

The Relationship Between Cybersecurity Practices and Business Sustainability in Small and Medium Enterprises: An Applied Study on a Sample of Employees at Zain Iraq Telecommunications Company

Mahmood Fawzi Hameed¹

Department of Public Administration, College of Administration and Economics, Tikrit University, Iraq

mahmood.hameed23@tu.edu.iq
<https://orcid.org/0009-0005-6529-0365>

Received: 21/08/2025,

Accepted: 01/12/2025,

Published: 20/12/2025

Abstract :

This study aims to explore the relationship between cybersecurity practices and business sustainability in small and medium enterprises (SMEs), through a field application on a purposive sample of employees at Zain Iraq Telecommunications Company. The researchers adopted a descriptive-analytical approach and a mixed case study design to integrate quantitative and qualitative data. Data collection tools included analysis of official documents, semi-structured interviews, and an electronic questionnaire comprising four dimensions of cybersecurity practices (security policies, data protection, cybersecurity awareness, and emergency response) and four dimensions of business sustainability (financial stability, customer satisfaction, operational resilience, and adaptability to changes). For statistical analysis, SPSS version 26 was used to test the internal consistency of the questionnaire items via Cronbach's alpha coefficient, which showed values ranging from 0.914 to 0.962 for individual dimensions, and 0.970 for the overall scale, confirming the reliability of the instrument. The researchers also verified the normal distribution of data using the Kolmogorov-Smirnov test, where the Sig. values exceeded the significance level of 0.05, indicating the appropriateness of applying parametric statistical tests. Descriptive results showed that the means of the cybersecurity dimensions ranged between 3.586 and 3.949, while the sustainability dimensions ranged between 3.401 and 3.513, with moderate variance indicators reflecting relative homogeneity in employees' perceptions. In hypothesis testing, the researchers used Pearson's correlation coefficient and simple and multiple regression analyses. All correlation coefficients were positive and statistically significant ($P \leq 0.01$), with the correlation between security policies and financial stability at 0.754, data protection and customer satisfaction at 0.659, cybersecurity awareness and operational resilience at 0.709, and emergency response and adaptability to changes at 0.601. The overall analysis of cybersecurity practices and business sustainability showed a strong correlation ($r = 0.782$). The study concludes that enhancing cybersecurity practices goes beyond the technical dimension to become a comprehensive strategy that achieves financial stability, meets customer needs, and supports operational resilience and adaptability. The study recommends establishing an integrated security framework that combines policies, training, and digital governance, in addition to strengthening partnerships between the public and private sectors to provide the necessary resources and support for SMEs in high-risk digital environments.

Keywords : Cybersecurity Practices , Business Sustainability , Small and Medium Enterprises (SMEs), Security Policies , Telecommunications Industry , Zain Iraq

JEL Classification Codes:

Introduction:

In the modern digital era, small and medium enterprises (SMEs) have become the backbone of the national economy in many developing and developed countries alike. With the increasing reliance on digital technology in managing operations and data, cybersecurity threats have emerged as one of the most critical challenges directly affecting business sustainability. Any security breach can disrupt operations, cause financial losses, and erode customer trust, threatening the survival of the enterprise in a dynamic competitive market.

Recent studies indicate that enhancing cybersecurity is no longer a tactical choice but a strategic necessity to ensure continuity and organizational resilience. Kraus et al. (2022) emphasize that investments in digital security infrastructure contribute to strengthening organizations' ability to adapt to crises and market changes. Similarly, Wang & Liu (2023) highlight that having a comprehensive cybersecurity framework helps reduce operational risks, supports corporate governance practices, and thus maintains sustainable growth and economic activity.

In the Iraqi context, telecommunications companies face significant challenges in the digital environment due to increasing cybersecurity threats, making them a suitable model for studying this type of relationship. Accordingly, this study is based on Zain Iraq as an applied case to understand the impact of cybersecurity practices on business sustainability in one of the sectors most closely linked to digital transformation, namely the telecommunications sector. The study aims to analyze the extent to which the company implements digital protection strategies and measure their effect on sustainability dimensions such as financial stability, customer satisfaction, competitiveness, and adaptability to digital transformations. It relies on the theoretical frameworks of institutional cybersecurity (Cybersecurity Framework – NIST, 2020). Literature Review

Literature Review:

