Available online at
https://journal.uitm.edu.my/ojs/index.php/JIKM

e-ISSN: 2289-5337

Journal of Information and Knowledge Management
Vol 15 Special Issue (2025)

Journal of Information and Knowledge Management

Cybersecurity Threats among SMEs in Malaysia: Risks and Challenges

Mohamad Syauqi Mohamad Arifin*, Salliza Md Radzi, Nur Ainatul Mardiah Mat Nawi
Mohamad Rahimi Mohamad Rosman, Noor Azreen Alimin

College of Computing Informatics and Mathematics, Universiti Teknologi MARA Kelantan, 18500 Machang, Kelantan, Malaysia

Corresponding author's e-mail address: mohdsyauqi@uitm.edu.my

ARTICLE INFO

Article history:
Received 24 December 2024
Revised 22 February 2025
Acceptance 12 March 2025
Online first
Published May 2025

Keywords:
Cybersecurity Threats
Cyberthreats
Small Medium Enterprise
Risk And Challenges

https://doi.org/10.24191/jikm.v15iSI1.6228

ABSTRACT

Small and Medium Enterprises (SMEs) play a crucial role in Malaysia's economic development by significantly contributing to employment and Gross Domestic Product (GDP). However, these enterprises increasingly face cybersecurity threats, which underscores the urgent need to address the specific operational risks and challenges they encounter. Therefore, this paper aims to provide an overview of cybersecurity and outline prevalent threats, emphasizing their impacts as demonstrated in the existing literature. Additionally, the paper examines the barriers and challenges SMEs encounter and offers practical recommendations aimed at enhancing their cybersecurity resilience. This work greatly enhances the understanding of cybersecurity issues for SMEs and addresses important gaps in the existing body of knowledge.

INTRODUCTION

SME is an acronym for Small and Medium Enterprise while it is also interpreted as Small and Midsize Businesses. SME can be categorised into two industries which are manufacturing, for example, focusing on spare part factories or production of physical goods. The annual sales should not be more than RM50 million or not more than 200 full-time workers. The other one is services, such as the services industry which is different from manufacturing industries. It includes a wide range of fields such as legal firms, and tourism that are connected to business and others. Its annual sales should not be more than RM20 million and 75 full-time workers. A business can qualify as an SME if it meets either one of the two specified criteria, namely sales turnover or full-time employees, whichever is lower. The definition covers all sectors, including services, manufacturing, agriculture, construction mining and quarrying.

SMEs have significantly contributed to the Malaysian economy since the early dependence phase, which relied on the agriculture sector as the main source of the nation's income until today's economy which depends on manufacturing and services sectors. SMEs play vital roles as they help to grow employment opportunities, especially in technological and product innovation, and poverty reduction through employing poor and low-income workers, especially in poor regions and rural areas. Despite their small size, the contribution of Malaysian SMEs in enhancing economic development and fulfilling the

social needs of the nation indicates their important role in strengthening the country to face the resilient challenges in today's knowledge economy (Muda, & Musman, 2022).

In most countries, SMEs constitute the vast majority of businesses. As in Malaysia, SMEs are often said to be the backbone of the economy. In 2023, a total of 1,101,725 SMEs were recorded in Malaysia, accounting for 96.9% of total businesses. SMEs continued to be resilient in 2023 with positive growth being recorded across key macroeconomic indicators (SME Corp Malaysia, 2024).

In today's digital world, the threat of cyberattacks is more significant than ever. For large corporations, cybersecurity is a top priority, but for SMEs, limited resources can make it challenging to prioritise. Often, SMEs rely on basic antivirus software and a general employee with some IT knowledge. However, recent trends indicate that this approach is no longer enough to protect the SMEs. According to the Malaysia Cybersecurity Insights 2024 report, Ransomware-as-a-Service (RaaS) attacks have increased by 45%, primarily targeting SMEs. Moreover, 72% of Malaysian businesses experienced supply chain attacks in 2022. These statistics highlight the growing risks SMEs face in the digital landscape. Years ago, an antivirus program might have been sufficient to protect SME businesses from cyber threats. However, as technology has advanced, so have the tactics of cybercriminals. Today, the threats are more sophisticated and varied, requiring a comprehensive approach to cybersecurity (Nik Sharmine A, 2024).

