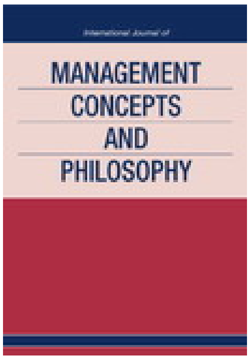
INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research



International Journal of
MANAGEMENT
CONCEPTS
AND
PHILOSOPHY

International Journal of Management Concepts and Philosophy

ISSN online: 1741-8135 - ISSN print: 1478-1484
https://www.inderscience.com/ijmcp

Digital empathy and supply chain cybersecurity challenges: concept, framework and solutions for small-medium enterprises

Anisha Banu Dawood Gani, Yudi Fernando

DOI: 10.1504/IJMCP.2022.10047679

Article History:

Received:	14 April 2022
Accepted:	18 April 2022
Published online:	03 February 2023

Digital empathy and supply chain cybersecurity challenges: concept, framework and solutions for small-medium enterprises

Anisha Banu Dawood Gani and
Yudi Fernando*

Faculty of Industrial Management,
Universiti Malaysia Pahang,
26300, Pahang, Malaysia
Email: anisharaffid@gmail.com
Email: yudi@ump.edu.my
Email: yudifernando.td@gmail.com
*Corresponding author

Abstract: Despite contributing significantly to the world's economy and being the most targeted by cybercriminals for being the weakest link in the supply chain, small-medium enterprises (SMEs) lag behind cybersecurity implementation. The budget and expertise constraint hinders them from catching up with cybersecurity initiatives. This study explores the management concept of digital empathy and proposes a solution framework for SMEs to overcome cybersecurity challenges. We found that three drivers can be the solution to overcome the cybersecurity barrier within firms' internal context, such as adequate funding, management support, and attitude towards cybersecurity risk. Our theoretical framework has also included the digital empathy approach incorporating subscription-based solutions, modular solutions, and zero-trust architecture. In addition, we suggest that the supply chain's cybersecurity systems be regularly monitored and maintained to balance cybersecurity and affordability. Furthermore, to enable future scalability, SMEs must implement the zero-trust architecture, which acts as a foundation for self-healing and self-correcting supply chain networks.

Keywords: digital empathy; cybersecurity; zero-trust architecture; COVID19; supply chain.

Reference to this paper should be made as follows: Gani, A.B.D. and Fernando, Y. (2023) 'Digital empathy and supply chain cybersecurity challenges: concept, framework and solutions for small-medium enterprises', *Int. J. Management Concepts and Philosophy*, Vol. 16, No. 1, pp.1–10.

Biographical notes: Anisha Banu Dawood Gani is an Operations Manager at a multinational manufacturing firm where she has worked for nearly 25 years. She is in her final year of her PhD program at Universiti Pahang Malaysia. Her areas of interests include cybersecurity, supply chain, technology, and operations management. She has expanded her role as an editor to several articles ranging from management to technology and looks forward to specialising in the topic of cyber supply chain and risk management in particular.

Yudi Fernando is an Adjunct Professor and holds a PhD. He is the Vice President of the Society of Logisticians, Malaysia/Pertubuhan Pakar Logistik Malaysia (LogM). He is the Editor-in-Chief of the *International Journal of Industrial Management* and *Journal of Governance and Integrity* at the

Universiti Malaysia Pahang. He previously held a managerial position in the electronics industry for several years. He has been appointed as an Honourable Lecturer at Binus University, Adjunct Professor at Faculty of Economics and Business, Universitas Airlangga, Indonesia and Visiting Professor for the postgraduate program at City University, Malaysia. He is a Research Committee Chair and founding member of the Malaysian Association of Business and Management Scholars (MABMS).

