JOURNAL OF GOVERNANCE AND DEVELOPMENT
https://e-journal.uum.edu.my/index.php/jgd

How to cite this article:
Wallang, M., Shariffuddin, M. D. K., & Mokhtar, M. (2022). Cyber security in Small and Medium Enterprises (SMEs): What's good or bad?. *Journal of Governance and Development, 18*(1), 75-87. https://doi.org/10.32890/jgd2022.18.1.5

# CYBER SECURITY IN SMALL AND MEDIUM ENTERPRISES (SMEs):WHAT'S GOOD OR BAD?

**[1]Muslimin Wallang, [2]Mohd Dino Khairri Shariffuddin & [3]Mokhtafizam Mokhtar**
Universiti Utara Malaysia, Malaysia

*[1]Corresponding author: muslimin@uum.edu.my*

Received:19/10/2022 Revised:1/11/2022 Accepted:18/12/2022 Published: 31/12/2022

## ABSTRACT

The Fourth Industrial Revolution (IR4.0) has provided immense benefits for the sustainability of businesses, with many businesses utilising websites to sell their products and services internationally. Cybersecurity has nonetheless emerged as one of the most significant global challenges posed by this new digitization trend. Currently, more than sixty percent of commercial transactions are conducted online or via digital wallets, necessitating exceptional security for transparent and secure transactions. Individuals are unable to maintain the security of their private data because of these evolving technologies, and cybercrime is on the rise. Information security is one of the most complex issues currently. Cybercrimes, which are increasing at an alarming rate, are the first thing that comes to mind when we think about cyber security. Consequently, numerous governments and corporations are enhancing their cybersecurity tools to combat cybercrime. Despite numerous precautions, cyber threats remain a major concern not only for government and large businesses, but also for Small and Medium-Sized Businesses (SMEs) companies.

This paper examines the challenges and solutions faced by small and medium-sized enterprises (SMEs) in relation to cyber security issues. In addition, it also examines the Malaysian context that may hinder the cybersecurity adoption gap for risk mitigation and high security in operational and development business environments.

**Keywords:** Cyber Security, Small and Medium Enterprises, Fourth Industrial Revolution.

## INTRODUCTION

Cybersecurity is the core for businesses and organisations to function and expand in a safe digital environment. Malaysia's government established the Digital Economy Blueprint (MyDIGITAL) to outline the significance of cyber security, which is one of the six key thrusts of the blueprint, to foster trust, security, and an ethical digital environment (MDEC, 2021). However, most local businesses lack adequate monitoring and security measures against unauthorised modification, resulting in unauthorised disclosure. Due to a lack of IT specialists and resources to implement the cyber security system with technological tools, SMEs face more cyber security-related development obstacles and concerns than larger businesses. According to Shaharuddin et al. (2021), SMEs frequently use a logging and alerting system but place less emphasis on organising employee awareness training. Low levels of physical security increase the risk of unauthorised people gaining access to sensitive information and equipment, resulting in the dissemination of inaccurate or incomplete data. A study will aid in understanding how local SMEs perceive the importance of cybersecurity, as well as the challenges and solutions confronting their sector in terms of keeping data secure and correcting any data mishaps that may have occurred. The study's overarching goal is to assist Malaysian SMEs in addressing and overcoming the unique challenges they face. This study was inspired by the findings of numerous academics in the field, and it employs technological advancement as a strategic implementation of cybersecurity awareness within businesses to increase safety and reduce instances of cybercrime.

### Background

Malaysia, a nation that prioritises information technology by promoting Internet usage, places a premium on cyber security practises. Through

the 1996 MSC agreement, the government introduced the concepts of e-government and e-commerce over the Internet. Consistent with the increase in internet usage in Malaysia, the country unquestionably faces numerous social issues, such as cybercrime. This is due to the reliance of internet users on new media.

