Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
January-June 2024 5(1), 2559–2569

ANALYZING CYBERCRIMES AND CYBER SECURITY LANDSCAPE IN THE BANKING SECTOR OF INDIA

Sagar Sharma[1], Monali Chouhan[1], Aishwarya Bhardwaj[1]

[1] Research Scholar, Department of Banking and Business Economics, UCCMS, Mohanlal Sukhadia University, Udaipur, Rajasthan

DOI
10.29121/shodhkosh.v5.i1.2024.2747

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

Since the onset of COVID-19, the banking sector has been completely digitalized, in terms of both back-end and front-end operations. With the emergence of latest technologies, the incidence of cyber-attacks is constantly increasing. Most of the banking institutions are online it has caused ransomware, phishing attacks, privacy concerns, and other risks. Both online and mobile services lack in strong security measures and cyber threats are getting more common. The banking sector always remains on the radar of cybercriminals for financial benefits.

This paper studies the devastating effect of cybercrime in the Indian banking sector, existing cyber security landscapes to curb the effects of cyber threats, and measures to protect the Indian banking sector. The study is based on secondary data collected from various online sources, articles, research papers, government portals, news sites, etc. It is also required for case studies of cyber crimes that have led to significant financial loss in recent years. This paper will look into cyber security measures that will help financial institutions, banks, and society by dealing with cyber-attacks that can be prevented for better security.

Keywords: Cyber Security Measures, Banking Sector, Financial Institutions, Cyber-Attacks, Cyber Threats, Indian Banking Sector, Phishing, COVID-19

1. INTRODUCTION

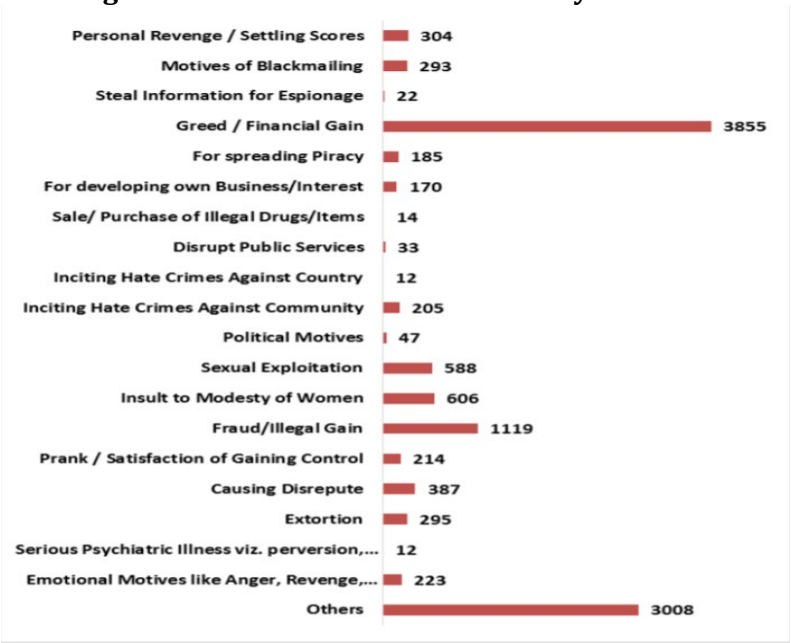
The term “Cybercrime” is defined as the crime in which internet connection and computer is used as a medium, tool, target, source, or crime scene (Moore, 2014). Some of the common cases of cybercrime are spamming, credit card fraud, e-money laundering, spoofing, phishing, ATM fraud, UPI fraud, identity theft, and “Denial of Service (DoS)”. These are very serious threats to the economy and because the incidents of the same are skyrocketing in banking and financial institutions the amount of risk involved in it is also high as banking sector is a huge industry with millions of billions of customers worldwide.

According to Global Findex 2017, over 1.2 billion people have opened their accounts in banks since the year 2011 (Klapper et al, 2017). Banking sector in India also is enjoying a rapid growth. With the increasing use of debit and credit cards, digital wallets, and UPI, cyber threats are rising rapidly. According to a study, around 51% of Indians who are going digital are using online banking mediums and 26% of them avail banking services through official websites and mobile banking. With the rapid digitalization in banks, there is also a rise in cyber security concerns. Around 22% of cyber-attacks across the world took place in Indian banks alone, according to Gulshan Rai, cybersecurity expert at “National Security Council Secretariat” in the PMO (Business Standard, 2019).

