ISSN 2320 -2610

Volume 14, No. 1, January – February 2025

International Journal of Multidisciplinary in Cryptology and Information Security

Available Online at http://www.warse.org/IJMCIS/static/pdf/file/ijmcis011412025.pdf

https://doi.org/10.30534/ijmcis/2025/011412025

Enhancing Cybersecurity Readiness in SMEs: Addressing Resource Constraints and Policy Gaps through Scalable Solutions and IT Investments

Opeyemi Isaiah Enitan[1,2]

[1]Manchester Metropolitan University, United Kingdom, yenitan1@yahoo.com

[2]Covenant University, Ogun State, Nigeria, yenitan1@yahoo.com

Received Date : December 25, 2024 Accepted Date : January 26, 2025 Published Date : February 07, 2025

ABSTRACT

This study investigates cybersecurity readiness in Small and Medium Enterprises (SMEs), an important yet understudied concern in light of rising cyber threats. Utilising survey responses from 63 SMEs from various industries, the research discovers significant challenges such as financial constraints, limited expertise, and insufficient employee awareness. The findings reveal substantial gaps in policy adoption and risk assessment practices with larger SMEs typically more prepared. Regression analysis identifies IT infrastructure investment as the most significant variable impacting readiness, while cross-tabulation reveals differences in policy adoption across organisational sizes. This study emphasises the critical necessity for SMEs to implement customised, cost-effective cybersecurity measures to reduce risks and maintain continuous operations. By addressing these gaps, SMEs can enhance their resilience, safeguard their digital assets, and contribute to the stability of broader economic systems. Recommendations focus on scalable solutions, policy integration, and external support to bridge existing vulnerabilities.

Key words: Cybersecurity Readiness, Cyber Threats, Policy Adoption, Risk Mitigation, Small and Medium Enterprises (SMEs)

1 INTRODUCTION

Recent national and international cybersecurity reports highlight a concerning trend: cyberattacks are becoming more widespread and sophisticated. These attacks often exploit vulnerabilities tied to human errors, and as businesses increasingly depend on technology for their critical operations, cybersecurity has become essential for ensuring their continuity [1]. In today's integrated business world, safeguarding a company's digital assets, ensuring business continuity, and maintaining customer confidence are essential [2]. Both domestic and international economies depend extensively on small and medium enterprises SMEs. 99.9% of all firms are small businesses, with 32.5 million small businesses in the U.S. alone employing 61.2 million people [3]. Economic growth, job creation, and innovation are all driven by SMEs. However, almost all net job creation is due to the expansion of existing enterprises [4]. A business is classified as a SME if it employs less than 1500 people and makes less than $38.5 million a year [5]. In cybersecurity, SMEs face specific challenges despite their economic significance. Many are at risk of cyberattacks because they lack the infrastructure, expertise, and resources necessary to safeguard their systems and data [6]. Due to their significance, it is crucial to make sure SMEs are prepared for cybersecurity. SMEs are particularly vulnerable to the rapid trend of cybercrime due to the increasing digitalisation of services and interconnectedness of systems. Cyberattacks against businesses of all sizes have increased as a result of the rapid growth of internet-based businesses [7]. Cyberattacks, which initially focused on basic disruptions such as viruses and worms, have evolved into more complex threats, including large-scale data breaches and ransomware attacks driven by financial gain [7, 8]. In addition, organisations' defence measures are further complicated by the fact that nation-states and organised crime groups have emerged as major actors in cybercrime [9]. In this evolving threat situation, SMEs, with their less effective defences, have become major targets for cybercriminals [10, 11]. Information Systems (IS) are crucial in strengthening an SME's competitive edge by improving information capture and data flow [12, 13]. Furthermore, because many SMEs are part of larger businesses' supply chains, a cyberattack on one can have far-reaching consequences across all sectors [14]. Cybersecurity refers to a set of techniques, technologies, and methods intended to secure systems, networks, data, and software against unwanted activity [15, 16]. Implementing comprehensive cybersecurity policies is critical for SMEs to safeguard their assets and ensure their long-term success. This study emphasises the crucial necessity of cybersecurity readiness for SMEs, focussing on the economic and operational effects of inadequate protection. The research aims to evaluate the current state of cybersecurity readiness among SMEs, with a focus on technical and strategic challenges. Utilising survey data from 63 SMEs, the research identifies significant threats, investigates the importance of IT infrastructure, and evaluates the effectiveness of current cybersecurity measures.

