ISBN: 978-81-974088-9-2

9. Cybersecurity in Financial Services

Dr. Vimmi Behal

Assistant Professor,
Atal Bihari Vajpayee Hindi Vishwavidyalaya,
Bhopal (M.A).

Abstract:

Scholars and experts are attempting to comprehend this issue from several angles since the cyber-security risk has emerged as a large concern to the financial industry. The security technologies and their ability to safeguard sensitive data and data assets are thoroughly examined in this article. Along with that, it will offer opinions on what technologies each kind of firm may affordably employ to defend against various cyberattacks. Small and medium-sized companies (SMBs) and large firms are the only research topics that are covered in the literature. For companies of all sizes, this study aims to provide a thorough analysis. Cybersecurity in Financial Services will be covered in this paper.

Keywords:

Cybersecurity, Financial Services, Threat, Data Protection, Prevention, Management, Safeguard.

9.1 Introduction:

Financial institutions as well as financial regulators are very concerned about cybersecurity. Concerns regarding the security and privacy of customer financial information have grown in light of recent data breaches at major financial institutions.

Because it contains so much valuable financial data and assets, the financial industry is a prime target for hackers. Because it safeguards private client information, guarantees the accuracy of financial transactions, and verifies regulatory compliance, cybersecurity is essential to the financial sector's performance.

Financial institutions need to be cautious while installing and updating their cybersecurity safeguards because cybersecurity threats are always changing. If this is done carelessly, there may be severe financial losses, harm to one's reputation, and legal repercussions. In order to preserve client, trust and guarantee the integrity of financial transactions, the financial sector needs to keep making investments in cybersecurity. [1]

Digital banking, online investing platforms, electronic payment systems, and other web-based financial services have all been made possible by technological advancements. The digital revolution has improved accessibility and convenience of financial services. But the move to digital platforms has also brought up new difficulties, especially with regard to cybersecurity.

Financial organizations are a popular target for cybercriminals because they handle large sums of money and sensitive data. These are the principal causes behind the financial industry's growing worry over cybersecurity. [2]

9.2 Importance of Cybersecurity in Financial Services:

Here are a few reasons cybersecurity is critical for financial services companies:

- **Sensitive Data Protection:**

Financial firms manage a tonne of personal and financial data, such as the names, addresses, credit card numbers, social security numbers, and transaction histories of their clients. Customers like this data, but hackers who exploit it for fraudulent operations also find it important.

Various cybersecurity tools are used by financial services businesses to safeguard sensitive financial data. Cybersecurity makes ensuring that the data is only accessible to authorized users and systems through strong authentication procedures, encryption, and secure networks. In order to reduce any harm, it also offers means to identify and address any illegal access or data breaches.

9.3 Trends in Financial Services Cybersecurity:

A. Regulatory Landscape:

Regulations have a big impact on the cybersecurity developments in the financial industry. Data management services and governance are becoming more important with the introduction of the GDPR, CCPA, and other data protection rules. Furthermore, strong financial services cybersecurity rules are crucial for guaranteeing that financial institutions follow Financial Industry Regulatory Authority (FINRA) guidelines.

B. Rise in Cyberattacks:

A concerning development is the rise in cyberattacks targeting financial services. Attacks with the primary goal of obtaining private information are phishing attempts. Next are cases of ransomware, in which criminals encrypt government data and demand a payment. Finally, it's not necessarily an external threat. Insider dangers can be just as dangerous yet are frequently disregarded. The significance of data lineage and comprehending the movements and transformations of data throughout the business are highlighted by these instances.

C. Enhanced Authentication and Biometrics:

Financial institutions are moving toward more sophisticated authentication techniques in response to growing cyber threats. Unique biological characteristics are used in biometric verification to make sure that only authorized users are granted access.

D. Secure APIs and Open Banking:

The need for safe APIs is growing as a result of open banking. This promotes strong financial services cybersecurity in addition to facilitating smooth interactions between financial platforms.

