due to lack of consensus a vast literature has been generated in this field. But substantial progress has not been achieved either in eliminating/curbing cyber-crimes in financial institutions, particularly Banks. Rather research gaps and gaps in study of crucial issues are widening.
In this context, this study is an initiative to supplement the existing literature and fill the research gap by investigating into critical loopholes, mostly omitted by the bankers in their banking process and investigating into developing a common platform to throw a frontal attack on cyber-crimes and attitudinal poverty attached to it.

3. Research Method

To carry out this study existing information/ data available through the various sources are collected and analyzed on a comparative basis for arriving at logical findings/answer to the research question. The sources are mostly the white papers, government documents, published academic papers, journals, print media and findings of RBI, NCRB, NITI Aayog and CERT-IN, statistical data bank plus historical records.
In this case, secondary method of collection and analysis of data is followed because a good collection of data already exists in a documented form. Conducting direct study may not be a feasible initiative keeping in mind the subject matter and the time factor. Here a historical perspective is taken in finding out accounts of earlier cyber-crime scenario and listing of preventive measure to provide an anti-cybercrime platform. Further steps have been taken to analyze the impact of cyber-attacks through case study approach. The scope of the research is to study impact of cyber-attacks on Indian banking system only thereby narrowing focus to bank fraud cases in India with the objective to standardize the points in banking process more prone to attack and identifying the types of cyber-attacks that the banks are likely to encounter every day.

4. Evolution Of Cyber Threats

Evolution of cyber-attacks started with a simple computer virus during the1980s.Virusis called set of self-replicating computer programs modifying other computer programs and inserting its own code to infect the system. In the late 1990s, hacking websites evolved as a threat to system with some applied research. During 2004, malicious code as an attack resurfaced which was an application security that could not be controlled with conventional antivirus alone. These codes are a wide category of system security terms that consists of attack scripts, viruses, Trojan horses, worms, and malicious content. Then with the rapid advancement of attacks resurfaced advanced Trojans and worms in

late 2008 and attacks such as identity thefts and phishing during 2012. Then in the late 2015, attackers evolved with significant threats such as DOS and DDOS attacks and then later towards 2015 until today cyber espionage and cyber warfare are widely used as a type of attack. DDOS attacks are more pervasive and dangerous than DOS attack because of the use of multiple internet connections, victim cannot identify the origin of attack [7].

4.1. Types of Cyber Attacks*:*

From the large array of data collected from various available resources and analysis made from those collected data, it is understood that Indian Banking Systems is mostly affected by these certain types of cybercrimes. According to data breach investigation report – Verizon 2017, several banking organizations have been surveyed and it was found that more than 50% of the organizations apparently affected by following major five cyber threats such as denial of service (DOS), phishing, malware, spear phishing and ransom ware. Out of most incidents reported, top 3 patterns of cyber-attacks such as denial of service(DOS), web application attacks and payment card skimming consist of more than 88% of all the security incidents [7].

4.1.1. 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.

4.1.2. 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.

4.1.3. 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 [8].

4.1.4. Vishing: It is the application of social engineering through telephone to gain access on private personal data from public for the purpose of ransom.

4.1.5. 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.

4.1.6. Insider threat:

It is a malicious threat that comes from inside of any organization from people, employees themselves which exposes the system to attackers.

4.1.7. 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].

4.1.8. ATM/Debit/Credit card frauds:

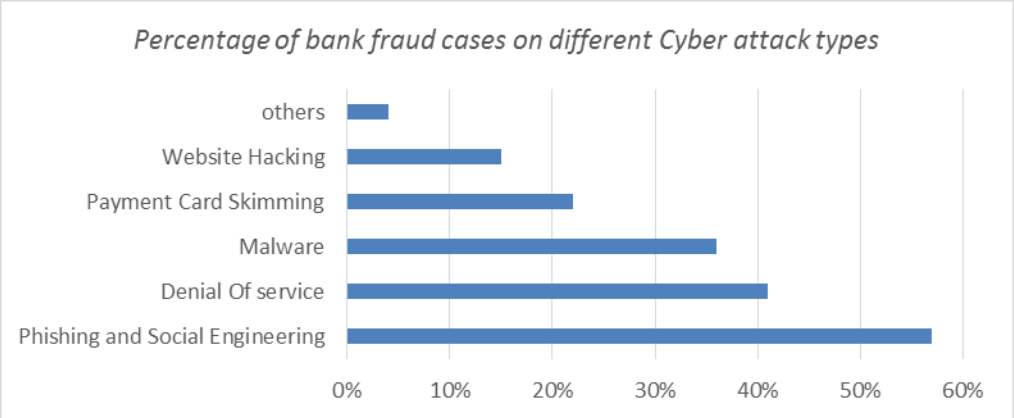
In these kinds of frauds, the fraudster uses a skimming machine typically affixed with the keypad of ATM machine or POS machine such that it does not appear to naked eye. Whenever customer enters his card details along with PIN, details goes to the installed skimmer using which money can be theft.