When a person relies on the internet, cyber security becomes a concern because good practises determine the safety of internet users, whether they are individuals or members of an organisation. Cybercrime is currently a significant threat and obstacle for the Malaysian government. In order to combat the issue of cybercrime in Malaysia, consumers must be aware of the significance of safeguarding personal or government confidential data or information.

The rapid digitalization of the world has compelled businesses, such as SMEs, to make rapid and substantial adjustments to their technology adoption. These include cloud services, network connection upgrades, and website redesigns. In general, the contribution of SMEs to Malaysia's GDP has increased to 38.2 percent in 2020, with a value added of RM 512.8 billion (Department of Statistics, 2021). Malaysia anticipates a substantial contribution to the country's GDP from digital SMEs between RM 79 billion and RM 99 billion by 2024 (MDEC, 2021). However, the changes have led to an increase in cybercriminal attacks and a threat to the internal security of virtually all businesses. According to the World Economic Forum's Global Risk Reports 2021, cybersecurity failure could be ranked as the fourth most significant global threat in the near future.

One of the nine pillars susceptible to external and internal cyber-attacks in a complex environment is cybersecurity (Tamyez, 2022). It is the capacity to manage information and communication systems that include protection and prevent unauthorised users from causing damage or being exploited. The purpose of cybersecurity is to serve as a vital tool to reduce the risk of hostile attacks on digital devices and internet connections, as well as identify intruders, viruses, restrict malware access, and authenticate users.

According to the Global Cyber Safety Index 2020, Denmark has the highest level of cyber security, while Myanmar has the lowest. The 2020 National Cyber Security Index Email phishing and pharming are the most frequently reported online threats to US consumers,

accounting for approximately 33 percent of all reported cybercrime smoothly (Alahmari & Duncan, 2020; Nobles & Burrell, 2018; Ponsard et al., 2018). Meanwhile, over 110,000 instances of non-payment and non-delivery have been recorded, accounting for 14.9 percent of all cybercrimes in the United States (Ponsard et al., 2018). Extortion, which uses ransomware to infiltrate data and devices and then demands bitcoin or another form of payment, is the third most prevalent form of cybercrime. It has recorded 77,000 incidents, or 11 percent of all cybercrimes committed in the United States (Ponsard et al., 2018).

Cybercrime incidents increased from 11,875 in 2019 to 14,229 in 2021, with total damages of RM 413 million in 2021, as reported by the Royal Malaysia Police (PMO, 2021). The intelligent digital system necessitates the management and control of seasoned professionals in a technological setting. Many SMEs have become hacker targets because they are less vigilant in managing proper cybersecurity precautions as their paradigms evolve to balance working and IT system implementation to maintain company operation. Consequently, despite their limited capacity to utilise it, SMBs must become increasingly dependent on digital technology.

Cybercrime is more difficult to investigate than physical crime because it involves a border connection issue involving multiple legal jurisdictions. According to the Malaysia Computer Emergency Response Team (MyCERT), the number of cyber events reported to Cyber999 and responded to will increase from 6512 in 2020 to 10,016 in 2021, with the majority involving fraud, infiltration attempts, and malicious programmes. Moreover, approximately 85 percent of Malaysian SMEs have been subjected to cyber-attacks, with approximately 75 percent of SMEs threatened by multiple attacks. The study aims to benefit SMEs by providing solutions for companies to overcome the identified cybersecurity issues and challenges. The objectives of the study are to analyse the cybersecurity challenges faced by Malaysian SMEs; and to identify solutions for SMEs to overcome cyber security challenges.

## LITERATURE REVIEW

The government of Malaysia is concerned about cyber security and is taking steps to protect people and systems that operate in this

country. Various researchers from around the globe have identified the problems by analysing them using hierarchical models of connectivity, applications, and cyberattacks to develop solutions that are in line with the government's approach. Studies and real-world experiences have demonstrated that businesses with well-developed cyber skills can handle cyber incidents more effectively than those with a flawed plan or insufficient resources to effectively counter cyberattacks.