1 Introduction

Cybersecurity management is a challenge for a large multi-national company, let alone small-medium enterprises (SMEs). To make matters worse, SMEs' struggle doubles owing to fewer resources, capital, and awareness of achieving cybersecurity maturity (Bada and Nurse, 2019). However, there is an urgency now more than ever to get SME's achieve cybersecurity resilience. This is because of SME's vulnerable network; cybercriminals often target it to penetrate large manufacturing firms. Moreover, with the pandemic-enabled increase in remote connectivity, cybercriminals have fertile ground. SolarWinds cyberattack is a perfect example of how sophisticated the cyberattack has become, which had its ramification continue throughout 2021 (Bernard, 2021). With businesses, especially manufacturing, embracing digitalisation for efficiency improvements, the convergence of people, processes, and technology is needed to mitigate these risks. And so, SME's can no longer be left behind in this endeavour, especially with them representing 90% of businesses and over 50% of employment worldwide (World Bank, 2022).

SMEs are forced to implement digitalisation to keep up with the fast-paced and dynamic technological advancement. However, they are unequipped both in resources and technical expertise to prevent cyberattacks (Yudhiyati et al., 2021). Despite this, there have been many proposals and efforts to assist SME's by providing training, awareness, and education; but the cybersecurity issues with SME's persist (Bada and Nurse, 2019). Low-security budgets, a lack of cyber-skills, and a rise in cyberattacks can all have a negative impact on SME competitiveness and even endanger the value chain to which they are linked (ENISA, 2021). The ramification of this continued state is the confidentiality, integrity, and availability of sensitive data. They possess about the customer, and proprietary information cannot be upheld. This failure would ultimately affect the reputation of their business partners and their survivability if not addressed. Studies have shown that firm's ability to manage cybersecurity has a positive influence on the firm's performance (Fernando et al., 2018a). Therefore, the reverse is a true consequence of poorly managing it. Furthermore, one of the five cybersecurity trends projected is that it will become a deciding factor for supply chain partnerships, with firms increasingly considering cybersecurity resilience and exposure when deciding which partners to engage with (Bernard, 2021).

Despite staggering security advancements, the state of the rising cyberattacks trends forces one to question the ability of technology alone to address cybersecurity. While firms' spending on cybersecurity solutions has doubled from 2011 to 2019, the cybersecurity-related damages have increased six times (FBI, 2019). Moreover, they recognised the devastating impact of cyber threats on firms regardless of large or small enterprises. As a result, security analysts are calling on firms to look into ways of achieving cyber resilience. And to achieve cyber resilience in the remote work environment post-COVID-19, both the leaders, security providers and even cloud technology solutions providers are urged to employ digital empathy by Ann Johnson, corporate vice-president of Microsoft's cybersecurity solutions group (Sara, 2020). The term 'digital empathy' is a novel way of articulating the balance in cybersecurity between user experience and IT functionality.

However, a review of the current literature found no published work on digital empathy in the context of cybersecurity. As a new buzzword attracting industry players and service providers, academics must catch up and contribute to awareness and its adoption. Therefore, this paper acts as a research agenda on the subject and will outline digital empathy concepts and how it is possibly the solutions that SMEs need to address their cybersecurity posture.

2 SME and cybersecurity challenges

SMEs are defined differently in different countries and organisations. SMEs are classified as micro, small and medium enterprises, with the number of employees being the most popular denominator for a definition, followed by turnover and assets. However, the definition has been simplified broadly under two categories, namely the manufacturing and service sector. For manufacturing, the sales turnover is 15 million to 50 million or employees not exceeding 250 (SME Bank, 2017). SMEs are a big contributor in most industries and manufacturing value chains, thus having the same opportunity to embrace digitalisation as their value chain members. However, they face challenges in managing big data and the privacy and security issues with its implementation (Han and Trimi, 2022).

SMEs lack maturity and are most vulnerable in regard to their cybersecurity and resiliency (Benz and Chatterjee, 2020). While SMEs suffer the same kind of cybersecurity challenges as large businesses, they typically lack the resources to address the threats properly. Moreover, some SMEs have an unfounded perception that cybersecurity will not affect them as larger firms possess data that would be more attractive to cybercriminals. Therefore, only a few SMEs invest in cybersecurity technologies (Cimini et al., 2021).