E. Incident Response and Cyber Insurance:

In light of the possibility of cyberattacks, prompt incident response is critical. Because cyber insurance protects financial institutions against potential losses, they are now better prepared to handle breaches. [3]

9.4 Review of Literature:

(Al-alawi, 2020) investigated "The Significance of Cyber security System in Helping Managing Risk in Banking and Financial Sector" This study's objective is to demonstrate the significant effects and advantages of integrating cyber security into an organization's systems, with a focus on the banking industry. Furthermore, the research aims to encourage the use of cyber security to protect data and effectively manage risk. However, many financial and banking organizations continue to exercise caution when it comes to the implementation and use of cyber security. It's possible that a large number of financial institutions are totally ignorant of the benefits of cyber security. Moreover, the application's increased costs might have contributed to its denial. Thus, a number of inquiries were made in order to gauge these banks' understanding of and proficiency with cyber security. [4]

The banking industry, according to Cawley (2017), is struggling to stay up with the latest technology advancements, particularly with regard to rules pertaining to the banking system's operations. Customers find the technical legacy inconvenient, and banks and their customers face serious security threats.

According to Cawley, one security measure against cyberattacks is the use of two-factor authentication, which shields customer bank accounts. In this scenario, attackers would require access to both the computer and the mobile device in order to access account information and financial transactions. Banks would often transmit codes to their customers' mobile devices prior to log-in.

Many financial organizations are not utilizing two-factor authentication to safeguard their clients' banking accounts and information, regardless of how successful the process is. He described the predicament in a Bangladeshi bank, where the bank's computer system contains flaws. They found malware on the client's computer system, which is used by hackers to get around risk controls and initiate the money transfer process. [5]

A. Objectives:

- Cyber security is key for Banks to keep customers money safe and secure.
- Threat detection, prevention, and response.

B. Research Methodology:

This study's overall design was exploratory. The research paper is an endeavor that is founded on secondary data that was obtained from reliable online resources, newspapers, textbooks, journals, and publications. The research design of the study is mostly descriptive in nature.

9.5 Result and Discussion:

Financial institutions as well as financial regulators are very concerned about cybersecurity. Concerns regarding the security and privacy of customer financial information have grown in light of recent data breaches at major financial institutions. For instance, a data breach at the insurance company First American Financial in 2019 resulted in the exposure of 885 million files containing sensitive financial information; at Experian, a data breach in 2020 exposed the information of 24 million customers; and in 2022, an employee of Block downloaded and disclosed the information of 8 million customers.

According to research, financial services organizations are the target of 25% of malware attacks. Moreover, the expenses incurred by financial institutions due to cybercrime surpass those incurred by other sectors. As an illustration, Figure 1 shows that the average cost of cybercrime for financial services organizations is approximately $18 million, which is approximately 40% greater than the cost for other industries, based on a 2019 private study. [6]