## The Importance of Cyber Security in SMEs Companies

Rectifying a data breach or cyber-attack could cost SMEs companies millions of dollars. When there is a data breach in SMEs companies' systems, it is not just the financial loss that is a concern. A breach of extremely sensitive personal data could have disastrous consequences for a SMEs companies' reputation and people's privacy. Theft of sensitive information, such as medical records, is becoming a more profitable venture for cybercriminals. As a result, it is critical that the SMEs companies implements a comprehensive and efficient cyber security system at multiple, if not all, levels to prevent cyber criminals from stealing or hijacking the information they hold.

Every industry must prioritise cyber security due to the prevalence of cybercrime and massive data breaches. To maintain robust security and reduce the risk of illegal activities, data security has become increasingly important for SMEs, corporations, and government agencies. The stolen information is then used in a variety of hostile operations, putting victims in perilous situations. Furthermore, the SMEs companies stores highly classified information that should be protected from unauthorised access so that it cannot be used for malicious purposes and victims do not suffer. There are numerous local and global legislative frameworks that call for stringent data protection standards to be in place to help secure the safety of personal and financial data of individuals and organisations from unauthorised access. All SMEs companies' software applications that collect users' information to provide services are required to be extra cautious regarding online data security of users to protect their information from data breaches, identity fraud, account takeover frauds, and other deceitful hackers from accessing highly classified information of people for nefarious reasons.

Aside from that, SMEs companies all over the world, like businesses, keep sensitive data on computers and in the cloud (online storage such as Google Drive or iCloud) (Adlakha et al., 2019). The information could be about national investments, defence plans, or citizen identity, among other things. Attempts by adversaries or hackers to breach SMEs companies' computers and gain access to public data, such as an adversary country obtaining defence blueprints through a breach of SMEs companies' system, are also possible in the future (Bilodeau et al., 2019; Boletsis et al., 2021). As a result, the companies' overall security is jeopardised, proving once again that cyber security is critical and required to protect sensitive personal data (Antunes et al., 2021; Benz & Chatterjee, 2020).

In addition, SMEs rely heavily on cyber security to ensure service continuity. Most SMEs' services are available via their websites. Every country also has plenty of websites linked to the SMEs that keep things running smoothly (Alahmari & Duncan, 2020; Nobles & Burrell, 2018; Ponsard et al., 2018). Attackers may attempt to compromise such critical websites and disrupt nationwide service. It may even have a negative impact on the economy. The SMEs companies also relies on a wide range of hardware to carry out a variety of tasks. Servers, computers, sensors, CPUs, and modems are just a few examples. As a result, SMEs companies must rely on cyber security to protect the nation's critical infrastructure, such as energy and water, by safeguarding information technology infrastructure.

Cyber terrorism is another security risk. Cyber terrorism is not limited to attacks conducted in or through cyberspace. Today, the Internet has become the primary medium for propaganda and communication, and it has the potential to be a powerful tool for mobilisation and radicalization (Benz & Chatterjee, 2020; Vakakis et al., 2019). Another type of cyber terrorism is the introduction of malware or the hacking of sensitive sections of SMEs' websites to gather confidential information via spies, which has a similar indirect relevance in the long run, because parties may use the information to exploit computer system weaknesses. As a result, this demonstrates the critical importance of SMEs implementing effective cyber security measures.

**Challenges of Cybersecurity Facing by SMEs Companies**

The challenge is an insufficient level of alertness in cybersecurity due to its complex issues that require direct dealing with technical

solutions and measures, which primarily concern IT professionals. There are various types of information system attacks that necessitate expertise at the hardware, firmware, and operating system levels (Pérez-González et al., 2019). As a result, cybersecurity must be embedded into organisational culture to at least encourage all employees to have basic self-awareness about cybersecurity, which will affect the overall cybersecurity culture of the organisation (Kim et al., 2019; Pérez-González et al., 2019). Employees, for example, have a basic understanding of how phishing attacks work, precautions to take when using personal digital devices to access the company's system environment, and other fundamental cybersecurity prevention measures (Heidt et al., 2019).

