UNVEILING THE PERILS AND CATASTROPHIC VULNERABILITIES OF CYBER SECURITY ATTACKS IN ACCOUNTING

*Marjan Mohd Noor[1], Norshimah Abdul Rahman[1]

[1]Faculty of Accountancy, Universiti Teknologi MARA, Cawangan Perlis
Corresponding author: marjan@uitm.edu.my

The field of cyber security is indeed constantly evolving, with new challenges and threats every year. It is crucial in the cyber realm, which is an entity made up of bits, to both protecting and enabling the defence of secret data and information. Using cutting-edge digital technology and their extraordinary, interconnected capabilities, cyber threat attacks become a reality. As a result, the term "cyber security" can be used to refer as a body of knowledge about the technologies, procedures, and practises used to safeguard computer systems, networks, or programmes as well as data stored in cyberspace against assault, damage, or unauthorized access (Li & Liu, 2021).

According to the Canadian Centre for Cyber Security (2022), the various kinds of cyber threats are becoming more sophisticated and threat actors are using various techniques that are difficult to detect. Survey conducted by the Office for National Statistics (ONS) for the year ending March 2022, compared to other crimes, people in England and Wales are most affected by fraud or cyber offences (ONS, 2022). Compared to the year ending March 2020, the number

of fraud offences increased by 25% (to 4.5 million offences), mainly due to a significant increase in "advance fee fraud" and "consumer and retail fraud". Computer misuse has increased by 89% (to 1.6 million offences) compared to the fiscal year ending March 2020, due to a sharp increase in offences related to unauthorized access to personal data (hacking) (ONS, 2022).

However, data is increasingly becoming a target for cybercriminals across the region, and Malaysia is no exception. With nearly four thousand reports of cyber threat incidents reported to the Cyber Security Malaysia through the Malaysia Computer Emergency Response Team (MyCERT) in 2022, online frauds were the most commonly reported cyber threats, followed by malicious codes (Statista Research Department, 2023). When analysing the impact of the adoption of cutting-edge digital technologies on the changes taking place in today's business organizations, it is important to consider the intrinsic complexity of all the systems, devices, and networks used to perform the relevant tasks as well as other professional practices. As the rate of cyber threats increases and may affect many areas of business of all sizes, there is no doubt the threat actors are looking at the accounting profession as their potential target (Salman, 2020). According to Gary Salman (2020), a CEO of Black Talon Security (specializing in business cyber security) reports that since the start of the COVID -19 pandemic, cyber-attacks on accounting firms have increased by 300%. This is because this professional sector is already vulnerable to cybercrime and is struggling to cope with the difficulties of remote working (Salman, 2020). Due to the increasing threats and risks to which accounting systems and financial data are exposed, accounting cyber security must be a top priority (Prince, 2022).

Cybersecurity Automation Team (2023) defines an accounting cyber security as a collection of procedures, controls, and tools aimed at preventing unauthorised access, cyberthreats, data breaches, and other potential risks to accounting systems, financial data, and related information. In order to secure the confidentiality, integrity, and accessibility of accounting data, security controls, protocols, and policies must be put into place (Tierney, 2021). Accounting cyber security aims to safeguard financial data, uphold the privacy of sensitive information, adhere to legal obligations, reduce risks, and prevent unauthorized activities that could compromise the accuracy and reliability of accounting procedures and financial reports. Hackers are aware that businesses with insecure systems that contain sensitive financial data and expose the data to cyber criminals can be an easy target as cyber-attacks increase. Thus, the cyber security in accounting is vital as its practices ensure the protection of company's sensitive financial data, not just for the sake of compliance but also for the safety of company's clients who have put their trust on the company with their financial, personal, and professional information (Lehenchuck et al., 2022).