Cybersecurity is 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 (Economic Planning Unit, 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 cybersecurity-related development obstacles and concerns than larger businesses (Wallang, Shariffuddin, & Mokhtar, 2022).

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. This research aims to identify the risks and challenges among SMEs in Malaysia related to cyber security threats based on the findings of numerous academics in the field.

LITERATURE REVIEW

Overview of Cybersecurity

The advancement of technology and the emerging threats of cybercrimes nowadays have raised a significant issue in the aspect of security. Cybersecurity is the method of securing information and computer systems from unauthorised access, cyber threats, and other forms of disruptions. The growth of digital technologies and the shift towards relying on the internet have improved the value of cybersecurity. Cybersecurity focuses on the strategies, tools, and techniques to prevent different cyber threats to the systems and data. The previous study stated that cybersecurity involves risk assessment, identifying threats, and designing methods for handling the threats (Stallings, 2020). Other than that, cybersecurity also includes the use of security such as software security, encryption, and also implementation of policies and standards. Kshetri (2017) in a study discusses that cybersecurity also involves correction of bugs and installation of patches that should be done more frequently. Hence, as IT solutions continue to be implemented, the security issue becomes an important element as it has impacts on the economy and organization (Anderson, 2020).

Small and Medium Enterprises (SMEs) have greatly changed the way they conduct their business with the use of digital platforms and the Internet. Even though the adoption of technology is giving positive impacts, it has also increased the exposure to cybercrimes. SMEs remain exposed to cyber threats since they lack sufficient resources, knowledge, and protection protocols as compared to the larger companies. The threats to the SMEs have increased and become increasingly frequent and advanced in recent years. As stated by the Association (2023) digital change has been adopted to enhance the operation of the SMEs. However, this resulted in a number of cybersecurity threats. These attacks may result in loss of money, reputation of the business, and trust from the customers. Thus, SMEs must consider ways to minimize these risks and guarantee the safety of customer assets, by investing in cybersecurity.

Cybersecurity aims to protect against both threats and vulnerabilities. Cyber threats can be defined as risk factors that may potentially cause damage or negatively affect information systems. They include malware, phishing, ransomware, and insider threats. Each threat poses risks to both the organizations and the individuals involved. Hence protective actions need to be implemented. Cybersecurity is a field that is always moving forward and experiencing improvement, with new technologies and trends in the future. The advanced technology of machine learning (ML) and artificial intelligence (AI) has developed better ways of identifying threats and ways of handling threats. According to Zhang (2023), these technologies imply the ability to analyze a large amount of data to determine trends or risks. Apart from ML and AI, blockchain technology could also secure transactions or data with decentralized and non-modifiable records (Kshetri, 2017; Saberi et al., 2019; Zamani et al., 2020). Once the data is added to the blockchain, they cannot be changed in any way which helps to add another layer of protection for digital transactions and data storage. Today, blockchain technology is being applied to numerous industries such as financial services, manufacturing, and even medicine. Thus, implementing IT security controls and being aware of the threats makes it easier to overcome the cyber risks and develop a successful business in the future.

Studies Related to Cybersecurity in Malaysia

The digital transformation driven by the Fourth Industrial Revolution (IR4.0) has enabled many Malaysian SMEs to adopt new technologies, such as e-commerce platforms and cloud services, increasing their operational efficiency and market reach. However, this rapid digitalisation has also exposed SMEs to significant cybersecurity threats. As Wallang et al. (2022) noted, approximately 85% of Malaysian SMEs have experienced cyber-attacks, with nearly 75% facing multiple incidents. The reliance on digital tools without proper security makes SMEs vulnerable to threats like data breaches, ransomware, and phishing attacks, leading to financial losses, reputational damage, and operational disruptions (Papathanasiou et al. 2024).

One of the major challenges for SMEs is the lack of resources and expertise to implement robust cybersecurity measures. Many SMEs operate with limited budgets, which are often insufficient to cover advanced security solutions, staff training, or the hiring of cybersecurity specialists. Furthermore, there is often a lack of awareness among SME management about the severity of cybersecurity risks, leading to inadequate prioritization of security measures. Most SMEs also lack a backup policy, anti-malware solutions, and proper training programs for employees, leaving them ill-equipped to handle cyber threats effectively (Tetteh, 2024; Wallang et al., 2024).