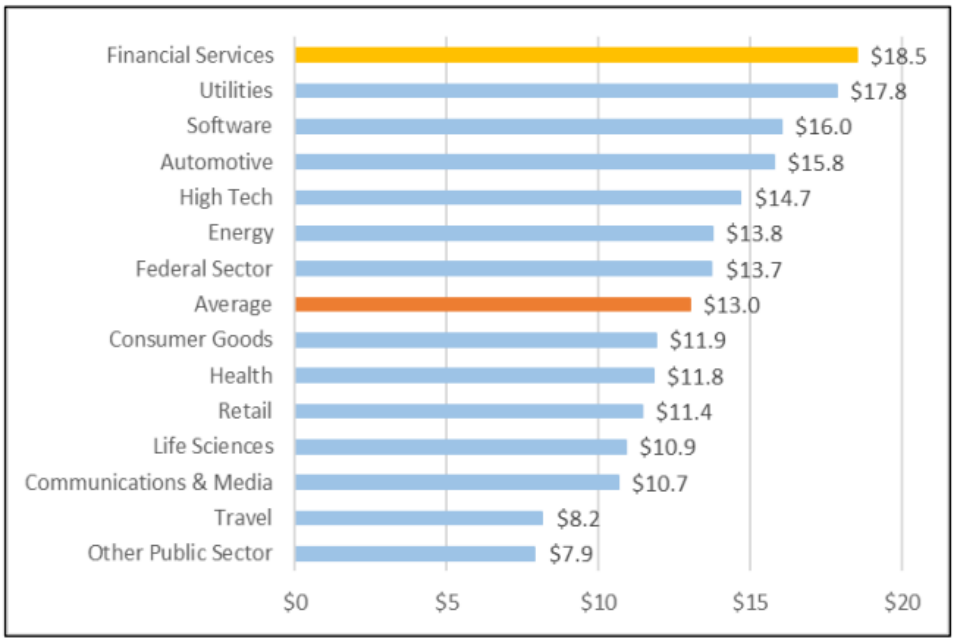

Figure 9.1: Costs of Cybercrime Across Sectors Source: Figure created by CRS, adapted from Accenture, Unlocking the Value of Improved Cybersecurity Protection, July 15, 2019.

9.5.1 Cyber Security in Financial Sector Management (CS-FSM):

To prevent unauthorized access to a system, network, or piece of technology, cybersecurity is essential. A corporation needs a dedicated cybersecurity team in today's technologically evolved environment to keep an eye out for potential cyber-attacks and develop countermeasures. Figure 2 shows the components that are crucial to cybersecurity.

Secure payment, user privacy online, antivirus software, firewalls, mobile security, security padlocks, data protection, computer protection, and a particular worldwide shield are all considered to be major components of cybersecurity. Payment security is essential to information security for any firm that handles electronic payments or transactions. As such, businesses should stay up to date on the latest advancements in e-commerce and secure transaction techniques, and seek advice on how to incorporate them into their operations.

Figure 9.2: Essential elements of cybersecurity in financial management. [7]

9.5.2 Financial Sector under Cyber-Attack:

The banking, financial services, and insurance (BFSI) industry is among the most regulated and developed businesses in terms of cybersecurity because of the nature of the data it contains. Digitalization has improved user experience and changed a number of channels. The primary cybersecurity-related trends in the financial services sector are listed in Figure 3.

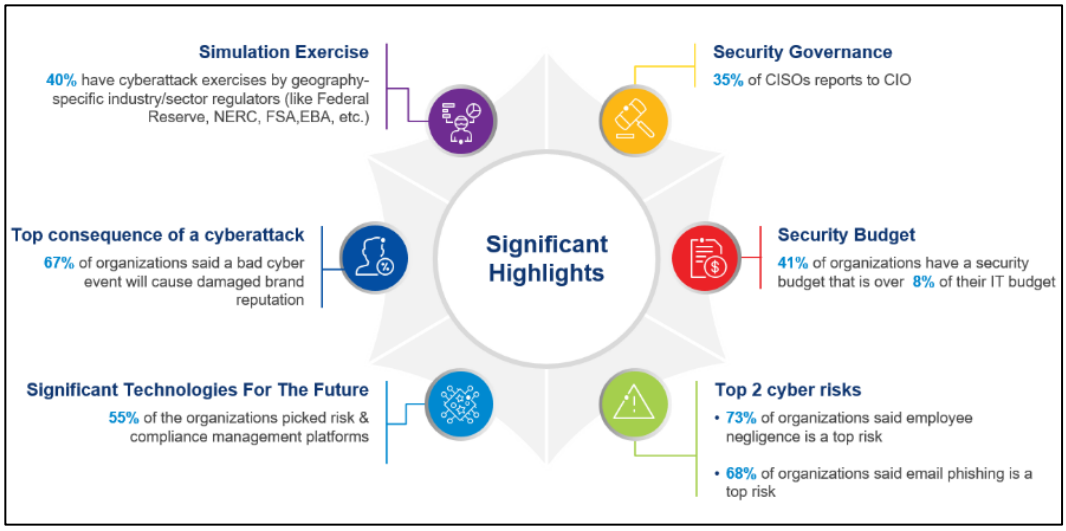

Figure 3: Financial sector under cyber-attack [8]

9.5.3 Attacks are Growing more Sophisticated:

Because cybercriminals are now more skilled at planning precise attacks, the number of breaches has increased. Since they are working in stealth mode, it is harder to find them.

Figure 4 displays the distribution of last year's data breaches by vertical. BFSI and healthcare saw the highest number of breaches. The financial services industry accounted for 20% of major data breaches that were made public.