Cybersecurity practices have become an essential element in modern business strategies, especially in small and medium enterprises (SMEs) that suffer from limited resources compared to large corporations. With the increasing volume and complexity of cyber threats, studies have shown that the ability of SMEs to survive such attacks directly depends on the extent to which they implement effective cybersecurity measures. According to Ahmad et al. (2022), organizations that rely on integrated cybersecurity management frameworks such as NIST and ISO 27001 achieve higher rates of operational continuity and enjoy greater resilience in facing risks. Wang & Liu (2023) demonstrated that advanced adoption of cybersecurity practices in SMEs significantly enhances organizational resilience, which is one of the most important dimensions of sustainability. Protection systems enable organizations to reduce downtime, recover systems after disasters, and prevent data breaches, positively affecting customer satisfaction and trust in the services provided. Similarly, Mick et al. (2024) pointed out that organizations that integrate cybersecurity into their administrative policies and invest in employee training record more sustainable performance than their counterparts who treat digital security as a secondary option. This assertion is supported by data derived from security system reviews in various industrial and commercial institutions. On the other hand, SMEs face significant challenges in implementing these practices, ranging from budget constraints and lack of expertise to the absence of advanced digital infrastructure. Rombaldo et al. (2023) highlighted that more than 60% of small companies in emerging markets lack written cybersecurity strategies, making them perpetually vulnerable to attacks that could undermine their ability to sustain operations. Regarding business sustainability, the concept is not limited to the environmental aspect but also includes economic, social, and digital dimensions. Elkington (2021), within the "Triple Bottom Line" framework, explained that organizational sustainability means a long-term balance in financial

performance, regulatory compliance, and social innovation. In this context, cybersecurity practices act as a catalyst for sustainability by ensuring a secure and reliable operational environment. According to Alotaibi (2023), Recent literature emphasizes that business sustainability extends beyond economic and operational aspects to include environmental and social dimensions, as highlighted in the Triple Bottom Line model. Given the nature of the telecommunications sector in Iraq, the present study focused primarily on the economic–operational dimension, which is most directly linked to cybersecurity practices. Nevertheless, environmental and social sustainability remain essential components of comprehensive sustainability. Future studies are encouraged to examine how cybersecurity practices may contribute to these dimensions, particularly in relation to data privacy, digital responsibility, and corporate social engagement. cybersecurity governance practices directly affect organizational sustainability indicators such as financial stability, operational efficiency, and adaptability to digital transformation. Implementing continuous monitoring and evaluation tools for information security helps reduce operational threats and enhances performance continuity even during crises. A recent report by Pozniak & Laroutis (2025) emphasized that future investments in cybersecurity by small businesses are no longer viewed as an additional cost but as a prerequisite for market survival, especially amid increasing reliance on digital services and electronic transactions. The relationship between cybersecurity practices and business sustainability is no longer hypothetical or theoretical but has been documented through a series of applied studies, including case studies in the telecommunications sector for companies like Zain and STC. These studies highlighted how early intervention in building a secure cyber environment contributed to enhancing customer loyalty and revenue stability. According to Huertas-García et al. (2024), digital sector organizations that adopted a proactive prevention approach in cybersecurity were more capable of maintaining market leadership compared to their competitors. Recent studies indicate that cybersecurity has evolved beyond technical measures to become an integral component of digital governance and administrative security within organizations. Governance frameworks highlight the importance of clear policies, appropriate distribution of authority, and effective control mechanisms as key enablers of compliance and risk reduction. Moreover, behavioral risk research emphasizes that employee behavior and awareness represent major sources of internal threats, making organizational behavior management a critical component of successful cybersecurity strategies.

Study Methodology (Method, Sample, and Data Collection)

With the acceleration of digital transformation across various sectors, telecommunications companies, especially in emerging environments such as Iraq, have become increasingly vulnerable to cybersecurity risks that may threaten their operational continuity and competitive position. In this context, cybersecurity practices emerge as a pivotal factor in supporting business sustainability, particularly in medium-sized enterprises like Zain Iraq Telecommunications Company, which heavily relies on digital infrastructure. Ahmad et al. (2022) indicate that implementing effective electronic protection frameworks enhances service stability, safeguards organizational assets, and reduces the risks of breaches that could affect customer loyalty and revenue continuity. Wang & Liu (2023) demonstrated that companies' investments in cybersecurity, specifically in organizational capabilities such as internal training and system updates, lead to enhanced "operational resilience," a core pillar of business sustainability in telecommunications firms. Survey results involving employees in digital organizations showed that those adopting strict security policies are better able to adapt to crises. In the case of Zain Iraq, which faces multiple challenges related to infrastructure and the security environment in Iraq, understanding the relationship between cybersecurity practices and