When discussing globally, over US$114 billion is lost to cybercrimes every year and over US$274 billion is spent to combat those crimes (Raghavan & Parthiban, 2014). Cyber threats mainly emerged in 1998 in India, especially when banking industry was privatized. Virus attacks, hacking attempts on websites, Trojan and worms, malicious codes sent by hackers, phishing, "Distributed Denial of Service (DDoS) and "Denial of Service (DoS) have been some of the most common cyberattacks on banks. Cyberwarfare and cyber espionage are some of the latest security threats. When it comes to recent cyber-attacks on Indian banks, $171 million was swindled from Union Bank of India in July 2016 with phishing email attack. In May 2017, thousands of systems were locked down by ransomware attack. Around 52% of 42 million cybercrime victims faced financial loss or some other losses because of scams, hacking, thefts, and frauds (Mohapatra, 2016).

With the upsurge in digital transactions through various modes and mobile devices, incidents of cybercrimes are also grown rapidly. These days, smartphones are used for various purposes, such as payment of utility bills, online shopping, digital payments, etc. and criminals are always in the lookout for sensitive banking information. Financial gain is one of the most common motivations behind a cybercrime over the past several years, followed by extortion, personal grudge, and political reasons (Figure 4).

Figure 4 – Common Motives behind Cybercrime



Source – Goel (2015)

Innate loopholes in existing software and systems used by banks, obsolete defense mechanisms which are highly susceptible to modern security attacks by hackers, and endless entry points to the web are some of the major cyber security issues for banks. Hence, banking institutions should prepare their mandatory cybersecurity landscapes. A lot of cyber security technologies and regulatory measures have been developed, given the increasing cyber threats. It is important to analyze emerging threats and cybersecurity landscape with increasing complexity and frequency of cyber threats. It is important to monitor the progress of banking systems to strengthen their resilience and response against those attacks.

2. REVIEW OF LITERATURE

More & Nalawade, 2015 suggested that with the ever-growing demand for convenient access to banking services from multiple devices by the customers, the significant growth of digital banking attracts cybercriminals. India ranked third in 2014 worst affected by online banking malware, followed by Japan and the US. In addition, there was around 48% hike in financial losses because of e-banking fraud in 2014, as compared to 2013.

Saravade & Bhalla, 2018 highlighted that organized criminals, hackers, and potential cyber threat vectors are constantly targeting Indian banks. One of the classic examples of that is 2016's cyber attack that happened on Canara Bank, where online payments were blocked by a malicious program inserted by a Pakistani hacker.

Mohapatra, 2016 stated that in July 2017, Union Bank was also attacked by cyber criminals who stole over US$170 million. Attackers used spear phishing technique to gain access. According to a KPMG survey, banks were not prepared well with proper cyber security measures. Hence, they were highly vulnerable to devastating cyber threats. Financial frauds rose up to 94% from 89% and financial losses were raised to 63% from 45%.

Soni, 2019 stated that Hackers use different cyberspaces with the advancement of technology to commit cybercrime. Artificial Intelligence (AI) can be used by banks and financial institutions to mitigate cyber threats. AI is directly associated with cybersecurity. AI-based "fraud detection systems" can prevent and detect different types of cybercrimes but the cost of maintenance and implementation is also high.

Bamrara et al 2013 revealed that several cyber threat vectors used by hackers against select banks across India. There is a positive correlation between brute force attacks, spoofing, "cross side scripting" and "buffer overflow" with private and public sector banks in India. In addition, the empirical study also suggests positive correlation between cyber-attacks and intruder detection, such as hacking, identity theft, DoS attack, malicious code, ATM/credit card frauds, etc. with system monitoring.

Gunjan et al 2013 explored the evolution, case study, types, preventive measures, and cyber security landscapes and other details related to cyber criminals because in cybercrime, different types of communication devices and channels are used either directly or any other way as a medium, such as desktop, laptop, smartphones, PDA, vehicles, and watches. Sensitive financial and personal data is shared rapidly for added convenience in online shopping and banking services. It is important to know how cyber criminals work to prevent cybercrimes.

Lekha & Prakasam 2017 presented a general overview on different cyber-crimes and data mining techniques in banking. They also surveyed important and effective data mining techniques to analyze cybercrime data. They recognized patterns in criminal activities to predict next move of criminals and stop them. They present novel techniques of data mining, such as "Influenced Association Classifier", "K-Means", and "J48 Prediction tree" to investigate datasets of cybercrime and sort out the problems.

Raghavan & Parthiban 2014 discovered cybercrimes in banking sector and financial losses to banks. They assessed the scenario of cybercrimes and identified attack vectors in this situation. They also determine different kinds of cybercrimes in banking industry and motives of criminals behind those activities. These acts affect bank's finances badly in terms of developing systems and curbing the effects. So, preventing those attacks is the need of the hour.

Pasricha & Mehrotra 2014 developed a conceptual framework on preventing cybercrime in banking sector in India. Making transactions free from cybercrime is one of the most vital aspects of banking industry. The banking system attracts different crimes due to weak and outdated systems. They made a conceptual framework of different crimes prevalent in banks like money laundering, credit card fraud, and ATM frauds.

