The Vulnerability of the Financial and Accounting System to Cyberattack

Aina Adlina Zainudin[1], Siti Aisyah Basri[2,3], Ahmad Daud Marsam @ Dollah[2,3*], Rozaiha Ab Majid[2,3]

[1]Industri Makanan Jati Sdn Bhd, No. 7, Jalan 22/5, Seksyen 22, Gravitas, 40300 Shah Alam, Selangor, Malaysia

[2]Faculty of Accountancy, Universiti Teknologi MARA Melaka Branch, Alor Gajah Campus, KM26, Jalan Lendu, 78000 Alor Gajah, Melaka, Malaysia

[3]Money Laundering Research Group, Universiti Teknologi MARA Melaka Branch, Alor Gajah Campus, KM26, Jalan Lendu, 78000 Alor Gajah, Melaka, Malaysia

***Corresponding Author**

DOI: https://doi.org/10.47772/IJRISS.2026.100300338

Received: 12 March 2026; Accepted: 18 March 2026; Published: 08 April 2026

ABSTRACT

Many accounting firms are increasingly exposed to cyberattacks due to evolving digital environments and inadequate cybersecurity preparedness. The rapid shift towards remote work has further intensified these risks, contributing to a significant rise in cyber incidents. Financial and accounting institutions are particularly attractive targets due to the sensitive nature of the data they manage, their reliance on technology, and insufficient cybersecurity measures. This conceptual paper synthesises existing literature to examine the key drivers of vulnerability and the potential consequences of cyberattacks. The findings highlight the urgent need for robust cybersecurity strategies to safeguard financial information and ensure organizational resilience.

Keywords: Cybersecurity, Cyberattack, Cybercriminal

INTRODUCTION

Cybersecurity refers to the measures and practices employed to protect data and systems from unauthorised access, cyberattacks, and data breaches (Saeed & Asaad, 2022).

Natalucci et al. (2024) claims that since the COVID19 outbreak, the number of cyberattacks has more than doubled. While the direct losses incurred by firms due to cyberattacks have historically been relatively small, some have borne a far larger cost. For instance, following a significant data breach in 2017 that impacted over 150 million consumers, US credit reporting agency Equifax had to pay more than $1 billion in fines. The frequency of ransomware attacks and the spread of cybercrime-as-a-service (CaaS) provide ongoing difficulty for financial institutions worldwide (Bank Negara Malaysia, 2023).

Many accounting companies are creating opportunities for hackers by failing to properly recognize the upcoming danger of cyberattacks. There has been a 300 percent surge in cyberattacks regardless of the size of the accounting firms as these institutions adjust to a remote workforce (Thompson, 2023).

It becomes much clearer as to why accounting companies and financial institutions are vulnerable to cybersecurity risks as well as the pressing necessity of better cybersecurity policies to safeguard private financial information.

LITERATURE REVIEW

Causes for vulnerability of the financial and accounting system to cyberattack

Scholars have identified several key factors contributing to the vulnerability of financial and accounting systems to cyberattacks. These include the nature of the business, insufficient cybersecurity measures, and a high degree of technological dependence.

The nature of the business

Due to the nature of its underlying business (that's where the money is), the financial sector's significant degree of digitalization, and its global interconnectedness, the industry is a prominent target for cybercriminal activities (Vedral, 2021).

Second, it is related to the type of data financial and accounting sectors deal with—personal financial information of clients.

Chin (2023) stated that targets for cybercriminals are finance companies since they handle and manage enormous volumes of financial data. One important thing to consider is that cybercrime especially targets financial and accounting systems because of their data content. Accounting firms store sensitive client information such as names, addresses, identification documents, and bank account details, which could be utilized for more fraudulent activities (Clinton, 2024).

Lack of cybersecurity measures

Aaron Bugal, Field Chief Technology Officer, APJ, Sophos Group, claims in The Economic Times that many small business owners foolishly think they are protected from cyberattacks just because of their size. However, according to him, small businesses often result in owners and employees having to handle several responsibilities across various job areas inside the organization. Consequently, cybersecurity tends to fall further on the never-ending list of priorities. The absence of proactive cybersecurity measures results in the occurrence of ransomware and other forms of attacks (Bora, 2023).

Furthermore, cybercriminals frequently target small businesses due to the lack of data protection measures implemented by them. Small and medium-sized accounting businesses are easy prey for hackers due to the sensitive nature of the financial information they manage (Carter, 2023).

Technological dependance

This strong reliance on technology brings major weaknesses even as it improves efficiency and innovativeness. Caruana (2016) stated that the widespread adoption of digital technologies has led to a growth in the frequency and magnitude of cyber-attacks, which represent a substantial risk to the security and privacy of customers' data on digital platforms.