The Malaysian government has recognized the importance of addressing these challenges and has introduced initiatives such as the Digital Economy Blueprint (MyDIGITAL) to promote cybersecurity awareness and resilience among businesses (Chan, 2024). Previous studies highlight several solutions to enhance cybersecurity practices among SMEs. These include implementing low-cost cybersecurity solutions, conducting employee awareness training, and encouraging SME management to support cybersecurity initiatives actively (Lee, 2023; Md Yusof et al. 2024; Othman et al., 2021). There is also a need for government subsidies to make advanced cyber security solutions more affordable for SMEs in Malaysia.

Despite these challenges, there are promising strategies for SMEs to improve their cybersecurity posture. Key recommendations include fostering a culture of cybersecurity awareness within organizations, investing in essential security tools such as firewalls and antivirus software, and collaborating with experts to design tailored security solutions. With stronger management support and a proactive approach, Malaysian SMEs can significantly reduce their vulnerability to cyber threats and ensure their long-term sustainability in a competitive digital economy.

Cybersecurity Threats

For SMEs, common cybersecurity threats include phishing, ransomware, malware, data breaches due to poor password hygiene, business email compromise, unpatched software vulnerabilities, social engineering, and lack of employee awareness. These threats disrupt operations and lead to financial losses unless mitigated through security measures like regular software updates, strong passwords, and employee training. The rising threat of malware to information security poses significant risks to the Windows operating system, including system exploitation that can compromise consumer login information. While existing systems are slow and inefficient, research proposes machine learning and IoT approaches for businesses to detect threats, adapt, and implement cybersecurity techniques. However, challenges remain, such as the impracticality of signature-based detection and the inability of machines to detect new-generation malware with complete precision (Judy S & Rashmita Khilar, 2023). Phishing for example poses a significant cyber threat to organizations (Gamisch & Pöhn, 2023) and phishing emails, which pretend to be legitimate messages, are a serious modern threat that cybercriminals use to trick individuals into revealing personal information (Anirudh et al., 2024). Besides phishing, the widespread availability of ransomware toolkits, ransomware as a service (RaaS), and numerous infection vectors have led to significant growth in ransomware attacks and severe cases of digital extortion. These attacks carry out various operations, including deleting backups, encrypting original files, and searching for crucial files on the victim's computer. This results in highly complex execution logs and dynamic exploitation patterns (Sharmeen et al., 2020). Other than the previous, data breach is another common critical threat to be discussed. In today’s digital age, data is crucial to every industry. To protect sensitive information, various methods and technologies emerge. Data breaches expose confidential data to unauthorized individuals. As our devices connect, the risk of leaks increases. These breaches threaten organizations financially and damage reputations. Beyond the organization, they impact users, staff, and remediation teams (Bargavi M et al., 2023).

Cyberattacks severely impact small to medium-sized enterprises (SMEs), which are primary targets of cybercrimes. SMEs face substantial financial losses due to limited recovery resources. Data breaches exceed $2.2 million annually and are projected to grow by 15% in the next five years. A survey revealed that 60% of SMEs cease operations after a cyber attack. In 2020, over 700,000 attacks against SMEs caused $2.8 billion in damages. The 2021 IBM report showed the average total cost of data breaches rose to $4.24 million, the highest in 17 years. Cybersecurity Ventures projects rapid economic wealth transfer through cybercrime, growing from $3 trillion in 2015 to $10.5 trillion globally by 2025. Beyond financial costs, SMEs may incur lost revenue and reputational damage, which are challenging to recover from. Phishing for instance, is also known as one of the serious cyber threats to organizations that potentially results in both financial losses and reputational harm which could threaten an organisation's survival (Gamisch & Pöhn, 2023). Since traditional supervised detection systems struggle to provide effective zero-day protection against future incidents of digital extortion due to the dynamic creation of ransomware (Sharmeen et al., 2020) and other threats, investing in cybersecurity and developing a comprehensive response plan is crucial to mitigate financial losses from cyber incidents (Binita Saha & Zahid Anwar, 2024).