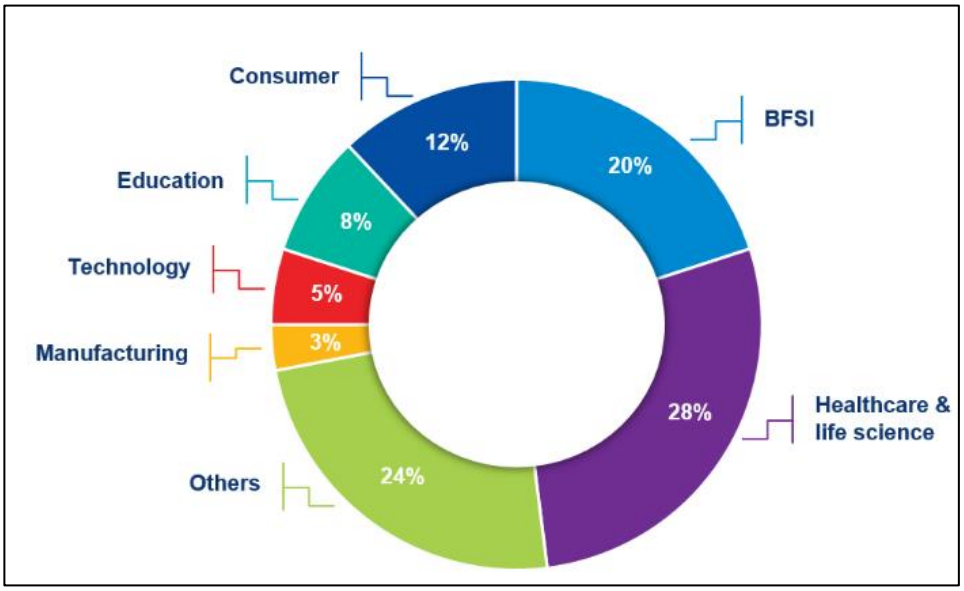

Figure 4: Attacks are growing more sophisticated [9]

9.6 Conclusion:

A wide range of disciplines, including but not limited to computer science and information technology, psychology, economics, organizational behavior, political science, engineering, sociology, decision sciences, international relations, and law, are required to fully understand the complex topic of cyber security. Although policy analysts and others might quickly become engrossed in the technical details, in reality, cyber security is not primarily a technology issue, even though technological solutions are vital.

9.7 References:

1. Uddin, Md Hamid and Ali, Md Hakim and Hassan, M. Kabir, Cybersecurity Hazards and Financial System Vulnerability: A Synthesis of Literature (30 07, 2020).
2. Boddy, C. (2016). Sample size for qualitative research. Qualitative Market Research, 19(4), 426–432. doi:10.1108/ QMR-06-2016-0053.
3. Donohue, W., Afridi, Z., Sokolyuk, K., Bedwell, T., York, E. R., & Salman, A. A. (2020, April). Cashless Society: Managing Privacy and Security in the Technological Age. In 2020 Systems and Information Engineering Design Symposium (SIEDS) (pp. 1-6). IEEE. doi:10.1109/SIEDS49339.2020.9106653.
4. 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).
5. Cawley, J. (2017). The Impact of Cyber Attacks on the Banking System. [Online] [Retrieved December 22, 2017]
6. Meng, W., Zhu, L., Li, W., Han, J., & Li, Y. (2019). Enhancing the security of FinTech applications with map based graphical password authentication. Future Generation Computer Systems, 101, 1018–1027. doi:10.1016/j. future.2019.07.038.
7. Djenna, A.; Harous, S.; Saidouni, D.E. Internet of things meet internet of threats: new concern cyber security issues of critical cyber infrastructure. *Appl. Sci.* **2021**, *11*, 4580.
8. Dasgupta, P.; Collins, J. A survey of game theoretic approaches for adversarial machine learning in cybersecurity tasks. *AI Mag.* **2019**, *402*, 31–43.
9. Humayun, M., Jhanjhi, N. Z., Alsayat, A., & Ponnusamy, V. (2021).