Following research gap are identified:

This study is mainly aimed to come up with world-class and robust security measures to prevent cyber-attacks in Indian banks. Various studies have been conducted on cybercrime and a lot of debates and conflicts are also present as well. Some researchers argue that cybercrime rate has been increased due to excessive digitalization, while others promote digitalization for adopting state-of-the-art and universal security measures. There is still lack of solid progress in curbing and eliminating cybercrimes in banks and financial institutions in India. Research gaps are widening in study of major cyber security issues. Hence, this study investigates major loopholes that are usually missed by banks in the process and develops a common platform to curb cybercrimes.

Research Objectives

- To review emerging threats and cyber security landscape
- To determine the effect of cybercrime on Indian banking sector
- To study emerging technologies and suggest cybersecurity measures to protect Indian banking sector

Methodology

In order to fulfill the above research objectives, secondary data was collected from various sources analyzed online to arrive at logical solutions. Some of the common sources used were research papers, journals, statistical data, media

sources, findings of NITI Aayog, RBI, etc. Good amount of information is already available online about cyber threats to banking system.

Hence, secondary method was selected for analysis and collection of data. To find out previous cybercrime incidents and to suggest preventive measures, historical perspective is important. To determine the effect of cyber-attacks, case study approach was used as further step. Scope of the study was to focus only on Indian banking system and bank fraud incidents in India and their impacts.

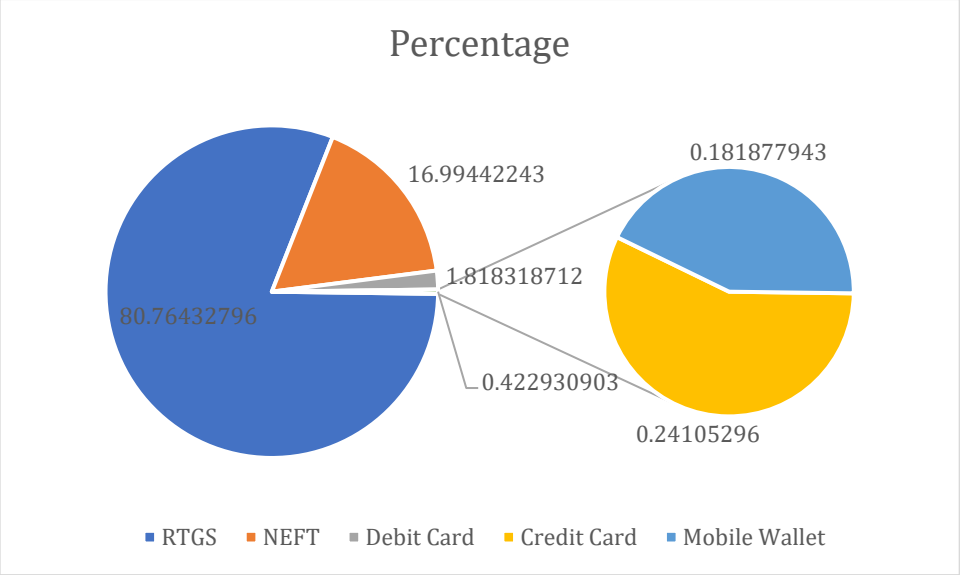
Discussion

Indian banking system is growing rapidly day by day in terms of market size. With the expansion of digital banking in India, a lot of users are switching to various payment modes from cash like mobile banking, net banking, debit cards, credit cards, and UPI. Table 1 illustrates number of transactions and values of them through different modes since May 2020.

Table 1 – Value (in Lakhs) and Number of Transactions (in Lakhs) through different modes (as of May 2020)

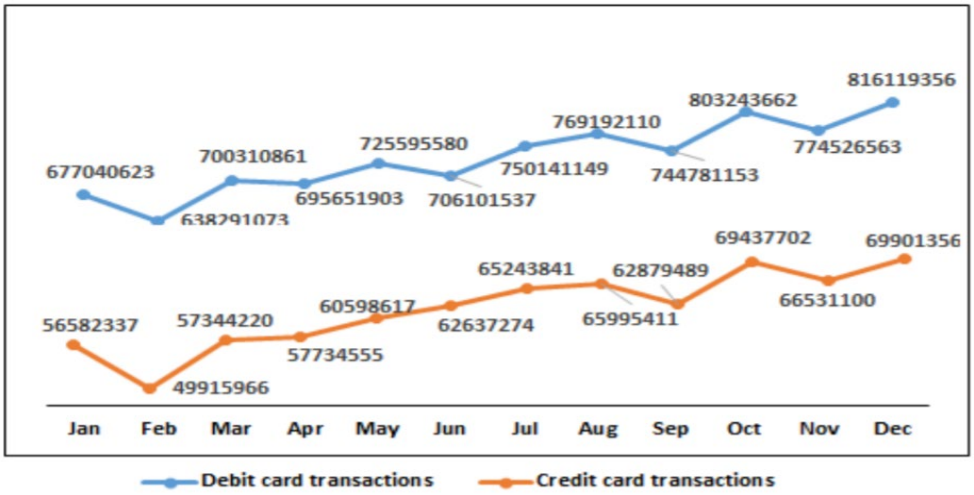
Payment Mode	Total Transactions	Amount
RTGS	9003796	704186936
NEFT	1929.4	148174950
Debit Card	507963710	15853983
Credit Card	77492598	2101749
Mobile Wallet	3958.3	1585800

