# IMPORTANCE OF CYBER SECURITY IN BANKING

**D.S. Jana, A.E. Khedkar and C.E. Khedkar**
Dr D Y Patil School of Management, Lohegaon, Pune, MS, India
debashree.aims@gmail.com

## ABSTRACT

*The growing use of internet has significantly increased the online banking transactions. That has also led to the increase in cyber security risks. The reasons for cyber security are increasing volumes of online transactions, reputation risks of banks, loss of time and money in fixing the breach and enormous amount of confidential customer data which banks possess. Given the importance of cyber security, a bank must take several measures to safeguard its systems. Firewalls, anti-virus and anti-malware applications, multi factor authentication, biometrics are some of the tools and techniques that help in preventing cyber-crimes. Moreover, a detailed security audit and customer education are the need of the hour.*

***Keywords:*** *cyber security, data privacy, firewalls, security audit*

## Introduction

The banking industry has been under attack for so many years. To start with, it was the physical theft of monies. Then it was computer fraud. Today, it's cyber fraud that however hacks into the servers to get a customer's personally identifiable information (PII). This is the reason, why cyber security for banking sector is of most extreme importance. As individuals & firms perform most of the transactions online, the risk of a data breachesincreases daily. This is the reason there's a higher emphasis to examine the importance of cyber-security in banking industry processes (Khatri, 2019).

## Importance of Cyber Security:

1. Everybody seems to go cashless, using digital currency, debit and credit cards. In this context, it has become very important to ensure that all the measures of cybersecurity are in place, to protect the data and privacy.
2. Data breaches can make it hard to confide in financial institutions and for banks, that is a serious problem. A weak cybersecurity system can result in the data breaches that can easily cause the customer base to take its money elsewhere.
3. Time and money are lost when there is a data breach. Recovering the losses from the same could not only be time-consuming but also stressful. It would require cancelling cards, checking statements, and keeping eyes open for complications.
4. Private data in some unacceptable hands can do a huge harm. Even though the cards are cancelled, and the fraud is immediately taken care of, the data is sensitive and could reveal a great deal of information that could be misused.
5. Banks are expected to be on the guard more than most of the other businesses. That's the expense of holding private and valuable personal data that banks do. This data with the bank could be breached if it is not protected from cyber-crime threats (HDFC Bank, 2021).

## Literature Review

There is ample research available on the topic of cyber security. Below are a few abstracts from the recent literature.

Wang et al. (2020), have posited that, this paper reports the discoveries from an examination project on cyber security in the Nigerian Internet banking industry, by introducing the principal cyber security breaches it has encountered, alongside its cyber-security capability and processes. An on-line survey was directed with 100 experienced professionalswho were working in both the Nigerian banks and banking security services sectors. Our discoveries uncover a transformation of the Nigerian cybercrime industry from low tech cyber enabled crimes to high tech sophisticated breaches, with viruses, worms or Trojan infections; electronic spam mails; and hacking being the best three most experienced breaches. In term of cyber security

practices, banking professionals have gotten satisfactory support and training.

Joveda et al. (2019), have argued that, cyberspace is a great media for exchanging information and data in the arena of e-banking. Banks are under pressure for the establishment of digitalization in its day-by-day operations to fulfill the clients' need. However, the abuse of IT has become a menace in the banking segment of Bangladesh. Concealing of primary source and using advancedtechnology-based solutions to illegally transfer money–the whole process is called Cyber laundering. This study offers insights to enhance an understanding of the relationship between corruption in banks, local economy and money laundering scandals. This research focuses on creating a Cyber-security system for detecting money laundering as it's anything but a threat to Bangladesh's economy.

Soni (2019), has opined that, with the advances in information technology, different cyberspaces are used by criminals to enhance cybercrime. To mitigate this cybercrime and cyber threats, the bank and financial industry attempt to implement artificial intelligence. Different opportunities are provided by AI techniques, which help the banking sector to increase prosperity and development. Information about customer's behavior and interest is provided by artificial intelligence techniques. Artificial Intelligence is additionally involved in protecting personal data. Proper design provided by AI towards the banking sector, by which they are able to identify fraud in transactions. Artificial intelligence is directly linked with the domain of cyber security. Different kinds of cybercrimes are prevented and identified by AI-based fraud detection systems. However, implementation and maintenance of artificial intelligence costs high expense.

According to Maharjan and Chatterjee (2019), banks have become increasingly relying in recent centuries on the latest information-based IT schemes that maintain their wealth in the type of data opposed to conventional companies, where actual money and securities are placed in a safe and secure area. Banks have become the component of internet and daily lives. It's anything but a real task to protect these bank procedures, systems from the attackers and minimize the security threats. With these Cyber-assaults increasing day-by-day, and this is a challenge faced by countries and organizations like banking where data is basic. In frequency, yet in addition in complexity, cyber threats are increasing. The number of cyber security assaults is increasing and becoming progressively destructive which is targeting and broadening the variety of techniques and attack vectors. The vast majority of such incidents can be avoided by implementing adaptable counter-measures quickly and minimizing risk. The objective of this research is to develop a framework to safeguard and minimize the cyber security issue that exists in banking sector of Nepal effectively and in a timely manner before cyber security incidents become a reality.