However, accounting faces a variety of challenges as it deals with the most valuable financial data that is highly likely to be breached (Vasilesky, 2023). The potential perils and the corresponding vulnerabilities posed by cyber security attacks on accounting firms can be catastrophic (Yap, 2023; Politzer, 2020). The cyber security breaches targeting accounting firms can undoubtedly result in calamitous outcomes, as these firms handle extremely sensitive financial and personal data. Even though the topic of cyber security in accounting is evolving, with new threats and risks emerging every day, familiarizing ourselves with several conceivable hazards and the corresponding vulnerabilities of accounting cyber security attacks including rising of data breaches, ransomware, phishing attacks, and legal consequences is a good place to start (Alawida et al., 2022).

Professional service accounting and auditing firms retain vast amounts of financial information, including tax records, payroll data and financial statements. They are often seen as attractive targets for hackers. This is mainly because they have a wealth of confidential data, and their data security measures are considered less advanced compared to financial services and healthcare sectors (Peacock, 2019). There are several factors have played a role in data breaches. These include cases such as an employee may click dubious Uniform Resource Locator (URL) links provided in unsolicited text messages or unwittingly providing security information during a phishing attack, introducing malware through a third-party system, or neglecting to update software, allowing vulnerabilities to be exploited (De Groot, 2023). Vulnerabilities encompass weak and inadequate passwords, unpatched software, and insufficient encryption may lead to identity theft, financial fraud, and reputational damage for both the firms and their clients.

Ransomware is a type of malicious software or also known as malware that encrypts files and data, rendering them inaccessible until a ransom is paid to unlock and decrypt them (Gillis & Lutkevich, 2021). Accounting firms can be extremely targets for ransomware attacks due to their significant potential impact. Ransomware is developed with the intention of gaining control over computers, networks, files, and sensitive data by encrypting files and preventing the owners access to them. Afterwards, usually the attacker demands payment, often in anonymous cryptocurrencies such as Bitcoin, to restore access to these files. This situation probably disrupts company's business operations and lead to significant financial losses. Unsecured remote desktop services are one of the vulnerabilities of ransomware. Basically, remote desktop services allow users to access a computer or network from a remote location. If these services are not properly secured, they can become a gateway for cybercriminals as the attackers can exploit weak or default passwords, open ports or known vulnerabilities in the service's software.

America Cyber Security and Infrastructure Security Agency (2021) defines phishing as a form of social engineering attack. Phishing is a common method used by cybercriminals to trick people into divulging confidential information or downloading malware. Accounting firms are an attractive target because they handle valuable financial data. Attackers send fraudulent emails that appear legitimate, often posing as trusted institutions such as banks, tax authorities or customers. Employees may be tricked into clicking on malicious links or downloading malicious attachments. In some cases, attackers specifically tailor their phishing attempts to employees of accounting firms. They conduct research to gather information about the target, such as their role, duties and contacts. This allows them to create highly convincing emails that are more likely to be opened. Accounting firms have to deal with a high volume of emails and messages every day. This sheer volume can make it difficult for staff to thoroughly review each message, increasing the likelihood of inadvertently interacting with malicious content. Although companies implement security measures and provide cyber security training, human error remains a major factor in security breaches. Even trained employees occasionally make mistakes and click on malicious links or unintentionally download harmful attachments.

The Professional Concepts Insurance Agency (2022) highlighted that accounting firms may face significant legal consequences such as client lawsuits and reputational damage if they fail to adequately protect sensitive data. These legal consequences can arise from a variety of sources, including clients and regulators. When accounting firm works with a client, there is often a contractual agreement that sets out the firm's obligations to protect sensitive data. If the

firm does not comply with these obligations, it may be in breach of contract, which makes it liable for damages under the contract. While clients can also bring claims for negligence on the part of the accounting firm. They may argue that the firm failed to take reasonable steps to protect their financial data, resulting in a data breach. If negligence is proven, the firm can be held for the client's financial losses. In the case of significant data breaches affecting multiple clients, affected parties may join together and bring to file class-action lawsuits against the accounting firm. These lawsuits can lead to significant financial liabilities for the firm. The legal consequences go beyond financial damage. A data breach can damage the reputation of an accounting firm. Clients may lose confidence in the firm's ability to protect their data, leading to loss of business and difficulty in attracting new clients.