Source – RBI Bulletin 2020



In 2015 alone, 9545797438 transactions were recorded using debit and credit cards with the rise of digital transactions (Figure 1). It is especially due to recent developments in e-commerce and online banking sectors (Goel, 2015).

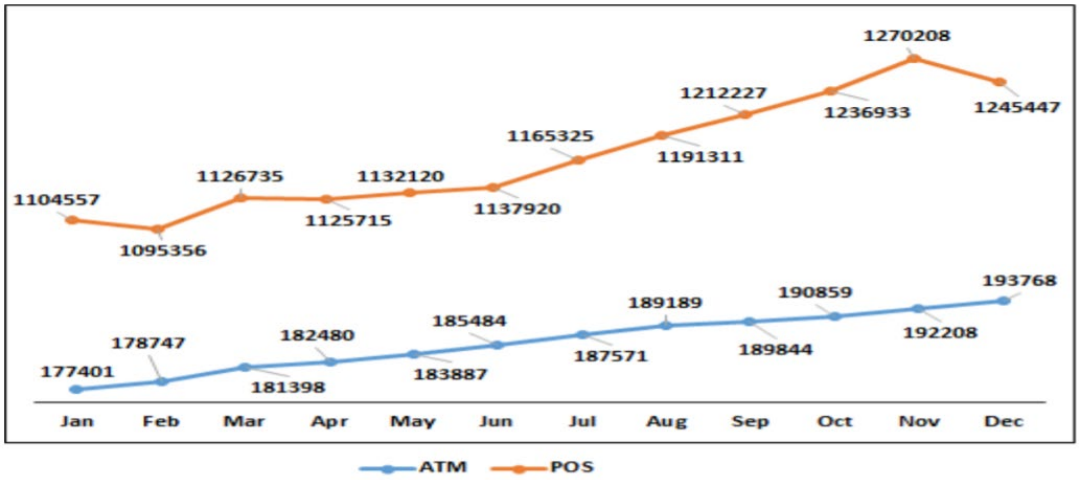
Figure 1 – Debit Card and Credit Card Transactions in 2015



Source – Goel (2015)

POS and ATM are other modes of cashless transactions for added convenience of customers. Figure 2 illustrates the rise in number of POS and ATM machines installed all over India in the year 2015 alone (Goel, 2015).

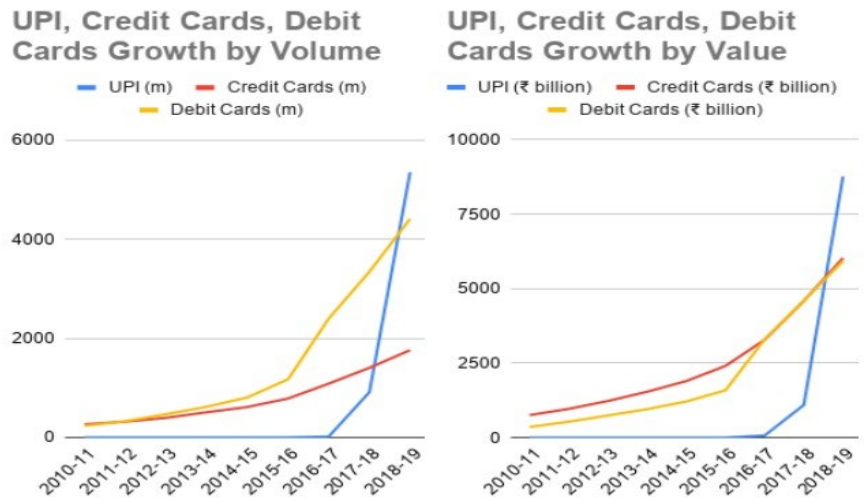
Figure 2 – POS and ATM Transactions (Month-wise) in 2015



Source – Goel (2015)

Later on, another digital payment measure "Unified Payments Interface (UPI)" was introduced in 2016 for added convenience of smartphone users. It surpassed credit cards and debit cards in terms of value and volume of transactions. According to RBI, over 5,353 million UPI transactions were recorded in 2018-19, followed by debit card (4,414 million) and credit card (1,762 million) transactions. This pace of adoption of UPI payments has left debit cards and credit card transactions in the lurch (Figure 3).