Risk and Challenges Related to Cybersecurity Threats

Cyber-attacks on small and medium enterprises (SMEs) are rising, yet many lack effective strategies to combat threats like malware, phishing, and other attacks. Their weak defences make them attractive

targets for hackers. Most SMEs have insufficient cybersecurity initiatives and awareness, and the limited information available online creates confusion. Unlike large enterprises with dedicated cybersecurity resources, SMEs often struggle to manage multiple threats. This highlights the need for comprehensive and reliable security solutions, as many vendors only offer targeted options, leaving SMEs vulnerable to other attacks. (Ahmed & Nanath, 2021).

FINDINGS AND DISCUSSION

Cybersecurity threats are continually evolving and represent a significant concern for anyone who uses technology and data. Numerous studies have shown that small and medium-sized enterprises (SMEs) are particularly vulnerable to these threats, making them frequent targets for cybercriminals. A major reason for this vulnerability is often the lack of essential cybersecurity measures. Consequently, the impact of cybersecurity incidents on small businesses is disproportionately severe, as they typically have fewer resources to prepare for and manage cyberattacks (Ahmed & Nanath, 2021). Organisations today face significant challenges in investing in and improving their security measures and software services, as well as increasing end users' awareness of cybersecurity threats and best practices. Additionally, there is a recurring trend in the literature indicating that small and medium-sized enterprises (SMEs) often do not take the threat of cybersecurity seriously. Addressing these issues is crucial for protecting sensitive information and maintaining operational integrity (Ahmed & Nanath, 2021).

An adaptable framework must be identified to extract the inherent nature of exploitation and encryption in new ransomware variants, achieving significant performance improvements and accuracy over supervised detection approaches (Sharmeen et al., 2020). The same goes for tackling phishing issues technically; by integrating various algorithms, this enhances the system's ability to detect subtle details and patterns commonly associated with phishing techniques, thereby improving email security more effectively than traditional methods. This advancement in cybersecurity technology represents a significant breakthrough, showcasing the versatility and effectiveness of modern machine learning in addressing the complexities of evolving threats (Anirudh et al., 2024). Small and medium-sized enterprises (SMEs) should also consider implementing a recommender system for cybersecurity initiatives. The prototype utilises a flowchart that guides organizations through the journey of developing a cybersecurity plan, ultimately recommending suitable solutions. This tool enables organizations to select features and technologies tailored to their specific needs. Once deployed on a web interface, this flowchart will serve as a recommender system that helps SMEs identify customized cybersecurity features and solutions based on their requirements (Ahmed & Nanath, 2021). Other types of technology SMEs might be looking for in their setup and choices of solutions include several technologies like next-gen firewalls, email security, endpoint security, encryption, cloud security, network access controls, vulnerability management, password management, network performance monitoring, and data leakage prevention (Ahmed & Nanath, 2021).

Technical measures alone are insufficient; therefore, combining them with comprehensive employee awareness training is crucial to combat the threat of phishing effectively. High participation levels among employees are crucial for enhancing understanding and evaluating the effectiveness of this training. To build long-term resilience, regular awareness training is needed, with recommendations suggesting intervals ranging from once a month to once every six months. The training method should be straightforward, time-efficient, engaging, and informative. Additionally, it should seamlessly integrate into the work routine and provide added value (Gamisch & Pöhn, 2023). Based on a study in the SME context, it is revealed that most small and medium-sized enterprises (SMEs) lack adequate cybersecurity awareness, and the overall cybersecurity awareness levels among colleagues and clients were low. Therefore, implementing training programs and educating employees about information security awareness is the most effective way to ensure compliance with organizational processes and policies. In this context, raising awareness about data protection and steps to mitigate attacks is crucial. SMEs are also encouraged to assess their organizational policies from a risk perspective, develop effective policies for implementation, and appoint individuals responsible for information security in each department (Ahmed & Nanath, 2021).