1.1 Challenges in Cybersecurity for SMEs

SMEs face significant challenges in implementing comprehensive cybersecurity safeguards due to their limited resources. According to Alahmari and Duncan [10] financial constraints and a lack of technical expertise placed SMEs at a disadvantage when compared to larger enterprises. SMEs are particularly vulnerable to cyberattacks because of this resource gap, which frequently leads to inadequate cybersecurity infrastructure. Additionally, many SMEs are unaware of the magnitude of the cybersecurity risk they face. According to Heidt, Gerlach, and Buxmann [11] many SMEs underestimate the probability and impact of cyberattacks because they think their smaller size makes them less attractive to attackers. This misperception creates a false sense of security, making SMEs vulnerable to threats like ransomware and data breaches. According to a survey conducted by the European Union Agency for Cybersecurity [17], only 10% of SMEs have a formal cybersecurity strategy, with the majority relying on outdated or basic measures. A lack of cybersecurity knowledge is another recurring problem. Walczuch *et al*. [12] noted that SMEs frequently use ad hoc security measures rather than systematic frameworks due to insufficient expertise. This reactive approach contributes to their vulnerability since they lack the knowledge to predict and mitigate threats properly. Furthermore, Rawindaran *et al*. [18] highlighted gaps in cybersecurity governance and policy among SMEs, advocating methods to improve awareness, education, and regulatory frameworks to address cyberattacks.

1.2 Strategies for Cybersecurity Readiness in SMEs

Recognising the significance of customised methods, academics have highlighted the need for scalable and cost-effective solutions for SMEs. Rezaei, Ortt, and Trott [14] proposed that simple but effective frameworks can greatly improve SMEs' cybersecurity capability. Such frameworks enable SMEs to incorporate security measures without affecting their operations, providing resilience to evolving threats. Another essential part of readiness is the integration of cybersecurity into overall company objectives. Fernandez de Arroyabe *et al*. [15] advocated for continuous evaluation and adaptation of cybersecurity measures to address the dynamic nature of cyber threats. This technique is important for SMEs, which lack the substantial infrastructure of larger enterprises. Babiceanu and Seker [16] advocated a risk-based approach, prioritising key assets to allocate resources and manage the most pressing threats. Additionally, integrating IT infrastructure and investment is critical to improving cybersecurity readiness. Hasan *et al*. [19] and Fasasi [20] emphasised that well-resourced IT infrastructures help to increase security and prevent breaches. Kong *et al*. [21] and Hsu *et al*. [22] reiterated this sentiment, stating that organisations with robust IT capabilities had effective information security management. Investing in IT resources increases SMEs' security measures while also lowering the long-term expenses connected with cyber incidents. The importance of cybersecurity frameworks in increasing organisational resilience cannot be emphasised. Pereira and Santos [23] emphasised the importance of integrating security functions with organisational policies and standards. Their research showed the importance of conducting regular audits to ensure compliance and effectiveness. Klimburg [24] observed that major countries such as the United States, United Kingdom, and Australia have formalised cybersecurity plans, which serve as models for SMEs to establish their own localised approaches.

1.3 Socio-Technical Approaches to Cybersecurity

The interaction of technical solutions and organisational practices is the foundation of socio-technical approaches to cybersecurity. Van Haastrecht *et al*. [25] proposed an integrated framework that blends technical tools with cultural changes inside organisations. This approach emphasises the importance of developing a cybersecurity culture, which is important for SMEs with minimal technical expertise. Cybersecurity threats are especially concerning for sectors such as online retail, where organisations regard cyberattacks as one of the most serious threats to corporate operations. Hui, Kim, and Wang [26] discovered that Distributed Denial of Service (DDoS) assaults frequently target banks, telecommunications businesses, and financial institutions for financial reasons. According to PWC [27], the average cost of a cybersecurity incident, including operational disruptions and data loss, is around £857,000. Despite the high risks, UK organisations lag behind their foreign rivals in preventing cyberattacks, underscoring the need for enhanced measures. Effective countermeasures combine technical, organisational, and human aspects. Uma and Padmavathi [28] emphasised the necessity of understanding cyberattacks and establishing suitable controls. According to Duchek [29] and Ferdinand [30], organisational resilience requires readiness in the form of business continuity plans, vulnerability assessments, and employee training. These procedures ensure a prompt and coordinated reaction to incidents, hence reducing disruption.