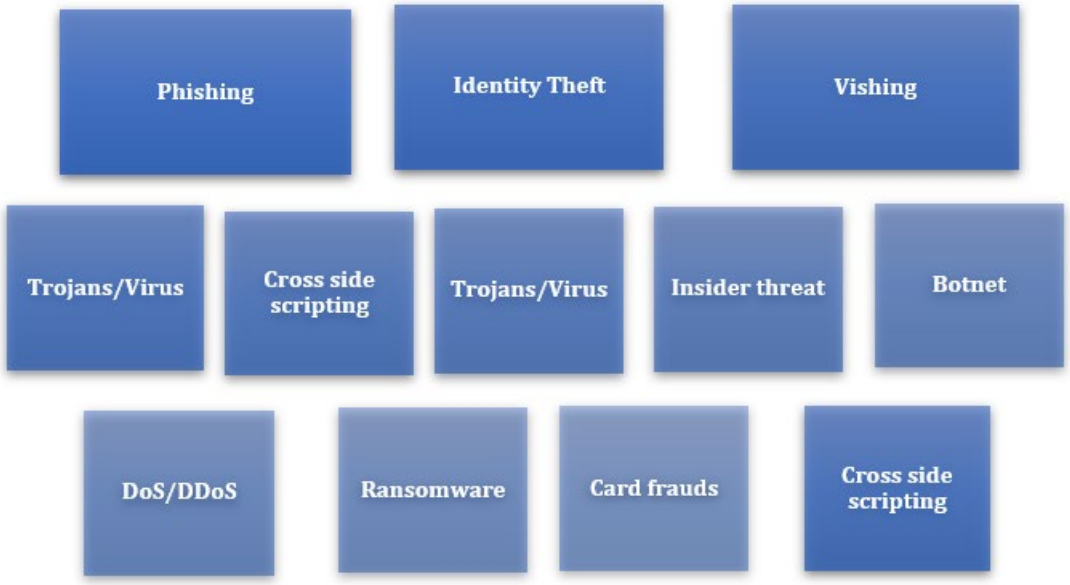
Figure 3 – Growth of Volume and Value of UPI, Debit Cards and Credit Card Transactions



Source – RBI

Bank deposit grew during Financial Year 2016-17 at a CAGR of 11.11% and crossed $1.86 trillion by financial year 2018-19 and, as of Feb 2020, bank deposits stood at US$1893.77 billion (RBI). With the growth of big data due to increase in financial transactions and huge client base, lack of multi-layered and robust security, and widespread businesses, the threats to banks are increasing regarding cybersecurity. Around 88% of impacts on banks are due to data and financial losses by cybercrime. Cyber criminals are not always aimed to cause loss or theft of money. Sometimes they steal personal and financial data to get information on different types of businesses and clients' information (Goel, 2016). This espionage can severely affect banks' reputation and loss of huge customer base out of privacy concerns.

Different types of cybercrimes in Banking Sector:



Phishing - The main objective of this attack is to steal user data, including credit card numbers, ATM pin, and user credentials to access bank account of customer.

Identity Theft – Hackers attempt to steal important personal data like Aadhar details, credit card data, social security number, or other data to impersonate the victim and gain access to something with their name.

Vishing – It is a kind of social engineering application that is used to access personal data through smartphone for ransom purposes.

Cross side scripting – Attacks simply inject scripts from client's side into web pages to bypass the access controls of users.

Trojans/Virus – Virus is simply malicious code which imitates itself without human intervention just like human virus. Trojan is a destructive application which doesn't replicate itself like virus. But it can spread really fast. It is usually sent as attachment on spam emails.

Botnet – In this kind of cyberthreat, attackers infect a network of personal computers using infected codes and this group controls those computers without letting the owners know.

Insider threat – As the name suggests, this threat comes from within the organization. Employees leak the inside information and customer data to attackers themselves for financial gains or other motives.

Card frauds – The fraudsters affix a skimming device with ATM machine's keypad or POS machine and this device is not easily visible through naked eye. The skimmer installed on the system steals the information when a customer enters their card details and PIN and money can be stolen using this machine.

Ransomware – It is one of the most popular threats in cyberspace. This malicious program is meant to block access to a system or a whole network to demand a ransom, mostly in the form of funds. Hackers threaten the victims to transfer specified amount of funds or they would leak sensitive information.

DoS/DDoS – In Denial of Service, hackers take down the services or network denying access to the users. They overload the network traffic by sending a huge amount of data and keep authorized users from using the services. DDoS attacks take place usually on large organizations. It takes a lot of time and money to resolve the threats, although it doesn't cause theft or loss of important data.

