UNIVERSITI TEKNOLOGI MARA

Fakulti Perakaunan

FIELD REPORT

PAC 671

FACULTY OF ACCOUNTANCY

UNIVERSITI TEKNOLOGI MARA

UiTM CAWANGAN TERENGGANU

NAME : SHAFEEQ BIN SHAZALI

STUDENT ID : 2020847232

SUPERVISOR (UiTM) : EMIZA BINTI TAHAR

TABLE OF CONTENTS

SECTION A

1.0 Introduction

Zalghani & Co is a wholly owned and managed by Malaysian Bumiputra which offer service to the public and private sectors, whether big or small companies such as auditing and assurance, tax advisory and compliance and corporate and consultation services. The firm is staffed with professionals who are well versed in their fields of expertise gained from many years of job experience in both operational and consultation perspectives. T

he missions of the firm are to provide a quality service and become close partner to the clients, be reputable and recognised as professional chartered accountant. The objective of the firm is to perform the highest professional standards required by law and comply with the guidelines provided by the Malaysian Institute of Accountants (MIA) and other relevant professional bodies. While being registered with Ministry of Finance, the firm also a licensed tax agent beside being a licensed auditor.

The workplace environment at Zalghani & Co is very comfortable. I have my own personal desk and computer that I can use to do my job. The main reasons why I choose Zalghani & Co is because the firm has a lot of expertise with years of experience which I can learn a lot from them. The main office is located in Dataran Palma at Ampang, Selangor and the second branch is located in Bandar Baru UDA at Johor Bahru, Johor.

My practical training' duration are 6 months which starts from 4 March 2024 until 23 August 2024. I was placed in the Audit Department. The benefits provided by Zalghani & Co to me are allowance for travel or outstation for work and also a professional supervisor who could teach me very well.

2.0 Summary of Work Done

Audit Division

Firstly, I do the statutory audit. This is to ensure that all companies comply with the requirements of the Companies Act 2016 and professional accounting standards in Malaysia. I need to cross check all the information of the companies in details. For example, the registration of members, directors, managers, and secretaries. I need to check how much is the amount of share capital that the company actually have and summary of minutes. I have done the statutory audit for 9 companies during my internship.

Next, I also learn about audit field work. This means that I need to go to the company's office to do the audit. For example, I went to Ideation Sdn Bhd with my officemate to do the audit. I started by taking all the supporting documents that are needed as the audit evidence for my working paper later. If the documents cannot be found, I need to ask the client to explain or provide an explanation about the document. Some of the supporting documents that I take with me are the invoices, payment vouchers, official receipt, tenancy agreements and confirmation slip.

Lastly, I learn how to audit the companies. Before starting the audit, I had a talk about the accounting, information, and business nature of the audited company with the management team and other audit department colleagues since I needed to get a clear understanding of the entity's operation. Increasing the amount of data, I enter for the audit procedures will be really helpful. After that, in order to fully comprehend the entity and its surroundings, I will carry out the risk assessment and find any serious misstatements. It aids auditors in identifying potential and expected risks. Next phase, which is conducting an audit of the subsequent items on the balance sheet and profit and loss item. After that, I audit the asset via random sampling method. Any asset that is above materiality level should be highlighted in the audit working paper. Following the completion of the audit work, I go on to the draft report, where I create a report based on the audit work that was accomplished. In order to decide whether to offer an opinion—whether it be unqualified, qualified, a disclaimer, or an adverse opinion—I will confer with the supervisor. After that, our team leader will examine the report to see if it has any errors. If there is an error, I will make the necessary changes using the team leader's highlighted list. Once the audit work and draft report are completed, I must send the client a copy of the audit report, engagement letter, and management representation letter so that the client's director or directors can sign and approve the audit report that the auditor has prepared and finished.

3.0 Strengths and Weaknesses of Training

Strengths of Training

One of the numerous benefits of my internship experience was the chance to develop skills that would help me in my future profession and obtain real-world information related to my topic of study. Interns can gain expertise in areas that are not often included in academic programmes, such as communication, teamwork, and problem-solving. These are the kinds of skills that some interns might pick up while working for the company. Students can gain job experience and build abilities that are essential to a particular vocation through skill-development internships.