The concept of cyber resilience goes beyond prevention to include recovery and adaptation. According to Annarelli, Nonino, and Palombi [31], learning from past incidents allows organisations to optimise systems and improve future reactions. Similarly, Linkov *et al*. [32] proposed resilience metrics to assess and improve systems' ability to withstand cyber attacks. For SMEs, implementing such comprehensive frameworks is critical for managing the complexity of cybersecurity. Several significant studies have emphasised the diverse problems and threats businesses face in the evolving cybersecurity environment. Luo [33] offered a risk assessment paradigm centred on digital interdependence and regulatory difficulties, whereas Kshetri [34] examined worldwide cybercrime patterns. Hudakova *et al*. [35] recognised cyber events as a major business risk, especially for SMEs with limited defences. August, Dao, and Niculescu [36] and Say and Vasudeva [37] investigated the economic implications of cyberattacks, emphasising the importance of proactive risk mitigation techniques.

1.4 Materials and Methods

This study utilised a quantitative research methodology to assess the cybersecurity readiness of Small and Medium Enterprises (SMEs). The primary data collection instrument was a structured survey questionnaire, which provided a systematic way to collect empirical data from respondents. This method allowed for the identification of trends, relationships, and factors influencing SMEs' cybersecurity practices, which aligned with the research objective of assessing technological resistance to cyber threats. The questionnaire was carefully designed to cover three major topics: organisational demographics, cybersecurity challenges, and current strategies for strengthening cybersecurity readiness. A total of 100 SMEs across various industries were contacted for this study. Participants were selected using a stratified random sampling technique to ensure a diverse representation of organisations based on size, sector, and geographic location. Out of the 100 SMEs contacted, 63 responded, resulting in a response rate of 63%. The sample size was considered sufficient for statistical analysis and for drawing significant conclusions about the state of cybersecurity readiness in SMEs. The survey utilised multiple-choice questions to obtain categorical and interval data for comprehensive analysis.

The collection of data was conducted over four weeks. The survey was delivered by email and internet platforms, with clear instructions and assurances of confidentiality to promote genuine involvement. The structured questionnaire was organised into three sections. The first section obtained demographic and organisational information, such as the size of the company, the number of employees, and the state of IT infrastructure development. The second section concentrated on cybersecurity challenges, gathering data on perceived risks, types of cyber threats encountered, and current security policies. The final section focused on cybersecurity strategies, including analysing the framework utilised, alignment with company objectives, investment in IT infrastructure, and employee training. The data collected were analysed with the Statistical Package for the Social Sciences (SPSS), an effective statistical analysis software. Descriptive statistics, such as means, medians, and frequency distributions, were used to summarise the sample's demographic characteristics and overall level of cybersecurity readiness. Inferential statistical approaches were also used to determine the relationships between variables. For example, regression analysis was utilised to examine the impact of IT investment and employee training on cybersecurity readiness, while cross-tabulation analysis evaluated the relationship between organisational size and the presence of formal cybersecurity policy.

2 RESULTS AND DISCUSSION

2.1 Organisational Demographics

The survey comprised 63 small and medium enterprises (SMEs) categorised by size and industry. 50% (32 SMEs) were small businesses with 10-50 employees, 30% (19 SMEs) were micro-enterprises with fewer than 10 employees, and 20% (12 SMEs) were medium-sized businesses with 51–250 employees. In terms of revenue, 48% (30 SMEs) indicated annual revenues of $1 million to $10 million, 35% (22 SMEs) indicated revenues less than $1 million, and 17% (11 SMEs) indicated revenues greater than $10 million. The distribution across industries revealed that 40% (25 SMEs) worked in the services sector, 35% (22 SMEs) in retail, and 25% (16 SMEs) in manufacturing. Regarding IT infrastructure, 60% (38 SMEs) classified their systems as intermediate, 25% (16 SMEs) as basic, and 15% (9 SMEs) as advanced. According to the survey, larger businesses were more likely to have formal policies in place, with 50% of medium enterprises, 25% of small enterprises, and only 15.8% of micro-enterprises adopting such policies (see Figure 1).