Thompson (2022) stated that if one tenant of the cloud services multi-tenant environments is compromised, it could potentially affect others, increasing the risk of cyberattack. Since all accounting firms use the same software, any security hole can be easily exploited. They have an infinite number of possible victims at their fingertips.

Effects of cyberattack

Scholars have found out some of the reason why financial and accounting institutions are often victims of cybercrimes Historically, ransomware has been employed as a tool to demand money, or a "ransom," in return for the decryption keys needed to unlock encrypted data. However, in an effort to put further pressure on the organization to pay the ransom, certain threat actors have also carried out coordinated DDoS (Distributed

Denial of Service) operations. Criminal gangs have started using "double extortion" and "triple extortion" tactics more recently (Conference of State Bank Supervisors, 2023).

Cost of a Data Breach Report 2024 described that the global average cost of a data breach cost in 2024 is USD 4.48 million, which shows a 10% increment over last year and the highest total ever (IBM, 2024).

Kokalitcheva (2021) reported that Sequoia Capital, a venture capital corporation based in the United States, experienced a cybersecurity breach in 2021. The email of an employee was successfully phished, resulting in a data leak. Sequoia Capital notified its investors since there is a possibility that some of their financial and personal data may have been accessed by a third party.

The data breach has the potential to endanger the financial data of both customers and businesses, leading to substantial financial losses.

Hopkins (2017) published in the Guardian the cyber attack faced by Deloitte, one of the world's big four accountancy firms. In the attack the hackers have successfully breached Deloitte's cloud email system due to not having "two-step" verification, granting them unauthorized access to a total of 5 million customer emails. The hackers may obtain crucial client data from the email database, including usernames, passwords, business plans, and health information. In response to a cyber incident, Deloitte implemented its comprehensive security protocol and began an intensive and thorough review including mobilising a team of cybersecurity and confidentiality experts inside and outside of Deloitte (Hopkins, 2017).

Deloitte informed its six most significant clients about the security breach. Accounting company cyber-attacks of this scale result in significant damages, including reputational expenses that can lead to a mass flight of clients and, in the worst situations, the closure of the business (Hopkins, 2017).

Significant data breaches resulting from cyberattacks can have negative effects not just on the operational side of the company but also have legal ramifications for corporate directors should top management be subject to regulatory investigation or lawsuit (Lehenchuk et. al., 2022).

Recovering from cyberattacks takes time as well as money. To know the breach, pay legal fees to negotiate the aftermath, and fix system flaws, institutions have to commit extensively in forensic investigations. When customers perceive that the institution is unable to protect their assets, it can result in a loss of trust, which in turn can lead to a decrease in business and a reduction in market share. Adverse publicity and reduced confidence can also impact the institution's stock prices and market perception, hence worsening financial difficulties. IBM reports that firms incur an additional cost of almost USD 1 million when attackers reveal a breach, as opposed to when the breach is detected internally (Villavicencio, 2023). Hence, it is important to have good internal security measurement in place to detect any unusual activity rather than having to pay more to recover from the attack.

CONCEPTUAL FRAMEWORK

Based on the prior literature, a conceptual framework is developed to illustrate the relationship between drivers of vulnerability, common cyberattack vectors, organizational control gaps, and the resulting impacts on financial and accounting institutions. This framework provides a structured understanding of how vulnerabilities are exploited and how inadequate controls may intensify the consequences of cyberattacks.

