International Journal of Advanced Research in Commerce, Management & Social Science (IJARCMSS)
ISSN : 2581-7930, Impact Factor : 5.880 , Volume 04, No. 03(I), July - September, 2021, pp 59-64

CYBER SECURITY ANALYSIS IN BANKING SECTOR

Dr. Neelam Sethi*

ABSTRACT

Banks are critical to nation-building, particularly in a developing economy like India. Computerization and technology in general have been ingrained in Indian banks from the days of globalization and privatization in the early 1990s. Until this time, the name "bank" conjured up images of a physical institution, a building with a Branch Manager and other officials behind the counters holding massive, voluminous ledgers and people queuing or waiting at cash and other counters. Those were the days. When you say "bank" to a modern-day teen, he doesn't think of a building or a person; instead, he thinks of his computer, an ATM, or his cellphone. Today's banking is more closely tied with technological delivery channels such as ATMs, mobile phones, point-of-sale terminals, and online banking than with any physical human being. It's no surprise that today's customer is unfamiliar with his banker, and that today's banker is unfamiliar with all of his customers. For hundreds of years, the banking industry has been under threat. The first was the actual theft of funds. Then there was the issue of computer fraud. Hacking into servers to steal a customer's personally identifiable information is now a common occurrence, in addition to cyber fraud (PII). The importance of cyber security in the banking industry Because most people and businesses conduct their business online, the risk of a data breach grows every day. This is why a greater emphasis is being placed on examining the role of cyber security in banking processes.

Keywords: *Cyber, Security, Banking, Computer, Transactions Online.*

Introduction

Newer sorts of risks to the safety and security of data, a crucial asset for every organization, are confronting banks and financial organizations. Criminal activities and data theft have gotten smarter and savvier in the age of the Internet of Things, with criminals increasingly employing technology to bypass technological obstacles within the financial system. Because bank cyber security attacks have minimal entry barriers, it is incumbent on them to invest in systems and technologies that go beyond simply preventing an attack.

The obvious reason for cyber security's importance in banking transactions is to safeguard consumer assets. Online checkout pages and physical credit scanners are becoming increasingly common as more people go cashless. PII can be routed to other locations and utilized for nefarious purposes in both cases.

This has an impact on the customer as well. It also causes significant damage to the bank while they attempt to restore the data. The bank may have to pay hundreds of thousands of dollars to get the information back if it is kidnapped. As a result, their clients and other financial institutions lose faith in them.

That isn't the only issue that happens when cyber security banking measures aren't taken. The customer must cancel all of their credit cards and open new accounts, maybe with a different bank. Even if their assets are insured by the FDIC, fraudsters are still attempting to steal their personal information.

* Assistant Professor, E.A.F.M., Government P.G. College, Nimbahera, Rajasthan, India.

Three Current Risks Related with Online Banking

The aforementioned examples only represent a small portion of the potential cyber security issues in banking. Among the other things to be cautious about are:

- **More Hazards from Mobile Apps:** More people are using mobile apps to access their bank accounts. Because many of these people have little or no security, the risk of being attacked is substantially higher. To avoid unauthorized activities, banking software solutions are necessary at the endpoint.
- **Breach at a Third-Party Company:** Hackers have turned to shared banking systems and third-party networks to get access as banks' cyber security has improved. If these aren't as well-protected as the bank, the attackers will have little trouble breaking in.
- **Increased Danger of Cryptocurrency Hacks:** In addition to traditional finances, the rising realm of cryptocurrency has seen an increase in hacks. Because the banking industry is confused how to apply cyber security software in an ever-changing environment, attackers have a better chance of stealing big sums of money. Especially when the number changes quickly.

Review of Literature

(Al-alawi, 2020) studied "*The Significance of Cyber security System in Helping Managing Risk in Banking and Financial Sector*" The goal of this study is to show the major impact and benefits of implementing cyber security in an organization's systems, with an emphasis on the banking sector. In addition, the goal of this research is to promote the use of cyber security in order to keep information safe and properly manage risk. Many banking and financial institutions, on the other hand, remain cautious when it comes to the application and usage of cyber security. In fact, many financial organizations may be completely unaware of the advantages of cyber security. Furthermore, its application's higher expenditures could be a factor in its rejection. As a result, numerous questions were posed to measure the level of cyber security awareness and abilities in these banks.