The topic of cybersecurity and SMEs is rich in the literature. Thus scholars have generally noted the vulnerability of SMEs who were becoming a frequent target for cyberattacks (e.g., Zec and Kajtazi, 2015). However, some SMEs may have considerably higher profiles than others, making them a more appealing target for attackers, who may use a variety of attack channels and capabilities (Lewis et al., 2014). Moreover, the geographical location of the SMEs, particularly from developing countries that were regarded to have weaker security systems are more prone to attacks (Yudhiyati et al., 2021). Despite the vulnerability, lack of investment, budget constraints and technical disability are continued to be cited as the major causes of SME cybersecurity issues (Fernando et al., 2022), which can stem from a lack of security awareness among SME owners and a lack of cost-effective practices (Shojaifar et al., 2018).

Past studies have attempted to classify factors that influence cybersecurity adoption among SMEs (Kabanda et al., 2018), taxonomies for identifying risk categories (Lewis et al., 2014), models or framework on SME's character that determines their approach to security adoption or avoidance (e.g., Browne et al., 2015), SME's maturity evaluations (Cholez and Girard, 2014) and even evaluating how security standards can be customised for small firms (Valdevit et al., 2009). However, despite the contributions and discovery, SMEs remain the weakest supply chain member, putting focal firms at risk. For example, it was reported that SMEs are subjected to 350% more social engineering attacks than larger corporations (Edward, 2022). Therefore, SMEs need to build sufficient capacity to handle thorny cybersecurity issues (Fernando et al., 2020).

SMEs face many challenges ranging from lack of awareness of cyber threats, lack of budget for adopting security solutions, lack of technical expertise and even poor security culture. This makes them more exposed to spear-phishing attacks, which cybercriminals are exploiting. Hence, security analysts and academia urge firms, especially SMEs, to invest in cybersecurity, either from education and awareness building perspectives or by purchasing off-the-shelf solutions to mitigate its challenges. However, while seemingly accurate, this approach has not yielded the intended result. And the reason for this is attributed to the fact that the cybersecurity solutions provider understands neither the SME context nor requirements (Shojaifar et al., 2018). Hence, there's a need for digital empathy on the part of service provider's tools and technologies to assist SMEs in addressing cybersecurity challenges.

3 Method

A reproducible literature search was done on Emerald and ScienceDirect (Elsevier) database with keywords' cybersecurity AND digital empathy' and 'digital empathy AND SME' in the title from 2012 to 2022. However, the search yielded zero suitable titles affirming the infancy stage of the concept among researchers. But when searched using 'digital empathy' alone, results were found. However, the literature revolved around media literacy, pedagogy, and digital health. Therefore, it is perceived that digital empathy within the cybersecurity context is still new and has not attracted much attention among scholars. But there is a pressing need for a clear concept of digital threat. Furthermore, it is vital to empirically explore and test the concept validity and actual adoption behaviour among industry players. Therefore, this study sets the precedence by inviting scholars to converge knowledge from the industry and academia to build theory and identify the use cases, barriers, challenges, and motivations for its adoption.

Table 1 Keyword and search results from Emerald and ScienceDirect

Keyword	*Year*	*Emerald*	*ScienceDirect (Elsevier)*
Cybersecurity AND (digital empathy)	2012–2022	Zero titles related to digital empathy and cybersecurity	
Digital empathy AND (SME)	2012–2022	Zero titles related to digital empathy and SME	

4 Results

4.1 Digital empathy

One of the reasons for the imbalance between rising expenditure for security solutions and an equally rising number of attacks is the lack of empathy. Security vendors are developing solutions based on the threat categories but fail to solicit feedback from their prospects or customers. Not understanding the customer requirements results in solutions that are either unmatched to their needs or too costly to afford. Hence, SMEs are often left out, citing budget, expertise, and awareness. This is why the security experts advocate a digitally empathetic approach to offering security solutions to customers, particularly SMEs. According to a security analyst from ViewQwest, there are many cybersecurity solutions available to large enterprises, but few are designed to cater to the cybersecurity needs of SMEs (Vignesa, 2022).

Digital empathy arises due to the existing commercial security solutions' inability to cater to firms with varying sectors and sizes. It entails considering how regular people interact with technology and ensuring that security is integrated into their working practices rather than cybersecurity experts (Business World, 2021). Rather than offering a catalog solution based on external knowledge of a threat; service providers need to understand:

a the SMEs motivation for wanting a protection

b the type of protection most suited to the nature and size of their business

c the features more valuable to their immediate need and above all

d a solution that caters for their budget and is scalable.