Cyber-attacks in Banking Sector in India

Cybercriminals practice different techniques on financial institutions and banks. Here are some of the recent and most popular cyber-attacks that have caused huge financial loss (Ranjitha, 2021) –

Aadhar Portal Hack – It is one of the biggest data breaches ever happened in recent years. Aadhar card data of whopping 1.1 billion Indian citizens was leaked. The official notification was released by UIDAI itself regarding this attack and also declared that hackers hacked over 210 government websites in India. The data breach covered PAN details, Aadhar info, IFSC codes of bank accounts linked with respective Aadhar cards, and other personal data of users. It was also reported that Aadhar data was sold by unknown sellers for Rs. 500 using WhatsApp and printout of Aadhar card for only Rs. 300.

Canara Bank ATM Hack – Around the mid of 2018, hackers targeted ATM servers of Canara Bank. They hacked card details of 300 users and drained Rs. 20 Lakhs from several accounts. Their modus operandi was using ATM skimming devices to steal sensitive data and steal amounts from customers' accounts. Hence, it is very important for banks to improve security measures in their respective ATMs.

Cosmos Bank Attack – Again in 2018, Pune-based Cosmos Bank was targeted by cyber criminals when they wiped off Rs. 94.42 crores. They hit ATM server of the bank, stole all card details, and siphoned the funds off 28 nations and withdrew the amount to the immediate effect. Authorized people should strictly need to strengthen their security systems to prevent such attacks in future.

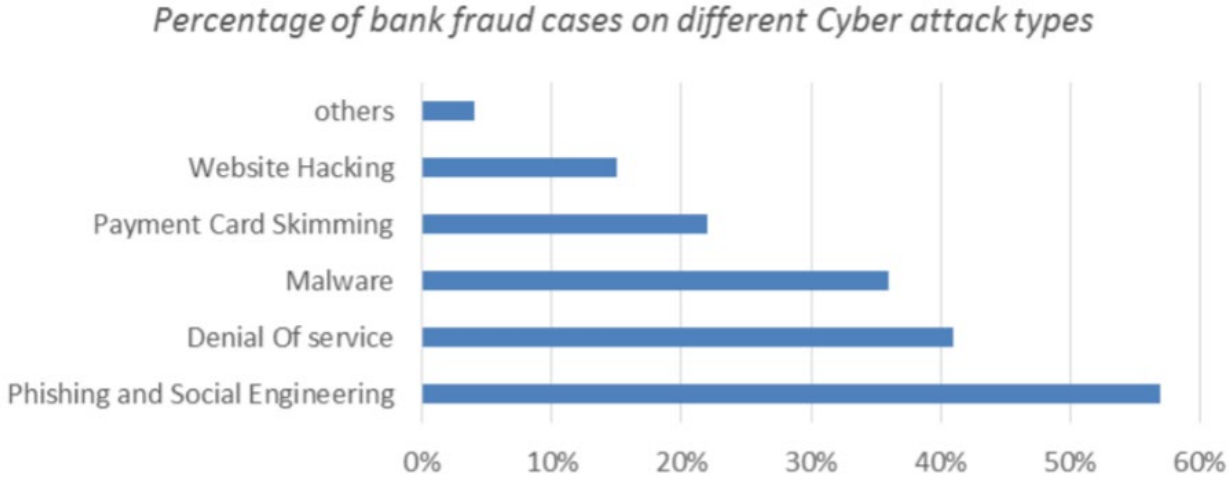
SIM Card Swap – In August 2018, two hackers accessed SIM card data fraudulently and transferred whopping sum of Rs. 4 Crores from the bank accounts. They used online banking to conduct such unauthorized transactions.

These cyber-attack stats and incidents should be considered as the wakeup call to prevent latest cyberattacks in financial sectors in India, which are still susceptible to such threats. There is a strong need to put cybersecurity practices in banking organizations. For customers, the only way to prevent those attacks is never sharing their private data with unknown sources.

Common cyber security threats Indian banks should be aware of.

It is worth noting that banking systems in India have been worst affected by different types of cyberattacks, given a huge volume of data gathered from various resources and analysis from those data. According to Verizon's "data breach report" in 2017, over 50% of banking organizations were apparently affected by phishing, DoS, spear phishing, malware, and ransomware out of various organizations surveyed. DoS, card skimming, and web application attacks are top three cyber-attacks which accounted for over 88% of all incidents (Yue, 2003).