4.1.9. 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.

4.1.10. 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.



(**Fig 1** – Percentage of Bank Fraud Cases on Different Cyber Attack Types: As per NITI-Aayog Cyber-Security report 2017)

5. Statistics And Analysis

So, the question is why banks are so vulnerable to cyber-attacks? Major cause of attacks seems to be money which causes attackers blind to do anything. Besides that, the market size of Indian banking system is huge and growing day

to day. With the proliferation of digital banking system and financial inclusion schemes in India, huge numbers of online as well as offline users are now transacting through various modes of such as net banking, mobile banking, and mobile wallets credit/debit cards etc. As per RBI data, bank deposit grew are at CAGR 11.11% during FY09-17 and accumulated to $1.86 trillion USD by FY19. Deposits stood at $1893.77 billion as of Feb 2020 [9]. Below graph (Table 1) shows statistical data of no of transactions and value of transactions through various modes as of May 2020[9]. Because of widespread businesses, huge volume of financial transactions, bulk amount of data and information regarding a huge client base, and lack of strong, multi-layered security system, banks are highly vulnerable to attacks. Major impact of cyber-crime to banks are financial and data losses that constitute 88% of the impacts as per studies. The motives of cyber-attacks are not always to cause theft or loss of money rather sometimes attackers attack to steal financial and personal data in order to gain insights about various types of business and clients' data [8]. This espionage can have severe impact to banks causing reputational risk and loss of huge amount of customer base because of fear of data security.

Table 1: Transactions and value of transactions through various modes as of May 2020: (Source: RBI Bulletin 2020 All values in lakhs)

Mode	No of transactions (in lakhs)	Amount (in Lakhs)
NEFT	1929.4	148174950
RTGS	9003796	704186936
Credit card	77492598	2101749
Debit Card	507963710	15853983
Mobile wallet	3958.3	1585800

In past there are many cyber-attacks on Indian banking system attempting to theft and/or causing loss of money and hence imposing huge financial, reputational, Operational impact and loss of money, client base and personal data. As per RBI data, number of cases related to ATM/Credit/Debit cards and online banking frauds were 13,083 and 11,997during 2014-15 and 2015-16 respectively [9]. Apart from that 44,697 and 49,455 cyber security cases related to phishing, malicious codes, denial of service, website hacking etc. have been reported in the year 2015 and 2016 respectively as per the information tracked by CERT-in (Buletin, 2020). There is an increase in the number of such cases now a days compared to those time in India. Some of the precious cyber- attack cases to Indian banking system have caused huge financial loss and put the bank into too many risks from existing customer. Among them phishing attack on Union Bank Of India in 2017 attempt to theft of $170m , malware attack on switching system of cosmos bank Pune in August 2018 theft of 94 crore

rupees, phishing attack on UTI bank on 14 February2007, SIM Card swap fraud cases causing loss of 4 crores and large number of customers, ATM System hacking in Kolkata with loss of 20 lakhs rupees and other website hacking cases, Rourkela police busted a racket including an online misrepresentation worth Rs 12.5 lakh are few largest cyber-attacks in Indian history [10].

This paper contains case study data of two out of the above noted cyber-attacks in order to analyze the loopholes in the system and shares findings to adopt the best preventive measures to protect the system from such types of attacks in future.