Figure 1 Cyberattack Vulnerability Framework

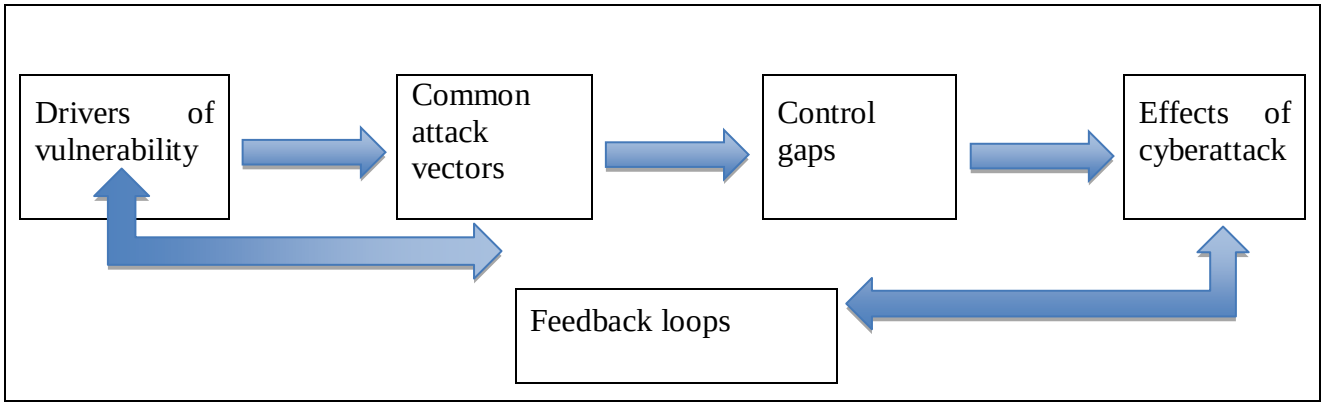

Figure 1 shows that the drivers of the vulnerability leads to common attack ventors facilitated by organizational control gaps resulting in effects of cyberattacks. Severe impacts can trigger improvements in controls.

RECOMMENDATION

Cost of a Data Breach Report 2024 stated that USD 2.22 million is the average cost savings for organizations that used security AI and automation in prevention versus those that did not (IBM, 2024). Given the increasing sophistication of cyber threats, it is essential for financial and accounting institutions to adopt proactive and comprehensive cybersecurity strategies.

Implement strong cybersecurity measures

Alkove (2021) claimed in a Forbes article that multifactor authentication (MFA) is a great method for boosting protection against everyday threats like credential stuffing, phishing attacks and account takeovers. He however suggests that when adopting MFA, organizations should prioritize identifying the strongest and most user-friendly authentication method possible for their organization.

Invest in cybersecurity technologies

Leveraging cybersecurity technologies is crucial for staying ahead of cyber threats. Investing in cybersecurity technology is not merely an optional expense but a fundamental necessity for modern businesses especially for SME businesses. The cost of implementing strong cybersecurity measures is significantly lower than the potential financial, reputational, and operational impacts of a data breach. By adopting a proactive approach to cybersecurity, companies can protect their assets, maintain customer trust, and ensure long-term operational stability. In an era where cyber threats are becoming increasingly sophisticated, the investment in cybersecurity is not just cost-effective; it is crucial for sustainable business success. CPA Credits states that the accounting sector is governed by several regulations and standards, including the General Data Protection Regulation (GDPR) and the Sarbanes-Oxley Act (SOX). The purpose of these regulations is to safeguard the authenticity and privacy of financial information (CPA Credits, 2023). By giving top priority to investing in cybersecurity, accounting companies can guarantee compliance and prevent possible legal and financial consequences. Financial and accounting institutions can take advantage of the advancement of AI for threat detection. AI technologies can analyze vast amounts of data to identify patterns and any anomalies in the financial system that may indicate a threat.

In addition, The Access Group recommends that accounting and financial firms allocate resources to internal cybersecurity in order to guarantee solid safeguards for data. This includes implementing IT controls, enforcing strict access controls, maintaining accurate records (e.g. incident response plans), and obtaining appropriate cyber insurance such as business or cybersecurity insurance (The Access Group, 2023).

Employee awareness

Abdullahel (2023) emphasizes the need for employee awareness and training programs to cultivate a security conscious culture within accounting firms. This should cover topics such as recognizing phishing emails, secure password practices, social engineering awareness, and the importance of data protection in the accounting environment. Accounting professionals and organizations can fortify their defenses by studying real-life case studies and implementing recommended cybersecurity measures reduce the chances of cyber-attacks.

Table 1 below summarizes the key vulnerabilities identified in this study and the corresponding control measures that organizations may implement to mitigate cyber risks.

Table 1: Summary of Key Vulnerabilities and Recommended Controls

Key Vulnerabilities	Recommended Controls
Nature of the business	Implement strong data protection policies, encryption, and strict access controls to safeguard sensitive information.
Lack of cybersecurity measures	Adopt comprehensive cybersecurity frameworks, including multi-factor authentication (MFA), firewalls, and regular security audits.
	Invest in advanced cybersecurity technologies such as AI-based threat detection and real-time monitoring systems.
Technological dependence	Strengthen system security through regular updates, patch management, and secure cloud configurations.
	Conduct regular cybersecurity training and awareness programmes to foster a security-conscious culture.

CONCLUSION

In conclusion, financial and accounting institutions remain highly susceptible to cyberattacks due to structural and technological factors. These attacks can result in significant financial losses, operational disruptions, and reputational damage.

To address these challenges, organizations must strengthen their cybersecurity frameworks through continuous investment in technology, enhanced internal controls, and increased employee awareness. A proactive and integrated approach to cybersecurity is essential to safeguard sensitive financial information and ensure long-term organizational sustainability.

Limitation of the study

This paper is a conceptual paper that uses previous literature as a source of content analysis. This paper analyses cyberattacks from the point of view of the causes for vulnerability of the financial and accounting system to cyberattack, the effects of cyberattack and the recommendation to diminish cyberattack. This paper is literature based and does not provide primary empirical testing.

