CYBERSECURITY CHALLENGES AND MITIGATION STRATEGIES: EMPOWERING MALAYSIAN SMES AGAINST CYBER RISKS

RABAATUL AZIRA HASSAN
rabaatul@uitm.edu.my

Today's businesses need to recognize the role of information and communication technologies. With the rise of remote working, increased use of the cloud and the integration of AI and IoT, the attack surface has increased significantly, requiring heightened vigilance. Small and medium-sized enterprises (SMEs) have been urged to capitalize on potential business opportunities by taking advantage of new technologies such as cloud computing services (Alahmari & Duncan, 2020). While these technological advances offer numerous benefits and opportunities for growth, they also bring new challenges, particularly cybersecurity threats. This is particularly important for SMEs, considered the least mature and most vulnerable to cybersecurity risks (Sukumar et al., 2023).

The rising number of cyberattacks in Malaysia highlights the growing digital footprint of SMEs. With the adoption of digital platforms, SMEs are becoming more connected to the global digital economy. Malaysian SMEs will likely face more hostile cyber activities as they adapt to the digital environment. Cybercriminals increasingly target SMEs as they gain prominence in the digital economy and sometimes have less robust security measures. According to a study by cybersecurity firm Palo Alto Networks, Malaysian businesses were subject to the most disruptive cyberattacks in the ASEAN region in 2022. The research found that almost a third, 29% to be exact, of these companies experienced a significant increase in incidents, a remarkable 51% increase (The Star, 2023).

The MCMC Network Security Center (MCMC NSC) documented 1653 phishing incidents in 2022 (MCMC, 2023). One of the most popular tactics in 2022 was using a malicious Android package (APK). Phishing is a cyberattack in which cybercriminals use various social engineering techniques to lure or trick people into performing specific actions or revealing sensitive information such as login credentials, financial information or personal data. There are also threats from cyber risks such as hacking, malware, attacks on the e-commerce supply chain and malicious insiders (Barlette et al., 2017; Chidukwani et al., 2022).

This increasing networking leads to greater susceptibility to unlawful acts. Unlike large companies, SMEs face challenges in mitigating cyber risks. The six potential barriers to investing in cybersecurity risk management in SMEs include financial capacity, lack of awareness, SME size, traditional trade, lack of risk standards and overconfidence of decision makers (Alahmari & Duncan, 2021). Due to their limited past exposure and financial constraints, SMEs generally have weaker risk management capabilities. This is because difficult economic conditions strain the budgets of small and medium-sized enterprises.

In addition, SMEs struggle to quantify their risk from cyberattacks due to limited resources and technical expertise. SMEs that invest in data security and governance can capitalize on market opportunities (Chidukwani et al., 2022). It has also been argued that SMEs need more risk culture and awareness. The tight market for IT experts is a significant obstacle to implementing cyber risk management in SMEs (Hoppe et al., 2021).

The study suggests that proactive approaches such as flexible organization, risk management, rapid decision-making and international market entry contribute to sustainable growth (Kulkarni et al., 2023). A risk management approach helps SMEs identify, assess and prioritize cyber risks to mitigate them in a targeted manner. A flexible structure allows SMEs to adapt their cybersecurity plans to evolving threats quickly. Quick decision-making is essential to respond to cyber incidents and implement security measures to minimize the damage. SMEs expanding abroad must proactively assess and manage the cyber risks associated with international market entry to comply with regulatory requirements and protect themselves from region-specific cyber-attacks.

In addition, proactive Cyber Threat Intelligence (CTI) can help mitigate cyber risks by analyzing malicious hacking tools and identifying key hackers, contributing to sustainable growth in cyber risk mitigation (Samtani et al., 2017). SMEs need to take measures to mitigate cyber risks. Otherwise, these risks will cause more problems for businesses if they are not appropriately managed. Adequate cybersecurity boosts SMEs' sales, profits and growth and is essential in mitigating cyber risks. Below are the steps to identify the risk based on the suggestions of Chidukwani et al. (2022).

NIST CSF Function	Category
Identify	Asset management; Risk assessment; Governance and compliance; Responsibilities; Risk Management; Procurement / supply chain risk management; Working with external partners; Recruitment
Protect	Identity management and user access control; Awareness and Training; Data Security; Information protection processes and procedures; Encryption; Maintenance; Patch and change management; Protective technology
Detect	Detection process; Security Incident Event Monitoring (SIEM) & anomalies; Security continuous monitoring
Respond	Response planning; Communications management; Forensics and impact analysis; Incident management; Emergency management; Lessons learnt and continuous improvement
Recover	Disaster recovery (DRP); Business continuity management (BCP); Improvements; Communications

Cyber security is becoming increasingly crucial as Malaysia develops its digital infrastructure and economy. With the increasing prevalence of cybercrime and cyberattacks, small and medium enterprises in Malaysia need to prioritize cybersecurity. The low awareness of cyber security among Malaysian SMEs is a significant obstacle. SMEs also face the challenge of not having the necessary resources, knowledge and expertise, but they need to take measures to minimize cyber risk in the ever-evolving cyber landscape. All businesses, regardless of size, can be exposed to cyber risk. Therefore, SMEs need to create a good security culture and implement awareness and training programs for SMEs to improve their security posture.

In addition, the government also plays a vital role in cybersecurity by ensuring a safe and trustworthy digital environment in which society can flourish and promote economic growth. This means that the government is at the forefront of the nation's cybersecurity initiatives, formulating a comprehensive national cybersecurity strategy with a well-defined execution plan.

References:

Alahmari, A., & Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), pp. 1–5.

Alahmari, A., & Duncan, R. A. K. (2021). Investigating Potential Barriers to Cybersecurity Risk Management Investment in SMEs. 2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), pp. 1–6. https://api.semanticscholar.org/CorpusID:237297132

Barlette, Y., Gundolf, K., & Jaouen, A. (2017). CEOs' information security behaviour in SMEs: Does ownership matter? Systèmes d'information et Management, 22(3), 7–45.

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations. IEEE Access, 10, 85701–85719.

Hoppe, F., Gatzert, N., & Gruner, P. (2021). Cyber risk management in SMEs: insights from industry surveys. The Journal of Risk Finance. https://api.semanticscholar.org/CorpusID:237645879

Kulkarni, M. S., Ashit, D. H., & Chetan, C. N. (2023). A Proactive Approach to Advanced Cyber Threat Hunting. 2023 7th International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), 1–6. https://api.semanticscholar.org/CorpusID:266089111

MCMC. (2023). Cybersecurity Trends: An Eye On Trends and Threats in Malaysia 2023 (Issue 22). https://www.mcmc.gov.my/skmmgovmy/media/General/pdf2/MCMC-MyConvergence-Vol-22.pdf

Samtani, S., Chinn, R., Chen, H., & Nunamaker, J. F. (2017). Exploring Emerging Hacker Assets and Key Hackers for Proactive Cyber Threat Intelligence. Journal of Management Information Systems, 34, 1023–1053. https://api.semanticscholar.org/CorpusID:29826603

Sukumar, A., Mahdiraji, H. A., & Jafari-Sadeghi, V. (2023). Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors. Risk Analysis, 43(10), 2082–2098. https://doi.org/10.1111/risa.14092

TheStar. (2023, September). Study: Malaysia most hit by disruptive cyberattacks in Asean last year. TheStar.