Digital empathy urges security vendors to focus first and foremost on the criticality of the cyber threat situation and its impact on society and nations ahead of making a profit. In other words, protecting the security of the critical infrastructure is everyone's responsibility, which will impact the nation if left unsecured. So, the paradigm shift here is to offer ways to make it possible for firms, especially SMEs, to adopt security solutions. Thus, with digital empathy in the field of cybersecurity, digital solutions can be more inclusive and adaptive and can adapt to a wide range of people's ever-changing situations.

Within the firm's context, insider risk reduction and organisational resilience require digital empathy, which is increasingly a frontline defence in information security. It is crucial for employee trust, morale, and loyalty, and it's at the heart of some of the world's most widely used technology. Negative deterrence measures such as employee limitations, monitoring, and punishment, according to Carnegie Mellon University's (2019) Security, do not minimise insider risk. What works is prioritising employee engagement, connection, and well-being.

4.2 Benefits of digital empathy

It takes a digital community to keep up with cyber threats, and so with digital empathy, the process gets better and more beneficial to everyone involved. Some of the benefits reported by industry experts, as reported in Caroline (2021), are as follows:

1. Digital empathy inspires solution providers to think out of the box and be creative and flexible in their product offerings.
2. Trust is enhanced through digital empathy. Both the service providers and the SMEs need to put their customers' needs in mind when tailoring a solution effectively. A personal touch can go a long way in helping prospective clients feel secure in the knowledge that their interests and information are being safeguarded under the care of their selected cybersecurity firm.
3. The scalable feature is enabled through digital empathy. Acknowledging that change is the only 'constant' in life or business, businesses should be ready to embrace those changes with a process and systems that are adjustable.
4. Reduced dependencies on the workforce to police security threat detections; rather, it is handled through a system. For example, Microsoft uses Insider Risk Management software to leverage signals from Windows 10 to detect anomalies; without having to configure, manage or maintain them physically.

5 Ways to achieve digital empathy

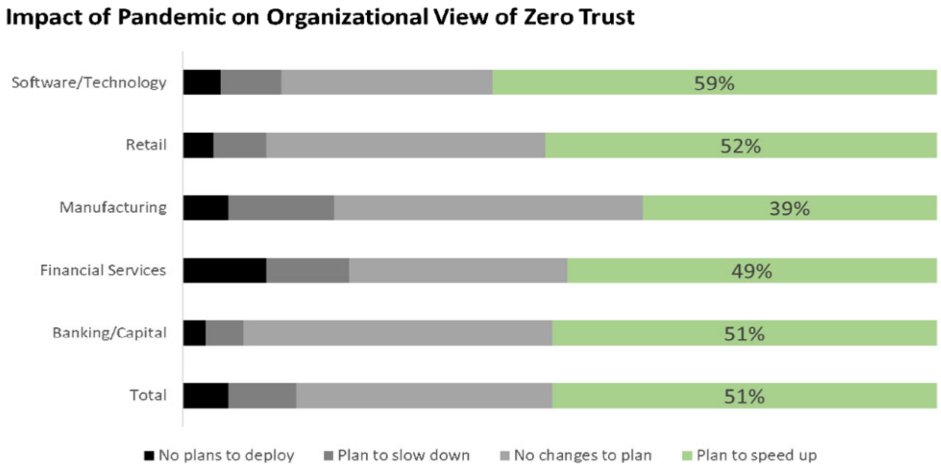
There are three essential approaches to achieving digital empathy, namely:

1. *Subscription-based service:* SMEs need an accessible subscription-based service instead of making upfront investments into hardware for cost efficiency. This would require customised, smaller solutions in scale and easier to deploy and manage to address the potential lack of in-house cybersecurity expertise. Past studies have advocated that firms select and apply the best technique which fits their firms' capacity and capability (Fernando and Tew, 2016).
2. *Modular security packages:* Rather than taking a premium solution package offer, SMEs should be offered the flexibility to customise the product based on the user's role and context to ensure that the client can utilise it without difficulty. Accordingly, the modular application would result in a cheaper cost for the SMEs Thus. Moreover, it can be adopted in stages, therefore not depriving the SMEs of securing their network.
3. *'Zero-trust' architecture:* Zero-trust architecture implementation is gaining popularity to defend and deter cyber threats or cybercrime (Alagappan et al., 2022). The zero-trust approach assumes every access request is a possible breach. This multi-factor authentication should be employed for anyone in the firm. Each employee or device associated with the access is monitored and given a risk score. Any suspicious activity or increase in attempts to deviate from the norm is evaluated. Risk scoring and evaluation are transparent to the user by the tool itself. The

simplicity of the tool and processes for risk assessment goes hand in hand with digital empathy.

