Cybersecurity in Banks and Engineering Solutions: Protecting Critical Systems and Financial Infrastructure

Neha Sharma
Neha456@gmail.com

Abstract

The engineering and banking industries have benefited greatly from the digital transition in terms of productivity and creativity. It has, nevertheless, also increased the cybersecurity threats associated with these industries. This study examines the vital role that cybersecurity plays in banking and engineering solutions, with a focus on protecting sensitive financial data and vital infrastructure. The study highlights the cybersecurity measures used by each sector and dives into the unique difficulties they encounter, such as IoT vulnerabilities in engineering solutions and data breaches. Engineering solutions apply network segmentation, patch management, and access control, while banks rely on multi-factor authentication, encryption, and intrusion detection systems. Through a comparative analysis of these methods, the article identifies similarities and differences and illuminates possible areas of mutual learning for both industries. To remain ahead of emerging dangers, banks, engineering businesses, government organisations, and cybersecurity specialists must collaborate and share information. Future trends and potential risks are also covered in the report, along with suggestions for improving cybersecurity in both fields to guarantee the security and dependability of crucial engineering projects and financial infrastructure going forward.

Key words: cyber, security, banking, computer, transactions online etc.

Introduction

Threats to the safety and security of data, which is an essential resource for every firm, are becoming more sophisticated and affect banks and other financial organisations. Data theft and criminal activity have grown more sophisticated and cunning in the Internet of Things era, with thieves leveraging technology to get past technological obstacles in the financial system. It is incumbent upon banks to invest in systems and technology that do more than only thwart attacks, given the low entry barriers to these types of attacks. The protection of client assets is the clear justification for the significance of cyber security in banking sector transactions. More and more transactions are being made using physical credit scanners and internet checkout pages. PII may be misused for nefarious purposes and diverted to other sites in either scenario.

Review of literature

(Al-alawi, 2020) studied "*The Significance of Cybersecurity System in Helping Managing Risk in Banking and Financial Sector* It discovered that, with a focus on the banking industry, the goal of this study is to illustrate the substantial impact and advantages of implementing cybersecurity in the organization's systems. Additionally, the goal of this study is to promote the use of cybersecurity to effectively manage information risk and maintain information security.

(Alghazo, Kazmi, & Latif, 2018) studied *Cyber Security Analysis of Internet Banking In Emerging Countries: User and Bank perspectives* and noted that online, virtual, and electronic banking—also referred to as Internet, or E- banking—is heavily advertised as a practical banking option. In the banking business, internet banking has shown to be a perfect and lucrative method of banking.

(Marshall, 2010) studied *Online Banking: Information Security vs. Hackers Research Paper* and discovered that banks and savings and loans are classified as financial institutions. These organisations are in charge of managing their clients' money as well as their personal and historical data.

(Ojeka, Ben-Caleb, & Ekpe, 2017) studied *Cyber Security in the Nigerian Banking Sector: An Appraisal of Audit Committee Effectiveness* and noticed that online fraudsters are constantly honing their techniques, resulting in losses that reach billions of naira annually. In light of this, the audit committee must acquire technological know-how since criminals are always gaining more authority and better tools with which to perform their crimes..

(Rajendran, 2018) studied *CYBER SECURITY IN BANKS CYBER SECURITY IN BANKS* and discovered that the service is Cybercrime! Given how deeply technology has permeated modern banking, it should come as no surprise that consumers are frequently just as tech-savvy as—if not more so than—the typical bank employee. Banks typically aren't able to get away with saying anything like, It's a computer problem," It's a software issue," or "It's a technological failure when a customer complains a problem, say with their remittance, statement, Account View, etc. Customer is undoubtedly more aware.

(Karunakar Mohapatra, 2018) studied *Cybersecurity vulnerability in Indian ban*ks He noted that the RBI recently issued out a notice to all Indian banks requesting that they modernise their security protocols and put in place a cutting-edge cybersecurity framework that adheres to RBI regulations.

(Baur-Yazbeck, Frickenstein, & Medine, 2019) studied *CYBER SECURITY* and discovered that the potential for digital financial services (DFS) to facilitate financial inclusion and hence enhance people's lives is rather promising. Nonetheless, cybercrime has emerged as a major danger to global progress in creating more equitable financial sectors and has become a major problem in the financial markets of developing and emerging nations.

(Ponemon, 2020) studied *TAILORING CYBERSECURITY* " He said that as banks have gone digital to promote client convenience, remain afloat in the competitive landscape, and lower transaction costs, cyber dangers in the banking sector have grown rapidly. At every touchpoint, a wealth of private and practical data is generated by the application of cutting-edge technology and digitization.