The next issue is a lack of safeguards for sensitive and confidential company information. SME businesses typically handle a variety of information, including customer information, product and service details, procurement information, financial data, organisational policies and procedures, and employee records. Although all information in businesses is valuable and must be protected, there is a lack of backup policy, no anti-malware solution implemented on all digital devices, and the use of outdated, obsolete software (Bada & Nurse, 2019). All these factors can jeopardise a company's sensitive and confidential data and make it an easy target for cyberattacks such as ransomware.

Another challenge is the budgetary issue, as not all businesses, particularly SMEs, can afford to set up a cybersecurity system (Bilodeau et al., 2019; Jayashree et al., 2021; Soong et al., 2020). The investment in a cybersecurity system includes cybersecurity awareness training for employees, the implementation of cybersecurity policies, the engagement of external experts, and the conduct of special trainings for IT staff. Subscribing to a dedicated cybersecurity solution, such as an advanced firewall and event management system, is typically a large investment for businesses which is not all SMEs companies afford to buy the systems. SMEs frequently choose to use the cloud on a subscription basis, but many of them do not invest in additional security controls (Adlakha et al., 2019). Because of the size of their businesses, they are frequently ineligible for high-level subscription plans that include advanced solutions. SME businesses, on the other hand, see this as an extra cost rather than an investment in business that necessitated controls for business protection (Adlakha et al., 2019; Tam et al., 2021).

Furthermore, a lack of cybersecurity expertise and personnel in businesses is a challenge when they lack specific personnel to manage and control (Bada & Nurse, 2019). Employees in small and medium-sized businesses frequently multitask and handle multiple roles. Several cybersecurity standards, such as ISO270000:2013 (Bilodeau et al., 2019; Tamyez, 2022), are required to improve their cybersecurity readiness, particularly as SME businesses grow and develop and the technology used changes. As a result, instead of managing these products by non-technical staff, they must hire external experts to assist and manage them by default.

SMEs also have low management support when it comes to implementing a cybersecurity system. Senior management is difficult to persuade because they believe that cyber-attacks only occur in larger organisations and that SMEs are too small for criminals to hack into. Unfortunately, all companies, whether large or small, can be similarly attacked, particularly SMEs, because they are easy targets with no tight cybersecurity system in place.

**Solutions for Cybersecurity Among SMEs Companies**

There are several recommended solutions and measures to consider, and cybersecurity does not have to be expensive to implement and maintain for SMEs. Cybersecurity training is required for SMEs to manage and maintain their IT systems by employees who do not have formal cybersecurity training (Boletsis et al., 2021). SMEs typically prefer in-house IT expertise over outsourced IT expertise. As a result, employees in charge of cybersecurity must receive proper training, as well as adequate budgeting and resources, to manage the system within the company (Tamyez, 2022).

Another option is to provide SMEs with a low-cost cybersecurity system. Typically, SMEs do not budget adequately for cybersecurity solutions such as purchasing products, services, and external consulting services. It is suggested that the government subsidise certain funding to assist SMEs in improving their cybersecurity posture, providing tools to reduce the cost of IT solutions based on effective procurement methods, and many other things (Tamyez, 2022; van Haastrecht et al., 2021). For example, after negotiation and consideration of authority, SMEs can subscribe to customised Service Legal Agreements (SLA) based on their size and suitability to fit SMEs cybersecurity needs.
Furthermore, management commitment is critical to ensuring the

effectiveness of cybersecurity in SMEs, as demonstrated by their leadership. The management team's support can ensure the availability of cybersecurity resources such as personnel time management, the purchase of cybersecurity software, services, and hardware, staff training, and effective cyber-related policies for businesses (Shaharuddin et al., 2021; Soong et al., 2020). Management should be more visible to all those who require resources by providing supportive leadership. Management in SMEs plays a critical role in ensuring cybersecurity by including it on the agenda of company management meetings and discussing it at the highest level within the company on a regular basis.