According to Kesharwani et al. (2019), in the dictionary of criminal terminology, cybercrime is a relative a new term; it has emerged mainly after the introduction of technology in financial sector in late 90's. The present study focuses on the current scenario and technical aspects of cyber-crimes concerning the banking industry and their related challenges and effect. It likewise highlights the measures to battle the resulting cyber-assaults for better enhanced security.

Moreover, Amrollahi et al. (2020), Srinivas et al. (2019), Bilodeau et al. (2019) have dealt with various aspects of cyber security threats.

## Safeguard against cyber-crimes

1. Security audit — A comprehensive audit is an imperative prior to any new cyber security software gets implemented. The thorough review exposes the strengths &weaknesses of the existing setup. Moreover, it provides suggestions that can help save money while also allowing proper investments.
2. Firewalls — Cyber security banking configuration does not just include applications. It also needs the appropriate hardware which can block attacks. With the help of an updated firewall, banks can block the malicious activity before it can reach other sections of the network.
3. Anti-virus & anti-malware applications — While the upgradation of firewall increases protection, it will not stop attacks unless

there are updated anti-virus and anti-malware applications. Older software probably won't contain the latest rules and virus signatures. In turn, it's anything but a potentially disastrous attack on your system.

4. Multi factor authentication — This type of protection, which is also known as MFA, is extremely crucial to protect the interests of customers who use mobile or on-line apps for banking transactions. Many users never change their passwords. Or, they make very small changes. Applying MFA stops the hackers from reaching the network because it has another level of protection. For instance, a six-digit code sent to a customer's cell phone.
5. Biometrics — This is yet another version of MFA which is even more secure as compared to a texted code. This form of authentication relies on thumbprints,retina scans, or facial recognition to confirm a user's identity. Even though the hackers have accessed these types of authentications in the past, it is harder to accomplish.
6. Automatic logout — Many apps and websites allow their users to remain logged-in if they agree. In this way, the users can access their information any time without entering thelog-in credentials. However, this also helps the hackers to easily obtain your records. Automatic log-out minimizes this by closing a user's access after few minutes of inactivity.
7. Education- All of the above-mentioned measures can enhance cyber-security in the banking industry. However, they can't help if customers continue to access their information from locations which are not protected or improperly protect their log-in credentials. For this reason, education is important.

## Conclusion

With the internet penetration increasing day by day, there is significant increase in the electronic banking transactions. At the same time, risk of cyber crimes is also increasing. There are several reasons why cyber security is important. First, increasing transactions means high requirement of privacy and data protection. Second, data breach will do enormous harm to the reputation of the banks. Third, there is significant amount of time and money lost in fixing the breach. Fourth, the private data breach can do many harms and not just the immediate financial frauds. Lastly, banking is different from other industries and hold lot of data about their customers hence need great level of protection.

Given that cyber security is of prime importance, there are several safeguards against the cyber threats. Firewalls, anti-virus and anti-malware applications, multi factor authentication, biometrics are some of the tools and techniques that help in preventing cyber-crimes. A detailed security audit is needed to assess the strength and weaknesses of the system. Moreover, educating the users is the most important step that can help prevent potential cyber-crimes.

## References

1. Amrollahi, M., Dehghantanha, A., &Parizi, R. M. (2020). A survey on application of big data in fin tech banking security and privacy. In Handbook of Big Data Privacy (pp. 319-342). Springer, Cham.
2. Bilodeau, H., Lari, M., &Uhrb, M. (2019). Cyber security and cybercrime challenges of Canadian businesses, 2017. Juristat: Canadian Centre for Justice Statistics, 1-18.
3. hdfcbank.com. (2021). Retrieved from https://www.hdfcbank.com
4. Joveda, N., Khan, M. T., Pathak, A., & Chattogram, B. (2019). Cyber laundering: a threat to banking industries in bangladesh: in quest of effective legal framework and cyber security of financial information. International Journal of Economics and Finance, 11(10), 54-65.
5. Kesharwani, S., Sarkar, M. P., & Oberoi, S. (2019). Growing Threat of Cyber Crime in Indian Banking Sector. Cybernomics, 1(4), 19-22.

6. Khatri, P. (2019). The importance of cyber security in banking - The Global Treasurer. Retrieved from https://www.theglobaltreasurer.com/2019/09/25/the-importance-of-cyber-security-in-banking/
7. Maharjan, R., & Chatterjee, J. M. (2019). Framework for Minimizing Cyber Security Issues in Banking Sector of Nepal. LBEF Research Journal of Science, Technology and Management, 1(1), 82-98.
8. Soni, V.D. (2019). Role of Artificial Intelligence in Combating Cyber Threats in Banking. International Engineering Journal For Research & Development, 4(1), 7-7.
9. Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. Future Generation Computer Systems, 92, 178-188.
10. Wang, V., Nnaji, H., & Jung, J. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. International Journal of Law, Crime and Justice, 62, 100415.