Safeguard against attacks with secured software

- **Security audit —** Before installing any new cyber security software, a comprehensive audit is essential. The review highlights the advantages and disadvantages of the current configuration. It also offers suggestions that can assist cut costs and make the right investments possible.
- **Firewalls —** Applications are not the sole part of the configuration for cyber security banking. To prevent assaults, the appropriate hardware is also needed. Banks can stop malicious behaviour before it spreads to other areas of the network by using an updated firewall..
- **Anti-virus and anti-malware applications —** Updating your firewall does not guarantee that attacks will stop; you still need to update your anti-virus and anti-malware software. The most recent virus signatures and rules may not be present in older software. Consequently, it can overlook a potentially catastrophic assault on your system.

- **Multi-factor authentication —** The use of multi-factor authentication, or MFA, is crucial for safeguarding clients who conduct their banking using mobile or web applications. A lot of individuals don't update their passwords. If they do, they alter things slightly. By requiring an extra layer of security, MFA prevents hackers from accessing the network. For example, sending a customer's cell phone a six-digit code.
- **Biometrics —** This additional MFA version is even more secure than a code that is texted. Retinal scans, thumbprints, or face recognition are used in this type of authentication to verify a user's identification. Even though this kind of authentication has been used by hackers in the past, it is more challenging to complete.
- **Automatic logout —** If they permit it, a user can remain logged in on a lot of websites and applications. As a result, they never need to input their login details to access their information at any time. But it also makes it easier for attackers to get your records. By terminating a user's access after a few minutes of inactivity, automatic logout reduces this..
- **Education —** By taking the aforementioned steps, the banking industry's cyber security can be strengthened. However, they are unable to intervene if users keep retrieving their data from unprotected sites or mishandle the security of their login credentials. For this reason, education is crucial. Customers may alter their behaviour out of fear of losing their assets if banks inform them of the penalties associated with these vulnerabilities.

Cybersecurity Challenges in Engineering Solutions

- **IoT Vulnerabilities:** Numerous potential vulnerabilities are introduced by the widespread use of Internet of Things (IoT) devices in engineering solutions, such as critical infrastructure or smart factories. Because these devices frequently have weak security features, attackers looking to access a larger network find them to be appealing targets.
- **Complex Systems:** Engineering solutions frequently require intricately linked systems that are difficult to fully safeguard. It might be challenging to detect and eliminate vulnerabilities caused by the interdependence of several components.
- **Legacy Systems:** Numerous engineering solutions continue to rely on antiquated methods that weren't created with contemporary cybersecurity in mind. These systems can be vulnerable to exploitation because they lack crucial security features.
- **Supply Chain Risks:** Vulnerabilities may arise from the worldwide supply chain for software and engineering components when hacked software or components may be incorporated into vital systems. One major problem is making sure the supply chain is secure.
- **Human Error:** An important aspect in cybersecurity issues is human factors. By making mistakes in setups or becoming targets of social engineering attacks such as phishing, engineers and operators run the risk of unintentionally creating vulnerabilities.
- **Regulatory Compliance:** Engineering solutions may find it difficult to comply with cybersecurity standards and laws because they frequently work in highly regulated sectors. It can take careful balance to meet these objectives while preserving operational effectiveness.
- **Resource Constraints:** Robust cybersecurity protections may not always be implemented in engineering projects due to limited finances and resources. Getting affordable solutions that offer sufficient security is a prevalent problem.
- **Emerging Threats:** Engineering solutions must constantly adapt to new and emerging cyber threats, such as zero-day vulnerabilities and sophisticated attack methodologies, due to the quickly changing threat landscape.

- **Safety Concerns:** Cybersecurity breaches may directly affect safety in some engineering solutions. A cyberattack on a vital infrastructure system, for instance, can result in harm to human life or physical property.
- **Data Privacy:** When designing solutions, it is crucial to protect sensitive data, such as private information and intellectual property. Adhering to data privacy laws, such the CCPA or GDPR, might be difficult.

Conclusion

Understanding cybersecurity is a multidisciplinary field involving knowledge and experience from computer "science and information technology, psychology, economics, organisational behaviour, political science, engineering, sociology, decision sciences, international relations, and law, among other fields. Although it is easy for policy analysts and others to become bogged down in the technical intricacies, cybersecurity is not primarily a technological issue in practise, even though technical measures are an important component. Moreover, the body of knowledge on cybersecurity is frequently divided into distinct fields, which limits the insights gained from interdisciplinary research. This overview aims to shed light on a few of these relationships. It aims to leave the reader with two main concepts above anything else. It will never be possible to completely fix the cybersecurity issue. Even though their breadth and durability may be constrained, the problem's solutions are at least as much nontechnical as they are technical. They provide secure socket layers (SSL) for common TCP/IP connections, as well as specific banking software development and cyber security solutions. Through MFA, One-Time Passwords (OTP), Single Sign-On (SSO), and SSH-based File Transfer Protocol, they also aid in reducing harmful behaviour (SFTP)". Get in touch with them for consultations or with any queries you may have.

Reference

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.