(Alghazo, Kazmi, & Latif, 2018) studied "*Cyber Security Analysis of Internet Banking In Emerging Countries: User and Bank perspectives* " Internet banking, also known as Electronic banking (E-banking), Online banking, and Virtual banking, is frequently pushed as a convenient banking alternative, according to the study. In the banking business, internet banking has shown to be an optimal and profitable method of banking. The majority of banks have quickly adopted this technology in order to save money and improve customer service. The adoption of technology is based on the gathering of knowledge and the formulation of a set of beliefs that will assist the user in accepting or rejecting it. The technology acceptance model (TAM) states that user acceptance of technology is influenced by two factors: ease of use and utility.

(Marshall, 2010) studied "*Online Banking: Information Security vs. Hackers Research Paper*" Banks and Savings & Loans were designated as financial institutions, and both are custodians of their customers' money, but a financial institution is even more responsible for their customers' personal and legacy data. Day-to-day transactions, such as deposits, withdrawals, balance amount, social security number, birth date, loan information, partnership agreements related to a loan, year-to-date statements, and a host of other extremely sensitive financial information are examples of information that financial institutions are the custodian of records for their commercial and personal banking customers. All of the above-mentioned records, transactions, and sensitive information are events that happen more than 50% of the time online.

(Ojeka, Ben-Caleb, & Ekpe, 2017) studied "*Cyber Security in the Nigerian Banking Sector: An Appraisal of Audit Committee Effectiveness*" and noticed that Internet cyber thieves continue to improve their fraud methods, resulting in annual losses of billions of naira. As a result, the audit committee will need to obtain technological skills, as the criminal has more authority and better technical facilities to carry out his or her crime. In the best interests of banks, the audit committee must develop technological knowledge in order to stay up with the worldwide community's developing trend. In terms of financial competence in cyber security, an audit committee needs a high level of financial literacy to successfully manage a company's financial control and reporting. The responsibility of an audit committee in overseeing managerial accountability is broad, encompassing the entire risk management process. This necessitates accounting skills on the part of the audit committee in order to gain a thorough understanding of the financial repercussions of cybercrime.

(Rajendran, 2018) studied "*CYBER SECURITY IN BANKS CYBER SECURITY IN BANKS*" I discovered that there is Cyber Crime as a Service! With technology so ingrained in today's banking, it's

no wonder that clients are often as tech-savvy as, if not more so than, a typical bank employee. When a customer notices a problem with their remittance, statement, or Account View, for example, banks can no longer use the standard routine remark or the overused cliché, such as "it's a computer problem," "a software issue," or "a technological failure." Customer, without a doubt, is aware of the situation.

(Karunakar Mohapatra, 2018) studied "*Cyber security vulnerability in Indian ban*ks" and pointed that that The Reserve Bank of India recently addressed all banks in India a statement urging them to update their security standards and deploy a revolutionary cyber security system in accordance with the RBI's guidelines. This requirement is common, and it is customary for the governing body of the world's central banks to introduce new and enhanced regulatory compliance legislation. While all of this may appear rudimentary on the surface, it does provide one reason to consider and reflect on the grounds for such a mandate.

(Baur-Yazbeck, Frickenstein, & Medine, 2019) studied "*CYBER SECURITY*" Research discovered that digital financial services (DFS) have a lot of potential for enabling financial inclusion and consequently improving people's lives. Cybercrime, on the other hand, has emerged as a major worry in the financial markets of developing and emerging countries, threatening to stymie global progress toward more equitable financial sectors. FSPs and their clients, as well as financial sector authorities and supervisors, confront difficulties in adapting their behaviors, processes, and regulations to adequately handle the rising risk of cybercrime and technology failures.