Post-pandemic, only 51% of the businesses are planning to accelerate zero-trust adoption (Figure 1). The rest of the firms are expected to catch up as it is predicted that zero-trust will become the industry standard (Russel, 2021). This architecture necessitates a well-thought-out strategy and roadmap for implementing and integrating security measures in order to achieve certain business goals. SMEs must establish an organisation-wide commitment to adopt this architecture, including cataloguing critical data assets and touchpoints for controlled access. Although initial preparatory work seems like a limiting process, in the long run, successful implementation of zero-trust architecture can result in a rapid view of the attack surface.

Figure 1 Zero-trust architecture is adopted by industry (see online version for colours)

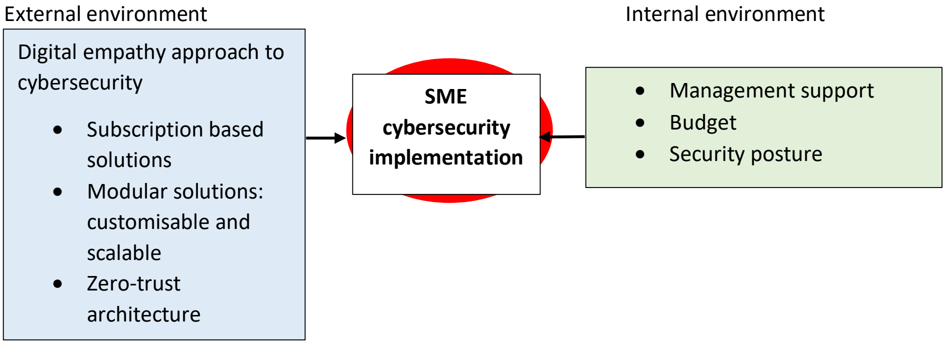


Source: Russel (2021)

6 Discussion – conceptualising digital empathy framework for SMEs

In reviewing literature from academia and industry on barriers for SMEs to adopt cybersecurity solutions and the clarion call for a shift into digital empathy solutions, this study proposes a digital empathy framework for SMEs as depicted in Figure 2. This framework agrees with Kabanda et al. (2018). The three main factors that act as barriers within firms' internal context are management support, adequate funding, and attitude towards cybersecurity risk translated as the firm's security posture. Management support is the critical factor for setting the security tone within the firm. It has been reported that management's commitment and clear vision inspire employees to embrace technology and the proposed culture (Fernando et al., 2018b). Coupling this with digital empathy solutions that offer subscription-based, modular solutions that are cost-effective and not dependent on human resources for constant monitoring and regular maintenance, the SMEs are expected to balance cybersecurity and affordability. Furthermore, to enable future scalability, SMEs must implement the zero-trust architecture, which acts as a foundation for self-healing and self-correcting supply chain networks.

Figure 2 Conceptual framework on digital empathy for SME (see online version for colours)


External environment
Digital empathy approach to cybersecurity
• Subscription based solutions
• Modular solutions: customisable and scalable
• Zero-trust architecture
SME cybersecurity implementation
Internal environment
• Management support
• Budget
• Security posture

7 Limitations and future direction

This paper is conceptual in nature, given the infancy stage of the term digital empathy. Thus, the framework proposed in this study needs to be enhanced, adjusted, or amended as more knowledge on the topic emerges. A case study approach is recommended to achieve an in-depth understanding of the digital empathy concepts and evaluate the extent of its offerings to SMEs. The case study is also useful in this exploratory context to add to the depth and understanding of the concepts. Similarly, an empirical study is also requested to test the framework with validated instruments for the questionnaire. Digital empathy offers vast opportunities for researchers, so it is the hope of this study that it acts as a propeller toward that objective.