5.1 Case of cyber-attack on UBI 2017:

The cyber-attack on UBI 2017 is a classic case of phishing which triggered from an e-mail that was circulated in disguise from the most trustworthy organization RBI. The e-mail carrying malicious codes was circulated to few email ids of customer cares, individuals, and e-banking persons. Out of all, few people reported the email to security team of the bank. They thought, although the e-mail was sent from RBI, it had a .xer file zipped inside instead of pdf or xls which might have created doubts about the content. But unfortunately, there were few not-so-tech-savvy people who opened the e-mail and soon after the malicious code entered inside banks network and servers which made way for hackers to cause a theft attempt of $ 170 m. But the attackers made a small mistake of deleting the transactions from SWIFT files which were caught by treasury department in the backend while doing reconciliation of their Nostro account [11].

So, what went wrong here? Even though bank's infrastructure had all the basic preventive measures, but attackers identified the vulnerability and created a foothold by gaining access of the system. Main motive of this attack was to gain financial information and theft of money. So, lack of awareness about cyber-crime, lack of proper training to the officials to identify cyber-attack at the initial stage and to prevent any such loss is the main reason that needs to be taken care of.

5.2 Malicious attack on cosmos bank of Pune

Next case study is malicious attack on cosmos bank of Pune on August 11 and 13, 2018, which is one of the best examples of malware attack. In this case, banks internal and ATM infrastructure were compromised. The crime involved multiple malicious central code attacks to the banks switching system between central and core banking system. Basically, the code generated false payment transfer request in response to transaction requests by the customers. After making false adjustments to targeted customers account balances, sending false standing -in, an activity that authorized ATM withdrawal of large amount of money using 450 cloned non-EVM debit cards from various countries. Attackers compromised with the bank's ATM/POS switching system by sending malicious codes into the system which in turn did not allow verification of any transactions requested by users at POS/ATM machine.

When there is a transaction of withdraw happens, a transaction request (TRQ) is sent to banks core banking system to verify and validate the user account and upon successful validation a transaction reply message is sent confirming the same to the same customer. So in this case, the malicious code used to send fake transaction reply message to every transaction requests at ATM/POS [12]. So, attackers successfully tampered the switching system of bank such that any transaction requests were not reaching out to banks core banking system for validation of amount and in this way. This attack on cosmos bank did help siphoned off 84 crores of rupees with 2 waves of huge transaction's in a more advanced and well-planned manner breaking layers of defense in banking system. After further studies, it had been found that the cybercriminals had made much research on the Cosmos bank's banking infrastructure and background surveillance system. The banks officers may have ignored all alerts produced by the system for unknown reasons. Periodic auditing of bank generated reports should not have been ignored as well [13].

5.3 A Comparison of no of cyber cases between nationalized banks and private sector banks between periods 2017-18 and 2018-19.

Apart from the above two case studies, this research paper also compared no of cyber cases between nationalized banks and private sector banks between periods 2017-18 and 2018-19 [9].Scope of the below research is only between Indian banks again. As per the below data (Table 2)it is inferred that percentage increase in fraud cases in private sector banks is lesser than that of public sector banks and the amount involved in frauds has increased more rapidly in public sector banks in comparison to private counterparts. There could be multiple reasons behinds this large disparity here. There is much more amount of budget in private sector banks dedicated to cyber security in which setting up multilayer high secured environments, protection of data and information, up gradation of old environments with latest version software's and hard ware's and setting up appropriate security frame work that constantly reviews and advises bank environment does audit on a fixed interval and provides trainings on security solutions.

Table 2- Frauds in Private Sector and Public Sector Banks: Source: RBI Bulletin 2019

	YR: 2017-2018		YR: 2018-2019	
Bank Institution	**Number of Frauds**	**Amount involved(millions)**	**Number of Frauds**	**Amount involved(millions)**
1	2	3	4	5
Public Sector Banks	2,885 (48.8)	382,608.7 (92.9)	3,766 (55.4)	645,094.5 (90.2)
Private Sector Banks	1,975 (33.4)	24,782.5 (6.0)	2,090 (30.7)	55,151.4 (7.7)

6. Results And Findings

- Major crimes in Indian banking sector is because of phishing, identity theft, malware.
- Even a big crime can happen from small mistakes and lack of awareness on cyber security policies. Any suspicious things should be carefully handled and concerned authorities should be informed first before acting.

- Systems should be audited on fixed interval basis to test of any security breach.
- Public sector banks should be more focused on enhancing security through Public private partnership; allocate more budgets on data protection and security framework enhancement.
- ATM/POS machines switching system connectivity with core banking system should be continuously monitored along with ATM/POS machine transaction monitoring. A constant network packet as acknowledgement signal should be sent and received between to validate connectivity.