(Ponemon, 2020) studied "*TAILORING CYBER SECURITY* " It found that while banks moved digital to improve consumer convenience, stay afloat in the competitive landscape, and cut transaction costs, cyber dangers in the banking sector have escalated rapidly. At every touch point, modern technologies and digitalisation generate a wealth of confidential and useful data. This vast amount of personal data, as well as the data stored in the bank's data centres, applications, and network, could be misused for a variety of reasons. Cyber incidents/attacks have increased in number, regularity, and severity in recent years.

Protect yourself from Cyber-Attacks by Using Secure Software

- **Security Audit:** Before implementing any new cyber security software, a thorough audit is required. The analysis exposes the current setup's strengths and drawbacks. It also makes recommendations that can help you save money while also allowing you to make the right investments.
- **Firewalls:** The setting of cyber security banking does not just contain programs. It also necessitates the proper hardware to thwart attacks. Banks can block harmful activity before it reaches other portions of the network with an updated firewall.
- **Antivirus and Antimalware Software:** While a firewall upgrade improves security, it won't prevent attacks unless anti-virus and anti-malware software is updated as well. Older software may not have the most up-to-date virus signatures and regulations. As a result, it may overlook a potentially catastrophic attack on your system.
- **Multi-Factor Authentication (MFA):** This security feature, also known as MFA, is crucial for customers who conduct their banking using mobile or web apps. Many users do not change their passwords on a regular basis. Or, if they do, they make minor adjustments. MFA prevents attackers from gaining access to the network by requiring an additional degree of security. A six-digit code, for example, might be transmitted to a customer's cell phone.
- **Biometrics:** This is a more secure kind of MFA than a texted code. To validate a user's identity, this type of authentication uses retina scans, thumbprints, or facial recognition. Although this form of authentication has been hacked in the past, it is more difficult to do so now.
- **Automatic Logout:** If a website or app allows it, a user can stay logged in indefinitely. As a result, they can access their data at any moment without having to input their login credentials. However, attackers will be able to readily get your records as a result of this. Automatic logout reduces this by denying access to a user after a few minutes of inactivity.
- **Schooling:** All of the aforementioned strategies can help to improve cyber security in the banking industry. They won't be able to help if clients continue to access their data from unsecure areas or save their login credentials incorrectly. This is why it is critical to get a good education. When banks inform their customers about the consequences of these vulnerabilities, they may adjust their behavior out of fear of losing their money.

Much of a bank's or financial institution's business is conducted via technology, especially the Internet. Your bank's sensitive data may be at danger if you don't have strong cyber security procedures in place. The five most serious dangers to a bank's cyber security are listed below.

Data That Isn't Encrypted

This is a fundamental but critical aspect of excellent cyber security. All data saved on your banking institution's systems and on the internet should be encrypted. Even if hackers steal your data, if it's encrypted, they won't be able to use it right away - if it's not encrypted, hackers will be able to use it right away, causing major difficulties for your financial institution.

Viruses

Malware-infected end user devices, such as PCs and mobile phones, represent a threat to your bank's cyber security every time they connect to your network. Sensitive data goes across this connection, and if the end user device has malware placed on it, that malware might attack your bank's networks if it is not secured properly.

Services Provided by Third Parties That Aren't Secure

In order to better serve their clients, many banks and financial institutions use third-party services from other providers. However, if those third-party providers don't have adequate cyber protection in place, your bank might be the one to bear the brunt of the damage. It's critical to consider how you'll defend yourself against third-party security dangers before implementing their solutions.

Data that has been Tampered with

Hackers don't always go in to take data; they only want to modify it. Unfortunately, this form of assault is difficult to identify immediately away and can cost financial organizations millions, if not billions, of dollars in losses. Because altered data doesn't always appear to be different from unmodified data on the surface, it might be difficult to tell what has and hasn't been changed if your bank has been hacked.

Parodying

Spoofing is a newer sort of cyber security problem, in which hackers imitate a banking website's URL with a website that appears and performs identically. When a user submits his or her login information, hackers steal it and store it for later use. Even more worrying is the fact that modern spoofing techniques do not rely on a slightly different but similar URL to target viewers who have already visited the right URL.