ACKNOWLEDGEMENTS/FUNDING

The authors would like to acknowledge Universiti Teknologi MARA Melaka for providing a grant for this study with grant reference no: 600-TNCPI 5/3/DDN (4) (004/2024)

REFERENCES

1. Abdullahel, M. K. (2023). Securing Financial Information in the Digital Realm: Case Studies in Cybersecurity for Accounting Data Protection. American Journal of Trade and Policy, 10(1). https://doi.org/10.18034/ajtp.v10i1.659

2. Alkove, J. (2021, January 29). Nail the basics of cybersecurity with multifactor authentication (MFA). Forbes. https://www.forbes.com/sites/forbestechcouncil/2021/01/29/nail-the-basics-of-cybersecurity-with-multifactor-authentication-mfa/
3. Bank Negara Malaysia. (2023). Financial stability review – Second half 2023. Bank Negara Malaysia. https://www.bnm.gov.my/documents/20124/13790687/fsr23h2_en_book.pdf
4. Bora, G. (2023, July 11). SMEs have to wake up to the need to make cybersecurity a top priority. The Economic Times. https://economictimes.indiatimes.com/small-biz/security-tech/security/smes-have-to-wake-up-to-the-need-to-make-cybersecurity-a-top-priority/articleshow/101657024.cms?from=mdr
5. Caruana, J. (2016). Financial inclusion and the fintech revolution: Implications for supervision and oversight [Speech transcript]. Bank in International Settlements. https://www.bis.org/speeches/sp161026.htm
6. Chin, K. (2023, August 21). Why is the finance sector a target for cyber attacks? UpGuard. https://www.upguard.com/blog/finance-sector-cyber-attacks
7. Clinton, C. (2024, February 25). Cyberattacks on the rise for accountancy firms. Naq Cyber. https://www.naqcyber.com/blog/cyberattacks-on-the-rise-for-accountancy-firms
8. CPA Credits. (2023, September 7). Cybersecurity and the Accounting Industry. CPA Credits. https://cpacredits.com/resources/cybersecurity-and-the-accounting-industry/
9. Conference of State Bank Supervisors. (2023). Ransomware: Lessons learned by banks that suffered an attack. Conference of State Bank Supervisor. https://www.dob.texas.gov/sites/default/files/files/Bank-Trust-Companies/Ransomware-Lessons-Learned-Banks.pdf
10. Hopkins, N. (2017, September 25). Deloitte hit by cyber-attack revealing clients' secret emails. The Guardian. https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails
11. IBM. (2024). Cost of a data breach report 2024. https://www.ibm.com/reports/data-breach
12. Carter, W. J. (2023, October 30). The crucial role of cybersecurity for accounting firms. AICPA & CIMA. https://www.aicpa-cima.com/professional-insights/article/the-crucial-role-of-cybersecurity-for-accounting-firms
13. Kokalitcheva, K. (2021, February 19). Scoop: Sequoia Capital says it was hacked. Axios. https://www.axios.com/2021/02/20/sequoia-capital-says-it-was-hacked
14. Lehenchuk, S., Vygivska I., & Hryhorevska, O. (2022). Protection of accounting information in the conditions of cyber security. Problems of Theory and Methodology of Accounting, Control and Analysis, (2(52), 40–46. https://doi.org/10.26642/pbo-2022-2(52)-40-46
15. Natalucci, F., Qureshi, M. S. & Suntheim, F. (2024, April 9). Rising cyber threats pose serious concerns for financial stability. IMFBlog. https://www.imf.org/en/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability
16. Saeed, V. A. & Asaad, R. R. (2022). Cyber security threats, vulnerability, challenges with proposed solution. Applied Computing Journal, 2(4), 227-244. https://doi.org/10.52098/acj.20226
17. The Access Group. (2023, March 2). Cybersecurity for accounting firms. The Access Group. https://www.theaccessgroup.com/en-au/blog/act-cybersecurity-concerns-accounting-firms/
18. Thompson, J. (2022, May 16). Why are accountancy firms targets for cyber attacks? North West Cyber Resilience Centre. https://www.nwcrc.co.uk/post/why-are-accountancy-firms-targets-for-cyber-attacks
19. Vedral, B. (2021). The vulnerability of the financial system to a systemic cyberattack. NATO CCDCOE Publications, Tallinn, 95-110. https://ccdcoe.org/uploads/2021/05/CyCon_2021_Vedral.pdf
20. Villavicencio, S. (2023, July 25). What's new in the 2023 Cost of a Data Breach report? [Online forum post]. Security Global Forum. https://community.ibm.com/community/user/security/blogs/sarah-dudley/2023/07/25/costofadatabreach2023