Network security is a technical issue that is critical for a business. The firewall solution was implemented at least 85 percent before the pandemic, with the figure rising to 90 percent during the pandemic (Lanz & Sussman, 2020). Security measures such as firewalls, antivirus, strong passwords, encryption, and so on are critical success factors that must be carefully implemented and maintained. SMEs can work with relevant experts to recommend the best solutions for business protection, such as filtering email and web traffic for malware prevention, blocking unauthorised access, and alerting for potential attacks (Lanz & Sussman, 2020).

## RESEARCH DESIGN

The qualitative method employs the depth interview method, which simply means having a conversation with the goal of gaining more real-world experience and insightful views on this research topic (Creswell, 2013). The semi-structured interview is considered flexible in that the sequence of questions during the interview, wordings, and time allocated to each question can be changed based on the needs of each separate interview (Markus & Lee, 1999; Martinez-Uribe, 2008).

The populations for this study are the 5,634 Malaysian SMEs who have received SME Business Digitalization Grants under the MDEC initiative, as of November 2020 (SME Corp, 2020). This study's sample consists of 30 Malaysian SMEs with top management and IT specialists who have implemented cybersecurity in their businesses and have received the SME Business Digitalization Grant. In this study, purposive sampling method was used to provide various categories of cases relevant to the specific event based on population characteristics

(Creswell, 2013; Myers & Avison, 2002). The interview will be conducted in three ways: by phone, by email, and in person. During the interview, protocols will be prepared that include a headline, description, and instructions for interviewers, the identification of important questions, the listing of major queries for investigation, transition information for interviewers, recording of interviewers' responses and answers, and space for investigators to make a reflective note. Thematic analysis is also will be used for providing reliable and credible analysis. It allows for detailed data exploitation to discover any construct specified by the researcher query. In the coding paper, a general coding scheme was created on general domains for research questions and interview protocols, as well as notational conventions used for interview transcription to describe the respondents' words.

## CONCLUSION

Cybersecurity has prompted every country to outline their approach to dealing with cyber issues. Although cybersecurity is a global phenomenon with complex social-technical challenges primarily for governments and private businesses, visibility and awareness have remained low. According to researcher Walter, appropriate learning on online performance and system protection has decreased vulnerabilities with a safer online environment (Tamyez, 2022). There are numerous cyberattacks that occur daily using various techniques to bleach data; therefore, cyber security has become an essential approach to ensuring a strict and sophisticated system to protect data and information within businesses. Companies' management should instil a culture of dealing with technology asset challenges, whether they are policy, monetary, or operational risks. This research must determine and communicate organisational risk management behaviour and approaches. As a result, cybersecurity challenges in SMEs include awareness, people, technology, and budget. Many of the findings indicate that employee cybersecurity awareness can alert companies to cyber-attacks. For data protection, all businesses must build and maintain a highly secure information system. The goal of this research is to develop a competency management strategy based on the available resources within companies, such as capital, resources, and employee capabilities. As a result, advanced levels of cybersecurity will include additional security protection to reduce cyber threats and ensure long-term success in business operations.

## ACKNOWLEDGMENT

This research received no specific grant from any funding agency.

## REFERENCES

Adlakha, R., Sharma, S., Rawat, A., & Sharma, K. (2019). Cyber Security Goal's, Issue's, Categorization & Data Breaches. *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*, 397–402.

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)*, 1–5.

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security*.

Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*, *63*(4), 531–540.

Bilodeau, H., Lari, M., & Uhrb, M. (2019). Cyber security and cybercrime challenges of Canadian businesses, 2017. *Juristat: Canadian Centre for Justice Statistics*, 1–18.

Boletsis, C., Halvorsrud, R., Pickering, J. B., Phillips, S. C., & Surridge, M. (2021). Cybersecurity for SMEs: Introducing the Human Element into Socio-technical Cybersecurity Risk Assessment. *VISIGRAPP (3: IVAPP)*, 266–274.