Figure 7 – Most Common Cyber Attacks reported on bank fraud cases in 2017



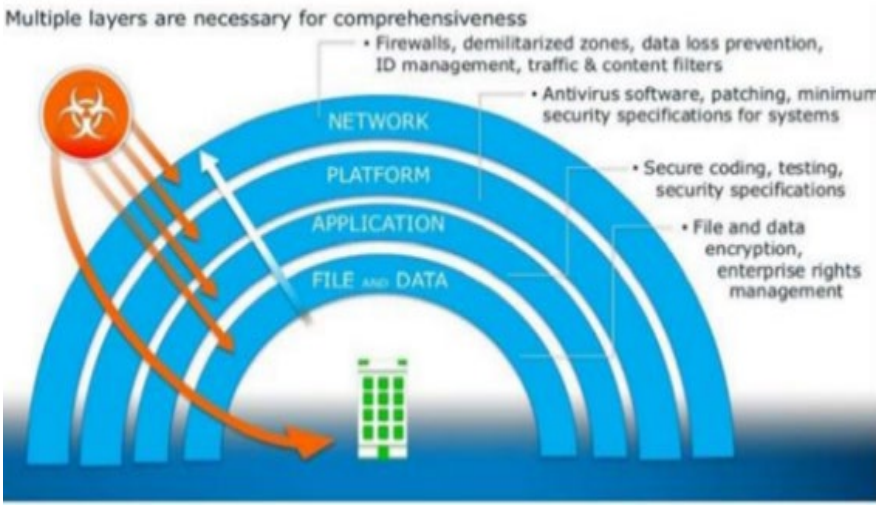
Source – Acharya & Joshi (2020)

Best cybersecurity measures to secure banking and financial institutions in India

Cyber attackers are upgrading their attack modes with time and emergence of technology. They have become even smarter in detecting and analyzing loopholes and security vulnerabilities in systems, so that they can easily disrupt the network and gain access. Banks should also adopt advanced cyber security measures and invest more in protection of their servers from security breaches and unauthorized access to stay ahead of modern attackers and their modus operandi. Proper firewall maintenance and protection can avoid unwanted attacks in banking space (Mugari et al, 2016). Banks should consider various safety measures to avoid any kind of cyberattack. Penetration test is another security measure that banks should adopt to protect their network infrastructure and test security in premises to look for any vulnerability in the network and detect breaches (Stiawan, 2017). Secured Socket Layer (SSL) protocol is one of the measures to prevent attacks on backend applications. SSL certificate adds another layer of security whenever any browser requests to access the website data. It inspects whether the request comes from certified authorities and whether it is being used by the one for which it is issued for. It enables the browser to access data only when all conditions are met.

Poor password management also attracts hackers to network systems. It is important to ensure that password is strong, changed from time to time, stored, and managed in an encrypted manner. At every security layer, password encryption is important. Passwords should be encrypted properly and must not be exposed in the whole system. It is important to follow decryption and encryption regime to access password. The hardcoded configuration file encrypts the passwords and it can be used anywhere in the code. At the same time, decrypted key file can be used for storage of encrypted password. It can protect source code from tampering by the hackers. Multi-factor or two-factor authentication is another way to protect login information (Lakshmanan, 2019).

Figure 8 – A Framework for Multi-layered protection



Source – Menon (2020)

s

Firewall setting must be checked to protect the networks. NITI Aayog has also proposed a framework for multiple layered protections (Figure 8) to protect system core. The traffic content filters and firewalls on the "Network" layer prevent unidentified and unauthorized data to get inside. Antivirus program in "Platform" layer ensures systems meet minimum security specifications. It is important to patch OS and other programs and upgrade them regularly and replace outdated hardware and software with latest variants and updated with latest security patches. There are several source codes in "Application" layer that are important for internal operations. It is important to apply important prevention measures to secure source codes. The developers should maintain password encryption to prevent vulnerabilities in code level. They also need to encrypt and protect files and data for auditing.

3. RESULTS

Along with the above security measures, banks should also introduce self-awareness programs to educate their employees, encourage them with cybersecurity laws, provide data protection training, and make them alert on any kind of vulnerability. On the other side, customers and users should also take precautions while engaging in online transactions. Over 60% customers don't know about common data security threats in banking transactions and 55% of them don't take proper care while using online banking (Ali et al, 2017). Here are some of the important preventive measures all bank employees should follow –

- Using unique and strong password for network login. All unused accounts must be deleted.
- VPN or "Virtual Private Network" must be used for all remote works rather than risking to expose information with remote desktop.
- They shouldn't keep shared software in .exe format in working folders. When needed, they can download from safe folder only after the approval of IT staff.
- They should monitor remote desktop access and disable once used.
- Keep browser up-to-date and ad pop-ups must be blocked.
- They should verify that the site they are browsing is genuine. In case of any doubt, they should report to the IT staff.
- To avoid visiting phishing websites, important websites must be bookmarked.
- Banks should prohibit staff from sharing their private data with unknown sources.
- Email security should be improved to detect and prevent malicious emails.
- Multi-factor authentication must be used for authorized use.
- Employees should scan each email to the back and avoid emails from unknown sources and report them to cybersecurity cell in their bank.
- They should update security software on regular intervals.
- Cover the webcam when they are not used.

- They need to backup data regularly on secured address.