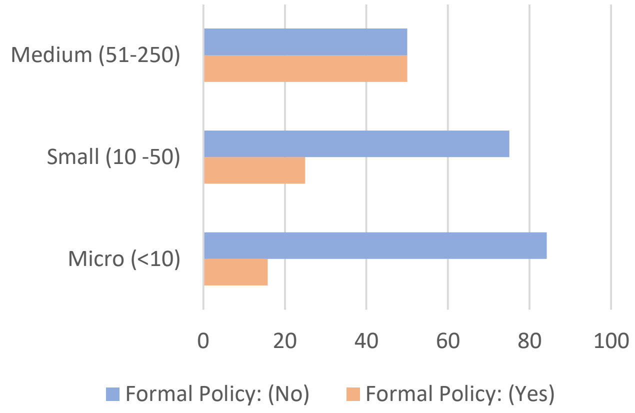

Figure 1: Proportion of SMEs with cybersecurity by size

2.2 Cybersecurity Challenges and Risks

The SMEs surveyed indicated various levels of confidence in their cybersecurity preparedness. Only 25% (16 SMEs) considered confident in their abilities to defend against cyberattacks, with 45% (28 SMEs) neutral and 30% (19 SMEs) lacking confidence. Furthermore, 40% (25 SMEs) had experienced a cyberattack in the previous year, with phishing (32%) and malware infections (28%) being the most common threats. Participants indicated three key challenges: financial constraints (38%), limited technical expertise (32%), and insufficient employee awareness (30%). Figure 2 illustrates these challenges, with financial constraints being the most major challenge, followed by problems relating to technical expertise and employee training.

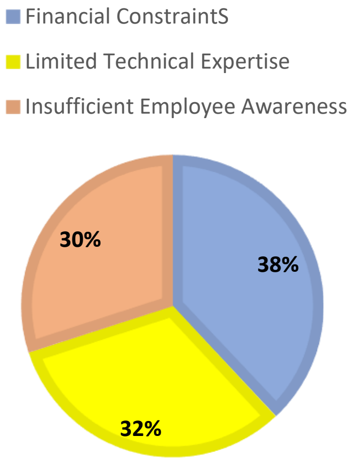

Figure 2: Distribution of cybersecurity challenges

2.3 Cybersecurity Strategies and Practices

Only 27% (17 SMEs) indicated formal cybersecurity policies, suggesting that structured approaches to cybersecurity are not widely used. 18% (11 SMEs) updated their cybersecurity tools weekly or more, whereas a greater percentage (42%; 26 SMEs) updated them quarterly. Despite these efforts, 57% (36 SMEs) allocated less than 5% of their IT budget to cybersecurity. Employee training was inadequate with only 20% (13 SMEs) regularly providing training. Furthermore, 52% (33 SMEs) never conducted cybersecurity risk assessments, and only 22% (14 SMEs) performed such assessments annually. Figure 3 indicates that cybersecurity readiness scores are better for SMEs with advanced IT infrastructure. An average readiness score of 1.5 was indicated by 16 SMEs with basic IT infrastructure, indicating limited practices including low policy adoption and infrequent updates or training. The average score for 38 SMEs with intermediate IT infrastructure was 2.0, indicating balanced but inadequate practices. However, SMEs with advanced IT infrastructure (9 SMEs) indicated the highest level of readiness, with an average score of 2.8, indicating their robust systems and proactive measures.

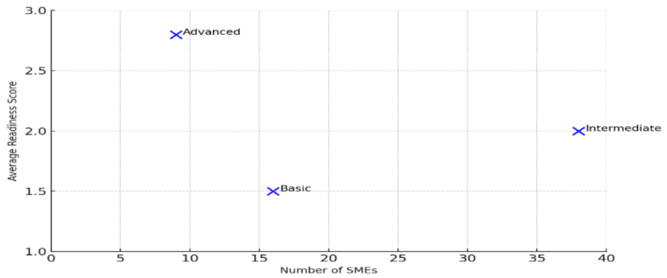

Figure 3: Correlation Between IT Infrastructure Levels and Cybersecurity Readiness

2.4 Inferential Statistics

Regression analysis was conducted to identify the factors that significantly predict cybersecurity readiness among SMEs. The regression model used the formula:

$$Y=\beta_0+\beta_1X_1+\beta_2X_2+\beta_3X_3+\epsilon \qquad (1)$$

Where:

Y: Cybersecurity readiness
β0: Intercept
X1: IT infrastructure level ($\beta1 = 0.52$, $p < 0.01$)
X2: Budg*et al*location ($\beta2 = 0.35$, $p < 0.05$)
X3: Employee training ($\beta3 = 0.28$, $p < 0.05$)
ϵ: Error term

The findings show that the most significant indicator of cybersecurity readiness is the level of IT infrastructure ($\beta = 0.52$, $p < 0.01$), which is followed by budg*et al*location ($\beta = 0.35$, $p < 0.05$) and employee training ($\beta = 0.28$, $p < 0.05$). These findings highlight how essential resource allocation is to strengthening cybersecurity resilience.

2.5 Cross-Tabulation Analysis

Cross-tabulation analysis examined the relationship between organisational size and the presence of formal cybersecurity policies. The results are presented in the table below:

Table 1: Organisational Size and Formal Cybersecurity Policy Adoption

Organisational Size	Formal Policy (Yes)	Formal Policy (No)	Total
Micro (<10)	3	16	19
Small (10 -50)	8	24	32
Medium (51-250)	6	6	12
Total	17	46	63

The findings indicated that as an organisation's size improved, so did the likelihood of having a formal cybersecurity policy. Only 15.79% (3 SMEs) of micro-enterprises had formal policies, compared to 50% (6 SMEs) of medium-sized businesses and 25% (8 SMEs) of small businesses.

2.6 Chi-Square Test

The Chi-square test was used to evaluate the statistical significance of the relationship between organisational size and the adoption of formal cybersecurity policies. The Chi-square statistic is calculated using the formula:

$$\chi^2 = \sum \frac{(O-E)^2}{E} \qquad (2)$$

Where:

X^2: Chi-square statistic
O: Observed frequency (from the sample)
E: Expected frequency (calculated under the assumption of independence)

$$E = \frac{Row\ Total\ x\ Column\ Total}{Ground\ Total} \qquad (3)$$

The Chi-square result ($X^2 = 18.76$, $p < 0.01$) indicates a statistically significant relationship between Organisational size and policy adoption, suggesting that larger SMEs are more likely to adopt formal cybersecurity policies.

2.7 Discussion

The findings of this study indicate substantial gaps in SMEs' cybersecurity readiness, which is consistent with previous studies on this topic. Only 27% of SMEs indicated that they had a formal cybersecurity policy, aligning with ENISA [17], which found that the majority of SMEs lack structured cybersecurity frameworks. This gap is compounded by resource limitations, as noted by Alahmari and Duncan [10], who stressed that financial and technical constraints render SMEs vulnerable to cyber threats. The significance of investing in IT infrastructure in enhancing cybersecurity readiness is highlighted by the regression analysis. The results of Hasan *et al*. [19] and Kong *et al*. [21], who found that IT infrastructure is a crucial enabler of information security management, were supported by significantly higher readiness scores of SMEs with advanced IT systems. Despite its importance, widespread underinvestment in technology resources is evident in the majority of SMEs surveyed indicating intermediate or basic IT systems.

Additionally, the study highlights the influence of organizational size on cybersecurity policy adoption. Cross-tabulation analysis showed that medium-sized SMEs were far more likely to implement formal policies compared to micro-enterprises. This supports the findings of Heidt *et al*. [11], who noted that larger enterprises are better equipped to allocate resources to thorough security measures. According to 38% of respondents, financial constraints were a significant challenge. This finding is consistent with that of Babiceanu and Seker [16], who highlighted the necessity of customised SMEs cybersecurity solutions that are both scalable and cost-effective. The findings of Fernandez de Arroyabe *et al*. [15], who argued for incorporating training programs into organisational procedures, are similarly consistent with the limited employee awareness and expertise that 32% of participants indicated.

3 CONCLUSION

This study emphasises the critical need for SMEs to prioritise cybersecurity readiness, given their increased vulnerability to cyberattacks. The findings revealed significant gaps in the implementation of formal policies, employee training, and IT infrastructure investment. Regression analysis identifies IT infrastructure as the most significant factor influencing readiness, while cross-tabulation demonstrates the variance in policy implementation across organisational sizes. To solve these problems, SMEs must align their strategy with best practices, relying on cost-effective solutions and external support. Future research should look into region-specific interventions and sectoral variances in cybersecurity demands. Overall, enhancing cybersecurity readiness is critical not only for individual SMEs but also for safeguarding supply chains and the broader economic system.