Creswell, J. W. (2013). *Research design: Qualitative, quantitative, and mixed methods approaches.* SAGE Publications Ltd.

Heidt, M., Gerlach, J. P., & Buxmann, P. (2019). Investigating the security divide between SME and large companies: How SME characteristics influence organizational IT security investments. *Information Systems Frontiers*, *21*(6), 1285–1305.

Jayashree, S., Hassan Reza, M. N., Malarvizhi, C. A. N., Maheswari, H., Hosseini, Z., & Kasim, A. (2021). The Impact of Technological Innovation on Industry 4.0 Implementation and Sustainability: An Empirical Study on Malaysian Small and Medium Sized Enterprises. *Sustainability*, *13*(18), 10115.

Kim, H.-K., So, W.-H., & Je, S.-M. (2019). A big data framework for network security of small and medium enterprises for future computing. *The Journal of Supercomputing*, *75*(6), 3334–3367.

Lanz, J., & Sussman, B. I. (2020). Information security program management in a COVID-19 world. *The CPA Journal*, *90*(6), 28–35.

Markus, M. L., & Lee, A. S. (1999). Special issue on intensive research in information systems: Using qualitative, interpretive, and case methods to study information technology. *MIS Quarterly*, *23*(1), 35–38.

Martinez-Uribe, L. (2008). Findings of the scoping study interviews and the research data management workshop. In *University of Oxford, UK*.

Myers, M., & Avison, D. (2002). *Qualitative research in information systems: An introduction to qualitative research in information systems*. SAGE Publications, Ltd. https://doi.org/10.4135/9781849209687

Nobles, C., & Burrell, D. (2018). Using Cybersecurity Communities of Practice (CoP) to Support Small and Medium Businesses. *ICIE 2018 6th International Conference on Innovation and Entrepreneurship: ICIE 2018*, 333.

Pérez-González, D., Preciado, S. T., & Solana-Gonzalez, P. (2019). Organizational practices as antecedents of the information security management performance: An empirical investigation. *Information Technology & People*.

Ponsard, C., Grandclaudon, J., & Dallons, G. (2018). Towards a Cyber Security Label for SMEs: A European Perspective-. *ICISSP*, *4*, 426–431.

Razak, D. A., Abdullah, M. A., & Ersoy, A. (2018). Small medium enterprises (SMEs) in Turkey and Malaysia a comparative discussion on issues and challenges. *International Journal of Business, Economics and Law*, *10*(49), 2–591.

Shaharuddin, A. B., Aminudin, E., Zakaria, R., Abidin, N. I., & Lau, S. E. N. (2021). Adoption of construction industry 4.0 among small and medium sized contractor in Malaysia. *AIP Conference Proceedings*, *2428*(1), 060001.

Soong, K.-K., Ahmed, E. M., & Tan, K. S. (2020). Factors influencing Malaysian small and medium enterprises adoption of electronic government procurement. *Journal of Public Procurement*, *20*(1), 38–61.

Tam, T., Rao, A., & Hall, J. (2021). The good, the bad and the missing: a narrative review of cyber-security implications for Australian small businesses. *Computers & Security*, *109*, 102385.

Tamyez, P. F. (2022). The Challenges and Solutions of Cybersecurity Among Malaysian Companies. In *Research Anthology on Business Aspects of Cybersecurity* (pp. 676–693). IGI Global.

Vakakis, N., Nikolis, O., Ioannidis, D., Votis, K., & Tzovaras, D. (2019). Cybersecurity in SMEs: The smart-home/office use case. *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 1–7.

van Haastrecht, M., Golpur, G., Tzismadia, G., Kab, R., Priboi, C., David, D., Răcătăian, A., Baumgartner, L., Fricker, S., & Ruiz, J. F. (2021). A shared cyber threat intelligence solution for smes. *Electronics*, *10*(23), 2913.