4. CONCLUSION

Cybercrimes are known to update with time and latest technologies and they don't have any barriers. The unexpected growth of devastating effects of cybercrimes is alarming to financial and banking institutions. They should come up with strong security guidelines. The increasing use of online banking services at different levels by millions of billions of people pose a significant challenge for cyber experts to come up with a reliable cybersecurity procedure. Indian banks also need to replace their traditional systems to prevent cyber threats and be prepared to curb those threats. They should adopt modern technologies with agile frameworks and review cybersecurity threats and existing measures. Banks are the backbone of any country in terms of financial support. Banking institution must not be compromised to maintain trust of customers.

CONFLICT OF INTERESTS

None

ACKNOWLEDGEMENTS

None

REFERNCES

Moore, R. (2014). Cybercrime: Investigating high-technology computer crime. Routledge.

Reserve Bank of India - Annual Report. (2022). Retrieved 16 February 2022, from https://m.rbi.org.in/Scripts/AnnualReportPublications.aspx?Id=1264.

Demirguc-Kunt, A., Klapper, L., Singer, D., Ansar, S,. and Hess, J. (2017). The global findex database: Measuring financial inclusion and the FinTech revolution 2017. International Bank for Reconstruction and Development. The World Bank.

Business Standard (2019). Banks most vulnerable to cyber-attacks, must strengthen software: Expert. Retrieved 16 February 2022,

https://www.business-standard.com/article/current-affairs/banks-most-vulnerable-to-cyber-threats-govt-official-119022000646_1.html.

Raghavan, A. R., & Parthiban, L. (2014). The effect of cybercrime on a Bank's finances. International Journal of Current Research & Academic Review, 2(2), 173-178.

Mohapatra, K. (2016). Effective operational risk management Cybersecurity vulnerability in Indian banks," CYBERSECURITY Framework. BANKS. https://financialit.net/sites/default/files/customerxps_white_paper_cybersecurity_vulnerability_in_indian_banks_1.pdf.

More, D. M. M., & Nalawade, M. P. J. D. K. (2015). Online banking and cyber-attacks: the current scenario. International Journal of Advanced Research in Computer Science and Software Engineering Research Paper.

Saravade, A. & Bhalla, N. (2018). Emerging trends and challenges in cyber security: Reserve Bank Information Technology Private Limited (ReBIT). https://rebit.org.in/whitepaper/emerging-trends-and-challenges-cyber-security.

RBI, "The Reserve Bank's Accounts," 2019. https://m.rbi.org.in/Scripts/AnnualReportPublications.aspx?Id=1267.

Goel, S. (2016). Cyber-Crime: A growing threat to Indian banking sector. In 3rd Int. Conf. Recent Innov. Sci. Technol. Manag. Environ (pp. 13-20).

Ranjitha, S. (2021). 4 Biggest Cyber Security Threats for Indian Banking Sector. Great Learning.

https://www.mygreatlearning.com/blog/biggest-cyber-security-threats-indian-banking-sector/.

Yue, O. C. (2003). Cyber security. Technology in Society, 25(4), 565-569.

Mugari, I., Gona, S., Maunga, M., & Chiyambiro, R. (2016). Cybercrime-the emerging threat to the financial services sector in Zimbabwe. Mediterranean Journal of Social Sciences, 7(3 S1), 135.

Stiawan, D. (2017). Cyber-attack penetration test and vulnerability analysis. International Journal of Online and Biomedical Engineering.

Lakshmanan, A. (2019). Literature review on Cyber Crimes and its Prevention Mechanisms. no. February. pp, 1-5.

Ali, L., Ali, F., Surendran, P., & Thomas, B. (2017). The effects of cyber threats on customer's behaviour in e-Banking services. International Journal of e-Education, e-Business, e-Management and e-Learning, 7(1), 70-78.

Menon V. Assessment of Cyber Security in India [Internet]. ifbi. 2020 [cited 17 February 2022].
https://www.ifbi.com/node/2217.

Acharya, S., & Joshi, S. (2020). 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), 4656-4670.

Soni, V. D. (2019). Role of Artificial Intelligence in Combating Cyber Threats in Banking. International Engineering Journal For Research & Development, 4(1), 7-7.

Bamrara, D., Singh, G., & Bhatt, M. (2013). Cyber attacks and defense strategies in India: An empirical assessment of banking sector. Gajendra and Bhatt, Mamta, Cyber Attacks and Defense Strategies in India: An Empirical Assessment of Banking Sector (January 1, 2013).

Gunjan, V. K., Kumar, A., & Avdhanam, S. (2013, September). A survey of cyber-crime in India. In 2013 15th International Conference on Advanced Computing Technologies (ICACT) (pp. 1-6). IEEE.

Lekha, K. C., & Prakasam, S. (2017, August). Data mining techniques in detecting and predicting cyber crimes in banking sector. In 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS) (pp. 1639-1643). IEEE.

Pasricha, P., & Mehrotra, S. (2014). Electronic crime in Indian banking. Sai Om Journal of Commerce and Management, 1(11), 7-14.