This study makes significant contributions to the understanding and management of cybersecurity challenges faced by Malaysian SMEs. By identifying key threats such as phishing, ransomware, and data breaches, it provides a comprehensive analysis of the vulnerabilities specific to SMEs, particularly in the Malaysian context. Furthermore, the study emphasizes the critical role of fostering employee awareness and adopting advanced technologies like AI and blockchain to mitigate these threats. These practical insights serve as a guide for SMEs to enhance their cybersecurity posture while balancing their limited resources and operational constraints. Additionally, the study supports the implementation of government policies, such as subsidies and training programs, aligning with Malaysia's Digital Economy Blueprint to promote trust and resilience in the digital transformation of SMEs.

CONCLUSION

Beyond immediate practical implications, this study advances the development of cybersecurity frameworks tailored to the unique needs of SMEs. By integrating technical measures with regular employee training, the study highlights the importance of a holistic approach to mitigating cybersecurity risks. This dual focus on technology and human capital provides a sustainable model for SMEs to strengthen their resilience. Moreover, the findings lay a foundation for further academic inquiry and innovation in cybersecurity strategies, not only in Malaysia but also in global contexts where SMEs face similar challenges.

Future research could focus on conducting comparative analyses across different SME sectors, such as manufacturing, services, and agriculture, to better understand sector-specific cybersecurity challenges and develop tailored solutions. Longitudinal studies are also essential to assess the effectiveness and sustainability of the proposed strategies, such as low-cost security measures and employee training programs, over an extended period. This would provide valuable insights into how SMEs adapt to evolving cybersecurity threats and whether the suggested approaches deliver long-term benefits. Another area for future exploration involves investigating the potential of emerging technologies, such as quantum computing and advanced machine learning, in enhancing SME cybersecurity. Additionally, the study could delve into cultural and behavioural factors that influence the adoption of cybersecurity practices, particularly in rural or underserved regions.

Studies examining the economic impact of cyberattacks, including indirect costs like reputational damage, could further highlight the importance of investing in robust cybersecurity measures. Lastly, collaborations between SMEs, government agencies, and private firms in addressing resource gaps present a valuable avenue for research, along with in-depth case studies of SMEs that have successfully implemented innovative cybersecurity solutions. These studies would provide actionable insights and practical models for SMEs globally.

ACKNOWLEDGEMENT

Acknowledgments: The authors would like to thank the financial support received from Universiti Teknologi MARA Cawangan Kelantan, Malaysia, under Internal Grant 600-TNCPI 5/3/DDN (03) (004/2020) 600-CK(PJIA/URMI 5/1).

REFERENCES

Ahmed, N. N., & Nanath, K. (2021). Exploring Cybersecurity Ecosystem in the Middle East: Towards an

SME Recommender System. *Journal of Cyber Security and Mobility*, *10*(3), 511–536. https://doi.org/10.13052/jcsm2245-1439.1032

Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.). Wiley.

Anirudh, S., Radha Nishant, P., Baitha, S., & Dinesh Kumar, K. (2024). An Ensemble Classification Model for Phishing Mail Detection. *Procedia Computer Science*, *233*, 970–978. https://doi.org/10.1016/j.procs.2024.03.286

Association, G. C. (2023). Cybersecurity for Small and Medium-Sized Enterprises (SMEs). https://globalcybersecurityassociation.com/blog/cybersecurity-for-small-and-medium-sized-enterprises-smes/

Chan, M. (2024). Malaysia: Digital Payments, Data Regulations, and AI as Most Promising Areas for Digital Economy Collaboration. In *The ASEAN Digital Economy* (pp. 76-96). Routledge.

Economic Planning Unit, Prime Minister's Department. (2021). *Malaysia digital economy blueprint*. https://www.ekonomi.gov.my/sites/default/files/2021-02/malaysia-digital-economy-blueprint.pdf

Gamisch, L., & Pöhn, D. (2023, August 29). A Study of Different Awareness Campaigns in a Company. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3600160.3605006

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications policy, 41(10), 1027-1038.