Next, those who participate in internships also stand a strong chance of growing their professional network within the industry of their choice. For those who have decided to get into the sector as their career, this is a fantastic opportunity. Making relationships with mentors, coworkers, and subject matter experts during an internship can open doors for future employment opportunities and insightful recommendations.

Last but not least, one advantage I see from my internships is that students can gain important insights about who they are and what kind of careers they want to pursue. Through actual experience in a range of environments, internships give students a window into their own interests, shortcomings, and talents. People can gain practical experience in a field linked to their interests and future aspirations through internships. Through internships, students can explore a range of industries and careers and gain a deeper understanding of their interests and aptitudes.

Weaknesses of Training

One of the weaknesses I've encountered during my internship training is a lack of accountability. Some interns could be placed in situations where they aren't given sufficient independence or responsibility to begin important activities or make a significant contribution to important decision-making processes. As a result, it could be harder for individuals to show off their abilities and contribute significantly.

Furthermore, although some internships provide mentorship opportunities, not all internships receive ongoing guidance and support from seasoned professionals. Not every intern gets ongoing guidance and support from seasoned experts. If their supervision is insufficient, interns risk missing out on important feedback and opportunities for personal growth.

4.0 Self-Reflection

I get a lot of advantages and experience from this 24-week practical training that helps me apply what I've learnt in the classroom to the real world of the workplace. I managed to add more value to myself after completing my industrial training at Zalghani & Co, which helped me become the employee that the employer was looking for when I graduated. It is crucial that I am exposed to this as a student at an early age in order to increase my marketability and land the job of my dreams.

Giving undergraduate students the chance to recognise, understand, and practise in a real-world working setting is the main objective of industrial training. The industrial training period is an undergraduate's only chance to obtain experience. I'm glad to report that I joyfully and successfully finished my industrial training, improving as a person from my student days.

I obtained some worthwhile experiences and learned some worthwhile lessons from my internship at Zalghani & Co. I've discovered that since it's my job as an auditor to make sure that my clients' accounts are accurate and free of errors, I have to work meticulously. Moreover, I could build up my confidence level significantly to communicate with one another. This is because I have low self-esteem when talking to new people that I do not know. However, everyone at Zalghani & Co has always encouraged me and help me in improving my lack of confidence.

Finally, I've always recognised the importance of having Microsoft Excel abilities in the business. Conversely, this internship helped me recognise how inadequate my Microsoft Excel skills were. I had to utilise a lot of Excel to finish the audit process. I was able to apply some of my senior abilities as a result, and I'll keep learning more.

SECTION B

NAVIGATING THE CYBERSECURITY MINEFIELD: HOW DATA BREACHES CHALLENGE THE ACCOUNTING FIRM

1.0 Issue and Problem Statement

In today's digital age, the accounting firm faces unprecedented challenges in safeguarding sensitive financial information from cyber threats. The increasing use of digital technologies among companies has emphasized the importance and role of cybersecurity as a new risk management dimension, not least because cyber threats and risks have attracted significant attention from the public (*Amir et al., 2018; Li et al., 2018*). Recent studies suggest that over the course of just a few years, cybersecurity has grown into one of the most significant risk challenges facing every type of organization and society (*Islam et al., 2018; Kahyaoglu and Caliyurt, 2018*). With the rise of sophisticated hacking techniques and the increasing prevalence of data breaches, the accounting field has become a favorable cybersecurity minefield. Accounting firm must navigate these cybersecurity threats while maintaining the integrity and confidentiality of client data. There are several issues for the accounting firm related to cyber threat.