REFERENCES

[1] S. Kabanda and M. Tanner, "**Exploring SME cybersecurity practices in developing countries**," *J. Organ. Comput. Electron. Commer.*, vol. 28, no. 3, pp. 269–282, 2018.

[2] ISO/IEC, ***Information Security, Cybersecurity and Privacy Protection: Information Security Controls***, International Organization for Standardization, 2022.

[3] SBA Office of Advocacy, "**Small Business Profile**," *Sba.gov*, 2021. [Online]. Available: https://advocacy.sba.gov/wp-content/uploads/2021/08/2021-Small-Business-Profiles-For-The-States.pdf. [Accessed: Jan. 3, 2025].

[4] J. Haltiwanger, R. S. Jarmin, and J. Miranda, "**Who Creates Jobs? Small versus Large versus Young**," *Review of Economics and Statistics*, vol. 95, pp. 347–361, 2013.

[5] A. Cameron, "**Think small—small business, that is. What is considered a small business?**," *Patriot Software for Small Business*, Apr. 9, 2021. [Online]. Available: https://smallbusiness.patriotsoftware.com/what-is-considered-small-business-classification-size/. [Accessed: Jan. 3, 2025].

[6] N. Rawindaran, A. Jayal, E. Prakash, and C. Hewage, "**Perspective of small and medium enterprise (SME's) and their relationship with government in overcoming cybersecurity challenges and barriers in Wales**," *Int. J. Inf. Manag. Data Insights*, vol. 3, no. 2, p. 100191, 2023.

[7] T. J. Holt, "**Situating the problem of cybercrime in a multidisciplinary context**," in *Cybercrime through an interdisciplinary lens*, 2016, pp. 15–28.

[8] Verizon Communications Inc., "**Data Breach Investigations Report**," *Verizon Business*, 2022. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir. [Accessed: Jan. 3, 2025].

[9] N. Huaman *et al.*, "**A Large-Scale interview study on information security in and attacks against small and medium-sized enterprises**," in *30th USENIX Security Symposium (USENIX Security 21)*, 2021, pp. 1235–1252.

[10] A. Alahmari and B. Duncan, "**Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence**," in *2020 Int. Conf. Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 2020.

[11] M. Heidt, J. P. Gerlach, and P. Buxmann, "**Investigating the security divide between SME and large companies: How SME characteristics influence organizational IT security investments**," *Inf. Syst. Front.*, vol. 21, no. 6, pp. 1285–1305, 2019.

[12] R. Walczuch, G. Van Braven, and H. Lundgren, "**Internet adoption barriers for small firms in The Netherlands**," *Eur. Manag. J.*, vol. 18, no. 5, pp. 561–572, 2000.

[13] A. Khatibi, V. Thyagarajan, and A. Seetharaman, "**E-commerce in Malaysia: Perceived benefits and barriers**," *Vikalpa*, vol. 28, no. 3, pp. 77–82, 2003.

[14] J. Rezaei, R. Ortt, and P. Trott, "**How SMEs can benefit from supply chain partnerships**," *Int. J. Prod. Res.*, vol. 53, no. 5, pp. 1527–1543, 2015.

[15] J. C. Fernandez de Arroyabe, M. F. Arroyabe, I. Fernandez, and C. F. A. Arranz, "**Cybersecurity resilience in SMEs. A machine learning approach,**" *J. Comput. Inf. Syst.*, pp. 1–17, 2023.

[16] R. F. Babiceanu and R. Seker, "**Cyber resilience protection for industrial internet of things: A software-defined networking approach,**" *Comput. Ind.*, vol. 104, pp. 47–58, 2019.

[17] ENISA, "**ENISA threat landscape 2021**," *Europa.eu*, 2021. [Online]. Available: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202021.pdf. [Accessed: Jan. 3, 2025].

[18] N. Rawindaran *et al.*, "**Enhancing cyber security governance and policy for SMEs in Industry 5.0: A comparative study between Saudi Arabia and the United Kingdom**," *Digital*, vol. 3, no. 3, pp. 200–231, 2023.