In summary, the potential perils of cyber security attacks on accounting firms are multifaceted, ranging from financial loss and reputational damage to legal and regulatory consequences. It is critical for accounting firms to prioritize cyber security to protect their clients, operations and reputation. Investments in cyber security should be viewed as a proactive strategy that accounting firms must prioritise especially in cyber security measures including robust data encryption, employee training, and compliance with relevant data protection regulations. While these investments may come at a cost, they are an essential part of modern business operations, especially for accounting firms that deal with sensitive financial data. This investment strategy is to ensure the firm's long-term resilience and success in an increasingly digital and connected world. In accounting, where trust and accuracy are paramount, cyber security is the foundation on which that trust is built and maintained.

REFERENCES

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey, *Journal of King Saud University – Computer and Information Sciences, 34*(10), 8176 – 8206.

America Cyber Security and Infrastructure Security Agency. (2021, February 1). *Avoiding social engineering and phishing attacks*. https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks

Canadian Centre for Cybersecurity. (2022, October 28). *An introduction to the cyber threat environment*. https://www.cyber.gc.ca/en/guidance/introduction-cyber-threat-environment

Cybersecurity Automation Team (2023). *What is cybersecurity in accounting*. https://www.cybersecurity-automation.com/what-is-cybersecurity-in-accounting/

De Groot, J. (2023, May 5). 4 steps to prevent phishing attacks (According to 33 experts). *Fortra*. https://www.digitalguardian.com/blog/phishing-attack-prevention-how-identify-prevent-phishing-attacks

Gillis, A. S., & Lutkevich, B. (2021, December). *Ransomware*. https://www.techtarget.com/searchsecurity/definition/ransomware

Lehenchuck, S., Vygivska, I., & Haryhorevska, O.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.

Li, Q., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments. *Energy Reports, 7*, 8176 – 8186.

Office for National Statistics (ONS). (2022, September 26). *Nature of fraud and computer misuse in England and Wales: year ending March 2022*. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2022

Peacock, I. (July, 2019). How can your practice defend itself against a possible cyber incident? *ACCA Think Ahead*. https://www.accaglobal.com/gb/en/technical-activities/technical-resources-search/2019/july/Cyber-risks-accountancy-firms-exposure.html

Politzer, M. (2020, March 16). Top cyberthreats targeting accounting firms. *Journal of Accountancy*. https://www.journalofaccountancy.com/newsletters/2020/mar/top-cyberthreats-accounting-firms.html

Prince, S. (2022, November 17). 5 Cybersecurity challenges in the accounting industry and how to overcome them. *Tech Rockstars*. https://www.techrockstars.com/security/5-cybersecurity-challenges-in-the-accounting-industry-and-how-to-overcome-them/

Professional Concepts Insurance Agency. (2022). *Accounting firms biggest risks*. https://www.pciaonline.com/news/accounting-firms-biggest-risks

Salman, G. (2020, August 24). The rise of cybercrime in the accounting profession continues. Accounting Today. https://www.accountingtoday.com/opinion/the-rise-of-cybercrime-in-the-accounting-profession-continues

Statista Research Department. (2023, February 27). *Number of cyber threat incidents reported to cyber security Malaysia 2022, by type of crime*. https://www.statista.com/statistics/1043272/malaysia-cyber-crime-incidents/

Tierney, M. (2021, July 26). *Data security explained: Challenges and solutions*. https://blog.netwrix.com/2021/07/26/data-security/

Vasilevsky, H. (2023, February 23). Accounting cybersecurity: Common cyber threats for accountants and how to avoid them. *Synder*. https://synder.com/blog/cybersecurity-for-accountants-the-most-common-threats-and-solutions/

Yap, V. (2023, March 29). Cybersecurity for accounting firms: What are the biggest concerns? Access. https://www.theaccessgroup.com/en-my/blog/act-cybersecurity-concerns-accounting-my/