It is critical for you, as a bank or financial institution, to identify strategies to limit cyber security dangers while still providing your consumers with easy, technologically sophisticated solutions. SQN has collaborated with Q6Cyber, a pioneer in the cyber security business, to assist provide greater security against potential data breaches.

Cyber-Related Issues are an Inevitable Component of Digitization

The digitalization of large amounts of private data and banking operations has been a top priority for banks in boardrooms (not limited to payments). Digital technologies such as cloud, Artificial Intelligence (AI), analytics, Internet of Things (IoT), and Machine Learning have gotten a lot of attention as a result of this urgency (ML). Confidential information will be kept on remote servers and will be accessible anywhere as a result of technological progress. Increased digitalisation and remote operations will create more vulnerabilities and possibilities for hackers, putting institutions at risk of data breaches or hacking. When dealing with cyber risks, banks must be aware of the following issues:

- **Cybercrime has become more Sophisticated**

Armed robbery is no longer a significant issue when compared to cyber threats and assaults. Even while the forms of cybercrime are comparable to the sorts of frauds that banks have been dealing with for years, cyber hazards have evolved to include more than data leaks, access controls, and system outages in today's environment. They've moved into the realms of cyber skulduggery, stealing customer debit and credit card data, siphoning funds through reprogrammed Automated Teller Machines (ATMs), interfering with the banking network's productivity, and engaging in data theft and money laundering through sophisticated software programs and network algorithms (that vary in nature, origin, and source). Cybercriminals can quickly adapt to any virtual operating environment, regardless of how advanced the platform is. Furthermore, unlike isolated frauds that pose microprudential risks to individual entities, cybercrime in banks (or any financial institution) can have systemic consequences (exacerbated by financial and technological links between financial and non-financial institutions), resulting in a multiplier effect and massive economic losses. Cybercrime, according to a recent IMF assessment, is a rising source of macro-critical risk.

- **Complications in Data Handling**

Because banks handle a vast quantity of Personally Identifiable Information (PII) and financial data, they are always a prominent target for hackers. To address the increased demand for better services at lower prices, more banks are turning to cloud and IoT for data transfers and transaction processing. With greater customer awareness of data privacy and regulators' worries about data governance, banks have made data security and efficient administration a top goal.

- **Constraints Imposed by Outdated Systems**

The IT architecture of banks is a jumble of on-premise core legacy systems and a slew of custom and supplementary applications. Although legacy systems are necessary for vital services, they are ill-equipped to handle the demands of "speed and mobile banking." Core applications are connected with new ones to stay up with the changing paradigm, exposing the former to unique, frequent, and ever-evolving security risks.

- **Ensuring the Safety of Third-Party Services (Vendors and Alliance Partners)**

The security of a bank is only as strong as its weakest link. In banking operations, the banking ecosystem is highly interwoven, and banks must rely on alliance partners and third-party vendors. Because these suppliers need access to banks' networks to carry out numerous of their activities, any flaw in their cyber security architecture might pose a security risk to banks. In other words, banks are also responsible for the cyber security of third-party services.

High risk of being exposed to a hacked network and devices More stakeholders are attempting to access to banks' networks digitally via personal devices as a result of COVID-19.

An increase in the volume of traffic flowing to the banks' network might result in increased cyber security risks and vulnerabilities. Employees' need for remote access, as well as consumers' usage of a variety of devices and networks to access banking services, may jeopardize banks' assets and networks. Banks will face a difficult problem in managing risks emerging from many access points (used by workers and consumers).

- **A Scarcity of Qualified Cyber Security Experts**

Despite the ever-increasing need and complexity of cyber hazards, the cyber security workforce is in limited supply throughout the world. The majority of respondents in a global study conducted by the Information Systems Audit and Control Association (ISACA) said that their cyber security teams were understaffed and had resourcing and retention issues. In India, there is a comparable scarcity of experienced people in this field. According to the Data Security Council of India (DSCI), India would require one million cyber security workers by 2020. It indicated in a recent analysis that cyber security services firms are projected to grow considerably in the near future, and that many of these organizations are re-skilling around half of its cyber security personnel. viii According to these reports, as banks improve their cyber security infrastructure, they will likely confront a lack of trained individuals as well as issues in training their own workers to deal with the increasing complexities of cyber dangers.