2.0 Discussion

1. **The issue of threat to data integrity**

   Data confidentiality and integrity are fundamental pillars of information security that play a crucial role in safeguarding sensitive and valuable data from unauthorized access, disclosure, or tampering *(Anyanwu et al., 2024*). The threat to data integrity is a significant concern for accounting firms due to the nature of the data they handle. Data integrity involves maintaining and ensuring the accuracy, consistency, and reliability of data throughout its lifecycle. It involves preventing unauthorized alterations, deletions, or corruption of data, thereby preserving its reliability for decision-making processes (*Duggineni, 2023*). Cyberattacks, such as data breaches and ransomware, directly threaten this integrity. When an accounting firm's data is compromised, it can lead to the alteration or destruction of sensitive information, which can have catastrophic consequences for both the firm and its clients. For example, if a cybercriminal gains access to an accounting firm's database and alters financial records, it can result in incorrect financial statements and reports.

This not only affects the firm's operations but also the decision-making processes of their clients, who rely on accurate data for their financial planning and regulatory compliance. Furthermore, ransomware attacks can encrypt critical data, rendering it inaccessible until a ransom is paid. Even if the ransom is paid, there is no guarantee that the data will be restored to its original state, or that the attackers haven't already exfiltrated sensitive information.

2. **The issue of legal and regulatory compliance**

As organizations navigate a landscape where data breaches and financial fraud pose significant threats, the importance of regulatory compliance cannot be overstated (*Kafi and Akter, 2023*). Legal and regulatory compliance is another critical issue for accounting firms, especially in the context of cybersecurity. As technology continues to advance, the need for comprehensive regulatory frameworks governing financial practices and digital security has never been more crucial (*Kumar et al., 2021*). Accounting firms must adhere to various data protection laws and regulations, such as Malaysia's Personal Data Protection Act (PDPA), the General Data Protection Regulation (GDPR) in Europe, and other relevant local and international standards. These regulations mandate stringent requirements for the collection, storage, and processing of personal and financial data. Non-compliance with these regulations can result in severe penalties, including hefty fines and legal actions, which can have a substantial financial impact on the firm. For instance, under the GDPR, fines can be as high as 4% of the firm's annual global turnover or €20 million, whichever is greater. Additionally, failing to comply with data protection regulations can lead to increased scrutiny from regulatory bodies and damage the firm's reputation.

3. **The issue of reputational damage**

Reputational damage is a significant risk that arises from cybersecurity breaches. For accounting firms, reputation is one of their most valuable assets, built on the trust and confidence of their clients. A data breach can severely undermine this trust, leading to a loss of clients and difficulties in acquiring new ones. When clients' sensitive financial information is compromised, they may feel betrayed and insecure about the firm's ability to protect their data. Unauthorized alterations or errors in financial records can have severe consequences, impacting the trust of clients and compliance with regulatory standards (*Liaw et. al., 2021*). The negative publicity

surrounding a data breach can also deter potential clients and partners. News of a breach can spread quickly, and the perception of poor security practices can have long-term repercussions for the firm's reputation. For instance, if an accounting firm is known to have experienced multiple data breaches, it may be viewed as a high-risk partner, leading to a decline in business opportunities and collaborations. Ultimately, reputational damage in cyber security can extend beyond the immediate aftermath, affecting a company's competitiveness and long-term viability (*Institute of Data, 2023*).

4. **The issue of operational disruption**

Operational disruption is a critical issue that arises from cybersecurity breaches, particularly for accounting firms that rely heavily on digital tools and technologies for their daily operations. Many organizations have created some level of resilience but have not adequately tested their resistance to disruptions (*PricewaterhouseCoopers, 2020*). Cyberattacks, such as ransomware, phishing, and malware, can significantly disrupt business activities by compromising critical systems and data. When an accounting firm falls victim to such an attack, it can experience a halt in its operations, leading to delayed services, financial losses, and client dissatisfaction. For example, ransomware attacks can lock firms out of their systems, making it impossible to access essential financial data and perform routine tasks. This disruption can last for days or even weeks, depending on the severity of the attack and the firm's preparedness to respond. During this time, clients may experience delays in receiving financial reports, tax filings, and other important services, which can damage the firm's reputation and client relationships. Phishing attacks, which often target employees with deceptive emails, can also lead to significant operational disruptions. This form of cybersecurity accounting attack involves deceptive tactics, often through emails, to trick individuals into divulging confidential information (*Rana, 2023*). If an employee unknowingly clicks on a malicious link or downloads an infected file, it can compromise the firm's network, leading to data breaches and system downtime. This not only affects the firm's ability to deliver services but also requires extensive resources to investigate and remediate the breach.