Lee, C. (2023). Strategic Policies for Digital Economic Transformation: The Case of Malaysia. *Journal of Southeast Asian Economies*, *40*(1), 32–63. https://www.jstor.org/stable/27211224

Lembaga Hasil Dalam Negeri Malysia. (2024). *SME: What is SME*. https://www.hasil.gov.my/en/company/sme/

Md Yusof, A., Zaini, M. K., Khairuddin, I. E., and Ahmad Uzir, N. (2024). Modeling a Digital Trust Framework to Address Cybersecurity Issues in Malaysia's Digital Economy. *International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies, 15(4), 15A4B*, 1-12. http://TUENGR.COM/V15/15A4B.pdf DOI: 10.14456/ITJEMAST.2024.21

Muda, S., & Musman, M. (2022). *SMEs in Malaysia: History and development*. https://ir.uitm.edu.my/id/eprint/68417/

Nik Sharmine A. (2024, August 16). Beyond antivirus: Protecting your SME business from evolving cyber threats. https://excelerate.asia/articles/beyond-antivirus-protecting-your-sme-business-from-evolving-cyber-threats/#:~:text=According%20to%20the%20Malaysia%20Cybersecurity,face%20in%20the%20digital%20landscape.

Othman, I. W., Topimin, S., Ahmad, S. N. B., & Hasan, H. (2021). Driving the development of SMEs' entrepreneurs in the era of digitalisation: From the dynamic perspective of law enforcement in Malaysia. *International Journal of Accounting*, *6*(37), 124-143. https://www.researchgate.net/publication/356718178_Driving_The_Development_Of_SMEs'_Entrepreneurs_In_The_Era_Of_Digitalisation_From_The_Dynamic_Perspective_Of_Law_Enforcement_In_Malaysia

Papathanasiou, A., Liontos, G., Katsouras, A., Liagkou, V., & Glavas, E. (2024). Cybersecurity Guide for SMEs: Protecting Small and Medium-Sized Enterprises in the Digital Era. *Journal of Information Security*, *16*(1), 1-43. https://doi.org/10.4236/jis.2025.161001

Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. International journal of production research, 57(7), 2117-

2135.

Shaharuddin. A. B., Aminudin, E., Zakaria, R., Abidin, N. I., & Lau, S. E. N. (2021, November). Adoption of construction industry 4.0 among small and medium sized contractor in Malaysia. *AIP Conference Proceedings, 2428* (1). https://doi.org/10.1063/5.0071094

Sharmeen, S., Ahmed, Y. A., Huda, S., Kocer, B. S., & Hassan, M. M. (2020). Avoiding Future Digital Extortion through Robust Protection against Ransomware Threats Using Deep Learning Based Adaptive Approaches. *IEEE Access*, *8*, 24522–24534. https://doi.org/10.1109/ACCESS.2020.2970466

SME Corp. Malaysia. (2024). *MSME statistics: MSME performance in 2023*. https://www.smecorp.gov.my/index.php/en/policies/2020-02-11-08-01-24/sme-statistics

SME Corp. Malaysia. (2024). *SME definitions*. https://www.smecorp.gov.my/index.php/en/policies/2020-02-11-08-01-24/sme-definition

Tetteh, A. K. (2024). Cybersecurity needs for SMEs. *Issues in Information Systems*, *25*(1), 235-246. https://doi.org/10.48009/1_iis_2024_120

Wallang, M., Shariffuddin, M. D. K., & Mokhtar, M. (2022). Cybersecurity 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

Wallang, M., Shariffuddin, M. D. K., & Mokhtar, M. (2022, December 31). 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

WP Media Sdn Bhd. (2018). *SME Malaysia: Everything you need to know about SMEs in Malaysia*. https://www.walkproduction.com/blog/sme-malaysia/#:~:text=Aside%20from%20significant%20economic%20growth,Malaysia%20are%20involved%20in%20services.

Yap, B. (2023, October 10). How private and SME businesses can thrive under the Malaysia MADANI roadmap. https://www.ey.com/en_my/insights/tax/how-private-and-sme-businesses-can-thrive-under-the-malaysia-madani-roadmaps#:~:text=SMEs%20make%20up%20roughly%2097,Gross%20Domestic%20Product%20(GDP).

Zamani, E., He, Y., & Phillips, M. (2020). On the security risks of the blockchain. Journal of Computer Information Systems, 60(6), 495-506.

Zhang, L. (2023). Artificial intelligence in cybersecurity: Opportunities and challenges. IEEE Transactions on Dependable and Secure Computing, 20(1), 23-37.