7. Safety Mechanism

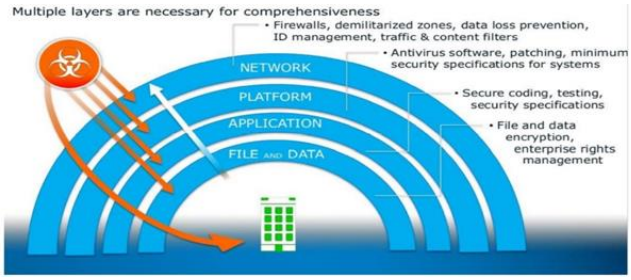
With the growing age of technology, modes of cyber-attacks are changing. Attackers have become more adept in analyzing and gathering vulnerabilities and finding loopholes in the system, to successfully gain privilege and disrupt the network. In order to make themselves well aware and advanced with latest hacking modus operandi, banks are now adopting latest cyber-security technologies and are ready to invest more amount of budget to protect their environment from unauthorized access and unnecessary data and security breaches. Proper setting and maintenance of firewall can prevent the banking space from unwanted attacks.[14]

There are different types of safety measures that banks should take to prevent any such known cyber-attacks. In order to test security of the network and infrastructure of banks, there is a test called penetration test is carried out in bank premises to find out vulnerabilities in the system and identify breaches in which the tester acts as an intruder and tries to breach the security system[15].Number of such tests have been carried out in past and as per the data collected from those tests, it was found that maximum percentage of vulnerabilities found in Indian banks are vulnerabilities in web application, insufficient network security, inefficient password management, improper server configuration and lack of awareness [14].

To prevent cyber-attacks to backend web applications of banks, certain measures such as use of secret socket layer (SSL) protocol is mandatory. Whenever there is a request by any browser to access a sites data, it first fetches the SSL certificate and checks whether the certificate is expired, whether it is issued by browsers certified authorities and whether the certificate is being used by the website for which it is issued, and if all conditions okay then it allows the browser to access it.

Inefficiency in password management can make attackers jobs easier to get inside the network and server layer. Passwords must be kept strong, changed at a fixed interval of time, managed, and stored in proper locked and encrypted way. Password encryption at every layer of security is a must. Passwords should not be exposed anywhere in the entire system and well encrypted. Encryption and decryption methodology should be followed to access any password. Passwords can be encrypted in a configuration file wherever hardcoded and then this file can be used everywhere in the code to access password. Simultaneously the decrypt key file is used to store the key to the encrypted password using logic to unlock the password. This set up can be

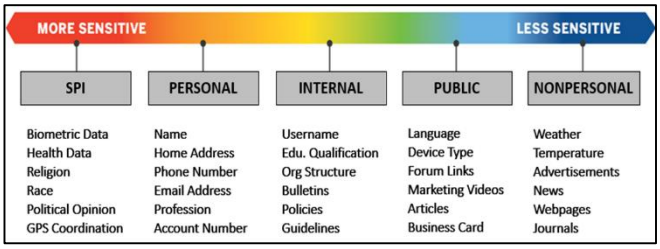
easily done to better prevent source code getting tampered. Two factor or multi factor authentications is a better way to handle login related issues. [16]



(Fig 2- Multiple layered protection framework. NITI Aayog cyber security report 2017**)**

Networks must be guarded by firewall setting. Multiple layered protection frameworks should be proposed to safeguard system core as shown in the diagram above. Top network layer must have firewalls and traffic content filters that prevents unauthorized and undefined data to flow inside. Platform layer below that should be guided with antivirus software's. Operating system and other software should be patched and upgraded on regular interval and old software and hardware to be replaced with latest versions with better security patches. Application layer has so many lines of source codes that are the backbones of back office IT. Necessary prevention framework must be applied to protect the source codes. Password encryption and reduction in code related vulnerabilities must be done by developers to protect their codes. Files and data also need to be encrypted and protected in a secured way for audit purposes.