3.0 Recommendation

To navigate the cybersecurity minefield and mitigate the impact of data breaches, accounting firms should consider the following recommendations:

1. Invest in robust cybersecurity measures to help maintain data integrity successfully.

Investing in robust cybersecurity measures is crucial for maintaining data integrity in accounting firms. This involves deploying advanced security technologies, such as firewalls, intrusion detection systems, and encryption protocols, to protect sensitive financial data from unauthorized access and cyber threats. By implementing robust cyber security models, organisations can ensure their data's confidentiality, integrity, and availability (*Institute of Data, 2024*). Regular security audits and vulnerability assessments should be conducted to identify and address potential weaknesses in the firm's IT infrastructure. Implementing multi-factor authentication (MFA) can further enhance security by requiring multiple verification steps before granting access to sensitive data.

This adds another layer of security, making it more difficult for unauthorized people to obtain access (*FM Contributors, 2023*). Additionally, accounting firms should adopt data loss prevention (DLP) solutions to monitor and control data transfer, ensuring that sensitive information is not leaked or misused. Cloud-based security services can provide continuous monitoring and real-time threat detection, offering an added layer of protection against cyberattacks. By investing in these comprehensive cybersecurity measures, accounting firms can ensure the accuracy, consistency, and reliability of their data, thereby maintaining data integrity and safeguarding client trust. Furthermore, staying informed about the latest cybersecurity trends and emerging threats is essential for adapting and enhancing security protocols, ensuring that the firm remains resilient against evolving cyber risks.

2. Implement comprehensive data protection to help comply with legal and regulatory standards.

To comply with legal and regulatory standards, accounting firms must implement comprehensive data protection strategies. This includes adhering to regulations such as Malaysia's Personal Data Protection Act (PDPA), the General Data Protection Regulation (GDPR), and other relevant local and international data protection laws. A critical step in achieving compliance is appointing a dedicated data protection officer (DPO) or forming a compliance team to oversee and manage data protection efforts. The firm should establish clear data handling policies, including guidelines for data collection, storage, processing, and disposal. Regular training programs should be conducted to ensure that all employees are aware of these policies and understand their role in maintaining data privacy.

Implementing strong access controls and encryption can prevent unauthorized access to sensitive information, while regular audits and assessments can help identify and rectify any compliance gaps. Plus, maintaining detailed records of data processing activities and conducting impact assessments for high-risk data processing operations can demonstrate the firm's commitment to data protection and regulatory compliance. By implementing these comprehensive data protection measures, accounting firms can mitigate the risk of legal penalties, protect client data, and enhance their reputation as trustworthy and compliant company. Organizations must remain vigilant, continuously adapting their practices to meet evolving regulatory requirements and emerging cyber threats (*hakia, 2019*).

3. Transparent communication with clients to mitigate the issue of reputational damage.

Transparent communication with clients is essential for mitigating reputational damage in the event of a cybersecurity incident. When a data breach occurs, prompt and honest communication can help maintain client trust and prevent the spread of misinformation. Accounting firms should have a crisis communication plan in place that outlines how to inform clients about the breach, the steps being taken to address it, and measures being implemented to prevent future incidents. Companies must communicate promptly with all relevant stakeholders, including customers, employees, investors, and regulators (*Institute of Data, 2023*). It is crucial to provide clients with clear and concise information about the nature of the breach, the potential impact on their data, and any actions they need to take to protect themselves.