- **Regulatory Compliance and Governance**

Over the last several years, the number of restrictions has skyrocketed. The Indian government began formulating the National Cyber Security Strategy 2020 (NCSS 2020) for the next five years (2020-25) under the aegis of the National Security Council Secretariat through a well-represented task force in early 2020. The goal is to ensure a "safe, secure, trusted, resilient, and vibrant cyberspace." Banks are obligated to meet their cyber security regulatory responsibilities. xviii With cyber dangers predicted to escalate, regulatory compliance requirements will only get more difficult for banks to manage and comply to. Since March 2020, the RBI has issued more than ten advisories/alerts to monitored businesses on different cyber hazards and best practices.

Conclusion

Cyber security is a complicated topic that necessitates knowledge and expertise from a variety of fields, including but not limited to computer science and information technology, psychology, economics, organizational behavior, political science, engineering, sociology, decision sciences, international relations, and law. In actuality, while technological measures are crucial, cyber security is not primarily a technological issue, despite the fact that policy analysts and others can easily become engrossed in the technical intricacies. Furthermore, most of what is known about cyber security is divided along disciplinary lines, limiting the benefits of cross-fertilization. This primer aims to shed some light on some of these ties. Most importantly, it tries to leave the reader with two main thoughts. The cyber

security issue will never be completely resolved. The problem's solutions, however restricted in scope and endurance they may be, are at least as much nontechnical as they are technical. They provide specialized banking software development as well as cyber security solutions such as secure socket layers (SSL) for TCP/IP communications. MFA, One-Time Passwords (OTP), Single Sign-On (SSO), and SSH-based File Transfer Protocol all assist to reduce malicious behavior (SFTP). Please contact them with any inquiries or to schedule a consultation.

References

1. Al-alawi, P. A. I. (2020). The Significance of Cybersecurity System in Helping Managing Risk in Banking and Financial Sector. *Journal of Xidian University*, *14*(7). https://doi.org/10.37896/jxu14.7/174
2. Alghazo, J. M., Kazmi, Z., & Latif, G. (2018). Cyber security analysis of internet banking in emerging countries: User and bank perspectives. *4th IEEE International Conference on Engineering Technologies and Applied Sciences, ICETAS 2017*, *2018-January*(November 2018), 1–6. https://doi.org/10.1109/ICETAS.2017.8277910
3. Baur-Yazbeck, S., Frickenstein, J., & Medine, D. (2019). Cyber Security in Financial Sector Development: Challenges and Potential Solutions for Financial Inclusion, (November). Retrieved from https://www.findevgateway.org/paper/2019/11/cyber-security-financial-sector-development-challenges-and-potential-solutions
4. Karunakar Mohapatra. (2018). effective operational risk management Cybersecurity vulnerability in Indian banks. *Cybersecurity Framework in Banks*. Retrieved from https://financialit.net/sites/default/files/customerxps_white_paper_cybersecurity_vulnerability_in_indian_banks_1.pdf
5. Marshall, P. J. (2010). Online Banking: Information Security vs. Hackers Research Paper. *International Journal of Scientific and Engineering Research*, *1*(1), 1–5. https://doi.org/10.14299/ijser.2010.01.001
6. Ojeka, S. A., Ben-Caleb, E., & Ekpe, I. (2017). Cyber Security in the Nigerian Banking Sector: An Appraisal of Audit Committee Effectiveness. *International Review of Management and Marketing*, *7*(2), 340–346.
7. Ponemon. (2020). TAILORING CYBERSECURITY, (May).
8. Rajendran, V. (2018). Security in Banks. *The Journal of Indian Institute of Banking and Finance*, *89*(01), 26–32.