8 Conclusions

Despite contributing significantly to the world's economy and being the most targeted by cybercriminals for being the weakest link in the supply chain, SMEs lag behind cybersecurity initiatives. The budget and expertise constraint hinders them from catching up with cybersecurity initiatives. Recognising the changes post-Covid19 with increased connectivity and remote access, security experts are calling for digital empathy. Digital empathy revolves around making technology user friendly, flexible, and scalable. To achieve digital empathy, security vendors need to devise packages that are subscription-based, modular and utilising zero cost architecture. In addition, the SMEs' top management must internally ensure the organisation's commitment to adopt a cybersecurity mindset, allocate budget, and establish a security posture favourable for cybersecurity solutions.

Acknowledgements

The authors would like to thank the Division of Research and Innovation at Universiti Malaysia Pahang for funding this study (RDU1903126; UIC211502; RDU212701).

References

Alagappan, A., Venkatachary, S.K. and Andrews, L.J.B. (2022) 'Augmenting zero trust network architecture to enhance security in virtual power plants', *Energy Reports*, Vol. 8, No. 1, pp.1309–1320.

Bada, M. and Nurse, J. (2019) 'Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs)', *Information and Computer Security*, Vol. 27, No. 3, pp.393–410.

Benz, M. and Chatterjee, D. (2020) 'Calculated risk? A cybersecurity evaluation tool for SMEs', *Business Horizons*, Vol. 63, No. 4, pp.531–540.

Bernard, M. (2021) 'The five biggest cyber security trends in 2022', *Forbes*, 17 December [online] https://www.forbes.com/sites/bernardmarr/2021/12/17/the-five-biggest-cyber-security-trends-in-2022/?sh=61cb4f7c4fa3 (accessed 18 April 2022).

Browne, S., Lang, M. and Golden, W. (2015) 'Linking threat avoidance and security adoption: a theoretical model for SMEs', *InBled EConference*, Vol. 1, No. 1, pp.32–43.

Business World (2021) 'Digital empathy' needed to combat rising cyberthreats', *Business World* [online] https://www.bworldonline.com/technology/2021/12/06/415479/digital-empathy-needed-to-combat-rising-cyberthreats/ (accessed 18 April 2022).

Carnegie Melon University (2019) *Common Sense Guide to Mitigating Insider Threats*, 6th ed., CMU CERT National Insider Threat Center [online] https://resources.sei.cmu.edu/asset_files/TechnicalReport/2019_005_001_540647.pdf (accessed 18 April 2022).

Caroline, C. (2021) 'Digital empathy – part 2', *Aindale Business and Technology*, 24 May [online] https://www.aindale.co.uk/digital-empathy-part-2/ (accessed 18 April 2022).

Cholez, H and Girard, F. (2014) 'Maturity assessment and process improvement for information security management in small and medium enterprises', *Journal of Software: Evolution and Process*, Vol. 26, No. 5, pp.496–503.

Cimini, C., Boffelli, A., Lagorio, A., Kalchschmidt, M. and Pinto, R. (2021) 'How do Industry 4.0 technologies influence organisational change? An empirical analysis of Italian SMEs', *Journal of Manufacturing Technology Management*, Vol. 32, No. 3, pp.695–721.

Edward, S. (2022) 'Small businesses are more frequent targets of cyberattacks than larger companies: new report', *Forbes*, 16 March [online] https://www.forbes.com/sites/edwardsegal/2022/03/30/cyber-criminals/?sh=122218bb52ae (accessed 18 April 2022).

European Union Agency for Cybersecurity (ENISA) (2021) *SME Cybersecurity* [online]. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/sme_cybersecurity (accessed 18 April 2022).

Federal Bureau of Investigation (FBI) (2019) *2019 Internet Crime Report* [online] https://www.ic3.gov/Media/PDF/AnnualReport/2019_IC3Report.pdf (accessed 18 April 2022)

Fernando, Y, and Tew, M.M. (2016) 'Reverse logistics in manufacturing waste management: the missing link between environmental commitment and operational performance', *International Journal of Integrated Supply Management*, Vol. 10, Nos. 3–4, pp.264–282.