Regular updates should be provided as the situation evolves, ensuring that clients are kept informed about the progress of the investigation and remediation efforts. For example, rejuvenate stakeholders' confidence and trust by focusing on breach preparedness, containment, and mitigation strategies (*Lukić, 2021*). Moreover, offering support services, such as credit monitoring or identity theft protection, can demonstrate the firm’s commitment to mitigating the impact of the breach on affected clients. By maintaining transparency and open communication, accounting firms can rebuild trust, reassure clients of their dedication to data security, and preserve their reputation in the long term.

4. Employee training regarding the cyber threats to mitigate the issue of operational disruption.

Employee training is a critical component in mitigating operational disruption caused by cyber threats. As employees are often the first line of defense against cyberattacks, it is essential to equip them with the knowledge and skills to recognize and respond to potential threats. Regular training sessions should be conducted to educate employees about the latest cyber threats, such as phishing, ransomware, and malware, and how to avoid falling victim to these attacks. For example, accountants should undergo regular training sessions which cover the latest cybersecurity threats and defense tactics (*Cybersecurity Training for Accountants: Best Practices and Top Solutions*, 2024). Training should cover best practices for creating strong passwords, identifying suspicious emails and links, and safely handling sensitive information.

Simulated phishing exercises can be an effective way to test and reinforce employees' ability to recognize and respond to phishing attempts. In addition, employees should be trained on the firm's cybersecurity policies and procedures, including how to report security incidents and respond to potential breaches. For example, to properly assess potential risks, accountants and auditors must be familiar with current and new technologies (*Lehenchuk et al., 2022*). By fostering a culture of cybersecurity awareness, accounting firms can significantly reduce the risk of successful cyberattacks and minimize operational disruptions. Continuous education and training ensure that employees stay updated on evolving cyber threats and remain vigilant in protecting the firm's digital assets, thereby maintaining business continuity and client trust.

5.0 Conclusion

In conclusion, accounting firms face considerable challenges in safeguarding sensitive financial data from cyber threats. These challenges have necessitated a robust approach to cybersecurity, incorporating advanced technologies and comprehensive risk management strategies to mitigate potential risks. Cyber threats have emerged as a significant risk dimension for all types of organizations, including accounting firms, due to the rising sophistication of hacking techniques and the increasing frequency of data breaches. The primary issues confronting accounting firms in this regard include threats to data integrity, legal and regulatory compliance, reputational damage, and operational disruptions. Data integrity is fundamental to the reliability and accuracy of financial information. Cyberattacks such as data breaches and ransomware pose direct threats to data integrity, potentially leading to unauthorized alterations or destruction of sensitive information. The preservation of data integrity through robust cybersecurity measures, including advanced encryption and multi-factor authentication, is essential to maintain the accuracy and reliability of financial data. Legal and regulatory compliance represents another critical challenge for accounting firms. Non-compliance not only leads to financial repercussions but also heightens scrutiny from regulatory bodies, potentially damaging the firm's reputation. Implementing comprehensive data protection strategies and appointing dedicated data protection officers are crucial steps toward achieving regulatory compliance. Reputational damage resulting from cybersecurity breaches can have long-lasting effects on an accounting firm's client trust and business opportunities. Clients entrust firms with their sensitive financial information, and a breach can severely undermine this trust, leading to client loss and difficulties in acquiring new clients. Transparent communication and prompt action in the event of a breach are essential to maintain client trust and mitigate reputational damage. Operational disruption, stemming from cyberattacks like ransomware, phishing, and malware, can significantly impact the firm's ability to perform routine tasks and deliver services. Such disruptions can lead to financial losses, delayed services, and client dissatisfaction. Regular employee training on recognizing and responding to cyber threats is crucial to minimizing operational disruptions.