[19] S. Hasan, M. Ali, S. Kurnia, and R. Thurasamy, "**Evaluating the cyber security readiness of organizations and its influence on performance**," *J. Inf. Secur. Appl.*, vol. 58, no. 102726, p. 102726, 2021.

[20] M. O. Fasasi, "**Enhancing Infrastructure Resilience with Non-Destructive Evaluation: GPR and IE Integration for Delamination Detection**," *Adv. Eng. Des. Technol.*, vol. 6, no. 1, 2024.

[21] H.-K. Kong, T.-S. Kim, and J. Kim, "**An analysis on effects of information security investments: a BSC perspective**," *J. Intell. Manuf.*, vol. 23, no. 4, pp. 941–953, 2012.

[22] C. Hsu, J.-N. Lee, and D. W. Straub, "**Institutional influences on information systems security innovations**," *Inf. Syst. Res.*, vol. 23, no. 3-part-2, pp. 918–939, 2012.

[23] T. Pereira and H. Santos, "**A security audit framework to manage information system security**," in *Global Security, Safety, and Sustainability*, S. Tenreiro De Magalhães, H. Jahankhani, and H. Ali, Eds. Heidelberg: Springer, 2010, pp. 9–18.

[24] A. Klimburg, *National Cyber Security Framework Manual*, *Ccdcoe.org*, 2012. [Online]. Available: https://ccdcoe.org/uploads/2018/10/NCSFM_0.pdf. [Accessed: Jan. 3, 2025].

[25] M. van Haastrecht *et al.*, "**A threat-based cybersecurity risk assessment approach addressing SME needs**," in *16th Int. Conf. Availability, Reliability and Security*, 2021.

[26] K.-L. Hui, S. H. Kim, Q.-H. Wang, and S. Management University, "**Cybercrime deterrence and international legislation: Evidence from distributed denial of service attacks**," *MIS Q.*, vol. 41, no. 2, pp. 497–523, 2017.

[27] PWC, "**Revitalizing privacy and trust in a data-driven world**," *Pwc.com*, 2018. [Online]. Available: https://www.pwc.com/us/en/cybersecurity/assets/revitalizing-privacy-trust-in-data-driven-world.pdf. [Accessed: Jan. 3, 2025].

[28] M. Uma and G. Padmavathi, "**A Survey on Various Cyber Attacks and Their Classification,**" *Open J. Eng. Sci.*, vol. 15, no. 5, pp. 390–396, 2024.

[29] S. Duchek, "**Organizational resilience: a capability-based conceptualization,**" *Bus. Res.*, vol. 13, no. 1, pp. 215–246, 2020.

[30] J. Ferdinand, "**Building organisational cyber resilience: A strategic knowledge-based view of cyber security management**," *J. Bus. Contin. Emer. Plan.*, vol. 9, no. 2, pp. 185–195, 2015.

[31] A. Annarelli, F. Nonino, and G. Palombi, "**Understanding the management of cyber resilient systems,**" *Comput. Ind. Eng.*, vol. 149, no. 106829, p. 106829, 2020.

[32] I. Linkov, D. A. Eisenberg, K. Plourde, T. P. Seager, J. Allen, and A. Kott, "**Resilience metrics for cyber systems**," *Environ. Syst. Decis.*, vol. 33, no. 4, pp. 471–476, 2013.

[33] Y. Luo, "**A General Framework of Digitization Risks in International Business**," *J. Int. Bus. Stud.*, vol. 53, pp. 344–361, 2022.

[34] N. Kshetri, "**Pattern of Global Cyber War and Crime: A Conceptual Framework,**" *J. Int. Manag.*, vol. 11, pp. 541–562, 2005.

[35] M. Hudakova, M. Gabrysova, Z. Petrakova, K. Buganova, and V. Krajcik, "**The Perception of Market and Economic Risks by Owners and Managers of Enterprises in the V4 Countries**," *J. Competitiveness*, vol. 13, pp. 60–77, 2021.

[36] T. August, D. Dao, and M. F. Niculescu, "**Economics of ransomware: Risk interdependence and large-scale attacks**," *Manage. Sci.*, vol. 68, no. 12, pp. 8979–9002, 2022.

[37] G. Say and G. Vasudeva, "**Learning from Digital Failures? The Effectiveness of Firms**' Divestiture and Management Turnover Re sponses to Data Breaches," *Strategy Sci.*, vol. 5, pp. 117–142, 2020.