A survey was carried out on few of the Indian banks regarding the safety prevention measures they used to protect their environment. It was found that most of the banks have implemented password encryption, and other prevention measures mentioned above but there is minimum user awareness programs found where few groups of people were surveyed with set of questions related cyber security but the result was only 5-10 % of people were aware about policies and security awareness with most of others have little or no knowledge [17]. There were few banks found to invest appropriate amount of budget on data protection and information security awareness programs. Everyone in an organization is responsible to maintain data confidentiality. A detailed classification of sensitive data is given in below figure.3 each person should have ample training and awareness to protect highly sensitive data breach otherwise small human error will put the bank at risk.



(Fig 3: Source: NIIT Technology website – Data sensitivity matrix)

Apart from all above, banks should focus on educating employees with self-awareness programs, providing trainings on data protection laws, and empowering them with knowledge on cyber security which will make them always alert to any kind of outer penetration. Extra care should be taken by online banking users while doing online transactions in day to day life. As per data collected from reports, it is found that more than 60% of the customers are unaware of the underlying information security threats involved in banking processes/transactions. Also, around 55% of users are not adept to take extra care while dealing with online banking services [17] . Below highlighted are few standard preventive measures as part of user awareness program to be followed by all bank employees.

- Use of strong and unique password for network share login accounts. Deletion of unused shares.
- Use of Virtual Private Network (VPN) for all remote work instead of exposing remote desktop (RDP).
- Shared software should not be kept in exe form in working folders. Download from safe repository when needed only after IT Security approval.
- Monitoring RDP access and disable the same when not used.
- Always updating the browser and keeping the add pop-ups blocked.
- Timely verification of the genuineness of the accessed browsing site. And immediate reporting to IT security of bank in case of any suspicion.
- Always bookmark important websites to avoid connecting to phishing sites.
- Prohibition of sharing of personal details in any unknown websites.
- Strengthening e-mail security to detect harmful attachments.
- Enabling multifactor authentication for legitimate access.
- Scanning each email directed to the bank. Avoid opening emails from unknown users and report such mails to phishing department of the bank.
- Ensuring that security software and OS are patched on fixed interval.
- Webcam should be covered when not in use.
- Regular back up of data on secured location.
- Sensitive information should not be shared on any platform that has not been approved or secured by IT Security.

8. Practical Implications

Apart from financial losses, banks must address the issue of reputational loss that stride ahead due to emergence of cyber-crime and attack online banking. Policy measures should be formulated training schedules should be designed;

customized banking transaction process should be introduced and so many other steps are should be taken by the banks to prevent occurrence of such attacks. This study highlights on the susceptible zones of banking process more prone to cyber-attack. It indicates towards the time probability of such attack, reasons for such attack and possibly the most effective measures in fighting cybercrime, it has become the master-key in the hands of the management /policy makers to foresee the future course of action to be taken in respect of system building, policy making, technology selection, expansion of banking business and so on. Such a study is also significant to the extent that it is inclined towards abandoning orthodox/ineffective banking framework and in emboldening the banking sector.

By this study one is easily escorted directly to the loopholes in the policy rules and regulations that need to be modified efficiently.

A research implication is the logical connection between a condition and its outcome. Through this study a detail analysis of cybercrime prone zone, nature of cyber-crimes committed, the degree of promptness in handling such incidence of crime and the pace of implementation cyber security measures, one can easily construe that besides technological and technical factors involved in this issue, there is a psychological snag in dealing with cybercrime.

9. Conclusion And Future Scope

Cybercrimes know no barriers and evolve at a pace at par with emerging technologies. The unprecedented growth of cybercrime and its disastrous consequences is a very potent threat to banking and financial institution. It aims at building a vibrant security preparedness among financial institutions, including banks. The unprecedented dependence on e banking technologies at multifarious levels by billions pose a great challenge before cyber experts in formulating a dependable cyber security protocol.

Fighting against the cyber insecurities, the banks in India also require fighting their attitudinal mindset and being in psychological preparedness to deal with cybercrimes and criminals on war footing. Orthodox process followed all along should be abandoned and modern technologies with agile and radical system of fighting needs be adopted. There is also a need to conduct review of cyber security landscape and emerging threats.

Indian banks are the financial back bone of the country and instrument in the hands of individual and institution. Healthy banking institution / trust worthiness of bank should not be compromised at any cost. Now time has come for banks to come out of their traditional banking framework and work in a team spirit with new technology and new vision in order to wipe out or minimise the cyber threat in the system.