References

1. Amir, E., Levi, S. and Livne, T. (2018), “Do firms underreport information on cyber-attacks? Evidence from capital markets”, Review of Accounting Studies, Vol. 23 No. 3, pp. 1177-1206.
2. Islam, M.S., Farah, N. and Stafford, T.S. (2018), “Factors associated with security/cybersecurity audit by internal audit function: an international study”, Managerial Auditing Journal, Vol. 33 No. 4, pp. 377-409.
3. Kahyaoglu, S.B. and Caliyurt, K. (2018), “Cyber security assurance process from the internal audit perspective”, Managerial Auditing Journal, Vol. 33 No. 4, pp. 360-376.
4. Anyanwu, A., Temidayo Olorunsogo, Temitayo Oluwaseun Abrahams, & Reis, O. (2024, January 21). *DATA CONFIDENTIALITY AND INTEGRITY: A REVIEW OF ACCOUNTING AND CYBERSECURITY CONTROLS IN SUPERANNUATION...* ResearchGate; Fair East Publishers. https://www.researchgate.net/publication/377958939_DATA_CONFIDENTIALITY_AND_INTEGRITY_A_REVIEW_OF_ACCOUNTING_AND_CYBERSECURITY_CONTROLS_IN_SUPERANNUATION_ORGANIZATIONS
5. Duggineni, S. (2023). Impact of Controls on Data Integrity and Information Systems. Science and Technology, 13(2), 29-35.
6. Duggineni, S. S. (2023). Data integrity as a code (DIAC).
7. Kafi, M.A., & Akter, N. (2023). Securing financial information in the digital realm: case studies in cybersecurity for accounting data protection. American Journal of Trade and Policy, 10(1), 15-26.
8. Kumar, S., Biswas, B., Bhatia, M.S., & Dora, M. (2021). Antecedents for enhanced level of cyber-security in organisations. Journal of Enterprise Information Management, 34(6), 1597-1629
9. Liaw, S. T., Guo, J. G. N., Ansari, S., Jonnagaddala, J., Godinho, M. A., Borelli Jr, A. J., ... & Kahn, M. G. (2021). Quality assessment of real-world data repositories across the data life cycle: a literature review. Journal of the American Medical Informatics Association, 28(7), 1591-1599.
10. Institute of Data. (2023, October 17). *How to Manage Reputational Damage in Cyber Security | Institute of Data*. Institute of Data. https://www.institutedata.com/blog/reputational-damage-in-cyber-security/
11. PricewaterhouseCoopers. (2020). *How to plan for and recover from business threats and disruptions: PwC*. PwC. https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/tech-and-operational-resilience.html

12. Rana, A. (2023, November 29). *Step-up your Digital Vigilance: Cybersecurity Strategies for Accounting in 2024*. Cogneesol Blog; Cogneesol. https://www.cogneesol.com/blog/step-up-your-digital-vigilance-cybersecurity-strategies-for-accounting/#:~:text=Malware%20attack%3A%20One%20of%20the,data%20loss%2C%20and%20financial%20damage
13. Institute of Data. (2024, March 12). *Implementing Effective Cyber Security Models | Institute of Data*. Institute of Data. https://www.institutedata.com/blog/implementing-cyber-security-models/
14. FM Contributors. (2023, June 27). *Cybersecurity in Fintech 2023: Protecting Customer Data and Financial Systems*. Financial and Business News | Finance Magnates; Finance Magnates. https://www.financemagnates.com/fintech/data/cybersecurity-in-fintech-2023-protecting-customer-data-and-financial-systems/
15. hakia. (2019, October 9). *Regulatory Compliance and Cybersecurity: Navigating Data Protection Laws and Standards* -. Hakia: Covering All Angles of Technology. https://www.hakia.com/regulatory-compliance-and-cybersecurity-navigating-data-protection-laws-and-standards/
16. Lukić, D. (2021, November 16). *Reputation Management in the Age of Cyberattacks*. Trustsignals.com; Media Orchard LLC. https://www.trustsignals.com/blog/reputation-management-in-the-age-of-cyberattacks
17. *Cybersecurity Training for Accountants: Best Practices and Top Solutions*. (2024, April 8). Practice Protect. https://practiceprotect.com/blog/cybersecurity-training-accountants-best-practices/
18. Lehenchuk, S. F., Vygivska, I. M., & Hryhorevska, 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. https://doi.org/10.26642/pbo-2022-2(52)-40-46