Fernando, Y., Chidambaram, R.R.M. and Wahyuni-TD, I.S. (2018a) 'The impact of big data analytics and data security practices on service supply chain performance', *Benchmarking*, Vol. 25, No. 9, pp.4009–4034.

Fernando, Y., Bee, P.S., Jabbour, C.J.C. and Thomé, A.M.T. (2018b) 'Understanding the effects of energy management practices on renewable energy supply chains: implications for energy policy in emerging economies', *Energy Policy*, Vol. 118, No. 1, pp.418–428.

Fernando, Y., Wahyuni-TD, I.S., Gui, A., Ikhsan, R.B., Mergeresa, F. and Ganesan, Y. (2022) 'A mixed-method study on the barriers of Industry 4.0 adoption in the Indonesian SMEs manufacturing supply chains', *Journal of Science and Technology Policy Management*, ahead-of-print.

Fernando, Y., Zainul Abideen, A. and Shaharudin, M.S. (2020) 'The nexus of information sharing, technology capability and inventory efficiency', *Journal of Global Operations and Strategic Sourcing*, Vol. 33, No. 4, pp.327–351.

Han, H. and Trimi, S. (2022) 'Towards a data science platform for improving SME collaboration through Industry 4.0 technologies', *Technological Forecasting and Social Change*, Vol. 174, No. 1, p.121242.

Kabanda, S., Tanner, M. and Kent, C. (2018) 'Exploring SME cybersecurity practices in developing countries', *Journal of Organizational Computing and Electronic Commerce*, Vol. 28, No. 3, pp.269–282.

Lewis, R., Louvieris, P., Abbott, P., Clewley, N. and Jones, K. (2014) 'Cybersecurity information sharing: a framework for information security management in UK SME supply chains', *ECIS 2014 Proceedings – 22nd European Conference on Information Systems* [online] http://www.scopus.com/inward/record.url?eid=2-s2.0-84905852035&partnerID=40&md5=02635f982ee12cd0c49447161597a238 (accessed 18 April 2022).

Russel, C. (2021) *New Data from Microsoft shows how the Pandemic is accelerating the Digital Transformation of Cyber-security*, Microsoft, February 26 [online] https://news.microsoft.com/en-nz/20Bern21/02/26/new-data-from-microsoft-shows-how-the-pandemic-is-accelerating-the-digital-transformation-of-cyber-security/ (accessed 18 April 2022).

Sara, B. (2020) *Interview: Microsoft's Ann Johnson on Digital Empathy and Zero Trust*, Security Brief Asia [online] 29 July [online] https://securitybrief.asia/story/interview-microsoft-s-ann-johnson-on-digital-empathy-and-zero-trust (accessed 18 April 2022).

Shojaifar, A., Fricker, S.A. and Gwerder, M. (2018) 'Elicitation of SME requirements for cybersecurity solutions by studying adherence to recommendations', *CEUR Workshop Proceedings*, p.2075.

SME Bank (2017) [online] https://www.smebank.com.my/en/about-us/sme-definition (accessed 18 April 2022).

Valdevit, T., Mayer, N. and Barafort, B. (2009) 'Tailoring ISO/IEC 27001 for SMEs: a guide to implement an information security management system in small settings', *Communications in Computer and Information Science*, Vol. 42, No. 1, pp.201–212.

Vignesa, M. (2022) 'Cybersecurity gap threatens SMEs following digitalisation', *Focus Malaysia*, 6 February [online] https://focusmalaysia.my/cybersecurity-gap-threatens-smes-following-digitalisation/ (accessed 18 April 2022).

World Bank (2022) [online] https://www.worldbank.org/en/topic/smefinance (accessed 18 April 2022).

Yudhiyati, R., Putritama, A. and Rahmawati, D. (2021) 'What small businesses in developing country think of cybersecurity risks in the digital age: Indonesian case', *Journal of Information, Communication and Ethics in Society*, Vol. 19, No. 4, pp.446–462.

Zec, M. and Kajtazi, M. (2015) 'Examining how IT professionals in SMEs take decisions about implementing cyber security strategy', *Proceedings of the European Conference on IS Management and Evaluation, ECIME*, pp.231–239.