References

L. Klapper, D. Singer, S. Ansar, and J. Hess, “Asli Demirgüç-Kunt The Global Findex Database Measuring Financial Inclusion and the Fintech Revolution 2017.” 2017, [Online]. Available: http://hdl.handle.net/10986/29510.

B. Standard, “Banks most vulnerable to cyber threats_ Govt official _ Business Standard News.” Business Standard Ltd, Mumbai, pp. 2–10, 2019, [Online]. Available: https://www.business-standard.com/article/current-affairs/banks-most-vulnerable-to-cyber-threats-govt-official-119022000646_1.html.

A. R. Raghavana and L. Parthiban, “The effect of cybercrime on a Bank’s finances,” Int. J. Curr. Res. Acad. Rev., vol. 2, no. 2, pp. 173–178, 2014, [Online]. Available: http://www.ijcrar.com/vol-2-2/A.R. Raghavan and Latha Parthiban.pdf.

K. Mohapatra, “effective operational risk management Cybersecurity vulnerability in Indian banks,” CYBERSECURITY Framew. BANKS, 2016, [Online]. Available: https://financialit.net/sites/default/files/customerxps_white_paper_cyber security_vulnerability_in_indian_banks_1.pdf.

M. M. MANISHA, J. M. P, and N. K.M, “International Journal of Advanced Research in Online Banking and Cyber Attacks : The Current Scenario,” Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 5, no. 12, pp. 743–749, 2015, [Online]. Available: https://www.researchgate.net/publication/290325373_Online_Banking_and_Cyber_Attacks_The_Current_Scenario.

A. Saravade, N ; Bhalla, “Emerging trends and challenges in cyber security _ Reserve Bank Information Technology Private Limited (ReBIT).” 2018, [Online]. Available: https://rebit.org.in/whitepaper/emerging-trends-and-challenges-cyber-security.

D. V. Saraswat, “Cyber security,” 2003. doi: 10.1016/j.techsoc.2003.09.022.

S. Goel, “Cyber-Crime: a Growing Threat To Indian Banking Sector,” 3rd Int. Conf. Recent Innov. Sci. Technol. Manag. Environ., vol. 2016, pp. 13–20, 2016, [Online]. Available: http://data.conferenceworld.in/IFUNA18DEC16/P13-20.pdf.

RBI, “the Reserve Bank ’ S Accounts,” 2019. [Online]. Available: https://m.rbi.org.in/Scripts/AnnualReportPublications.aspx?Id=1267.

MR. DIGPAL SINGH H. RATHORE & MR. KARN MARWAHA, “CYBER CRIME IN BANKING SECTOR -LAW MANTRA,” vol. 2, no. 7, 2014, [Online]. Available: www.lawmantra.co.in.

“HACKED: HOW $171 MN STOLEN FROM UNION BANK WAS RECOVERED,” 2017.

O. Kolesnikov, “Cosmos Bank Swift / Atm Us $ 13 . 5 Attack Detection Using Security,” 2018. [Online]. Available: https://www.securonix.com/web/wp-content/uploads/2018/08/Securonix-Threat-Research-Cosmos-Bank-Report.pdf.

“Cosmos Bank’s server hacked, ₹ 94 crore siphoned off in 2 days,” Live mint, 2018.

I. Mugari, S. Gona, M. Maunga, and R. Chiyambiro, “Cybercrime - The Emerging Threat to the Financial Services Sector in Zimbabwe,”

Mediterr. J. Soc. Sci., vol. 7, no. 3, pp. 135–143, 2016, doi: 10.5901/mjss.2016.v7n3s1p135.

D. Stiawan, M. Y. Idris, A. H. Abdullah, F. Aljaber, and R. Budiarto, "Cyber-attack penetration test and vulnerability analysis," Int. J. Online Eng., vol. 13, no. 1, pp. 125–132, 2017, doi: 10.3991/ijoe.v13i01.6407.

A. Lakshmanan, "Literature review on Cyber Crimes and its Prevention Mechanisms," no. February. pp. 1–5, 2019, doi: 10.13140/RG.2.2.16573.51684.

L. Ali, F. Ali, P. Surendran, and B. Thomas, "The Effects of Cyber Threats on Customer's Behaviour in e-Banking Services," Int. J. e-Education, e-Business, e-Management e-Learning, vol. 7, no. 1, pp. 70–78, 2017, doi: 10.17706/ijeeee.2017.7.1.70-78.