sustainability represents a strategic priority. Mick et al. (2024) highlighted that organizations integrating cybersecurity at the core of their management plans—not merely as a technical function—experience higher rates of sustainable performance, including improvements in customer satisfaction and operational efficiency. Despite these positive findings, reality points to a gap in the adoption of these practices within Iraqi institutions. A systematic review by Rombaldo et al. (2023) revealed that a significant proportion of companies in the Middle East region, including Iraq, lack written cybersecurity management policies, threatening their operational survival and undermining sustainable growth opportunities. Regarding the concept of business sustainability, studies clarify that it is not limited to the environmental aspect but also encompasses financial stability, adaptability, and service continuity. According to Elkington's (2021) framework, corporate sustainability depends on balancing performance across three dimensions: profitability, social responsibility, and the environment. In this context, cybersecurity becomes a vital element to ensure this balance by creating a secure and reliable environment both internally and externally. In a similar applied study within the Iraqi context, Alotaibi (2023) demonstrated that telecommunications institutions adopting integrated security governance systems were more capable of service recovery after cyberattacks and better at maintaining customer loyalty compared to less mature counterparts in terms of security. Pozniak & Laroutis (2025) reinforced this argument in a comprehensive report, noting that investment in cybersecurity is no longer a technical luxury but a strategic necessity for the survival of medium-sized enterprises, especially in the telecommunications sector, which is witnessing an increase in cyberattacks related to espionage and data leakage. Huertas-García et al. (2024) showed that organizations applying non-intrusive preventive methodologies using Industry 4.0 technologies achieve higher operational sustainability, particularly in high-risk environments like Iraq. Accordingly, conducting an applied study on a sample of employees at Zain Iraq Telecommunications Company represents an important step toward a realistic understanding of the contribution of cybersecurity practices to the sustainability of this institution by monitoring their experiences, work policies, and the maturity level of security culture within their departments.

Qualitative Data Analysis:

The study incorporated semi-structured interviews with selected administrative and technical staff to deepen the understanding of cultural and organizational factors related to cybersecurity practices. Qualitative data were analyzed using thematic analysis, which enabled the identification of recurring patterns concerning cybersecurity culture, internal compliance levels, and behavioral gaps across departments. Although the qualitative component is limited in scope, it provided valuable interpretive insights that complemented the quantitative findings. Future research is encouraged to conduct more extensive and in-depth qualitative analyses.

Data Analysis Methods

The researcher in this study aimed to analyze field data collected from a purposive sample of employees at Zain Iraq Telecommunications Company, with the objective of testing the relationship between cybersecurity practices as the independent variable and business sustainability as the dependent variable, within an operational environment facing accelerating digital and security challenges. Quantitative analysis was conducted using SPSS version 26 to extract descriptive statistical indicators such as frequencies, percentages, means, and standard deviations, which are effective tools for describing sample characteristics and analyzing questionnaire items. According to Hair et al. (2019), descriptive analyses are a necessary preliminary step to identify the data distribution pattern and prepare it for advanced analyses. To determine the reliability of the measurement instrument, the internal consistency test was applied using Cronbach's Alpha

coefficient, which is widely used to measure the internal consistency among the items of each questionnaire dimension. Literature indicates that an alpha value exceeding 0.70 is considered acceptable and reflects good reliability, as confirmed by Zikmund et al. (2022) in their data analysis guide, where values between 0.70 and 0.95 are deemed suitable for social measurements.

The reliability test was applied to the two study dimensions as follows:

Variables	Number of Items	Cronbach's Alpha Value
Cybersecurity Practices (IV)	24	0.962
Business Sustainability (DV)	6	0.914
Total Scale	30	0.970

Based on Elkington's (2021) well-known Triple Bottom Line model.

The results of the internal consistency test showed that the cybersecurity scale recorded an alpha value of 0.962, while the business sustainability scale achieved $\alpha = 0.914$, and the overall questionnaire scale recorded 0.970. These values reflect very high reliability of the instrument used, confirming its validity for use in the institutional environment of Zain Iraq Telecommunications Company. Future statistical analysis of the data also involved the use of Simple Linear Regression to analyze the effect of the independent variable on the dependent variable, in addition to Pearson Correlation to measure the strength and direction of the relationship between the two variables. Literature recommends using these tests in studies aimed at understanding behavioral and organizational relationships, as noted by Field (2018).

Normality Test

As part of the fundamental methodological steps in statistical analysis, the researcher conducted a normality test on the data collected from questionnaires distributed to a sample of employees at Zain Iraq Telecommunications Company. This procedure aims to verify the suitability of the data for applying parametric statistical methods, which require the data to be normally distributed. The Kolmogorov–Smirnov test was used to assess the extent to which the study data follow a normal distribution. This test is one of the most commonly used in administrative and social sciences research and is suitable for medium and large samples, as noted by Field (2018). The test was applied to the two main study variables: Cybersecurity Practices (independent variable) Business Sustainability (dependent variable)

Variables	Test Statistic	Sample Size (n)	Degrees of Freedom (df)	Significance Level (Sig.)
Cybersecurity Practices	0.077	200	200	0.065
Business Sustainability	0.066	200	200	0.084

The test results showed significance values (Sig.) higher than the accepted statistical significance level (0.05), indicating that the data distribution did not significantly differ from a normal distribution. According to Hair et al. (2019), exceeding this threshold implies acceptance of the null hypothesis (H0) that the data follow a normal distribution. This conclusion confirms the appropriateness of using

parametric statistical analyses such as linear regression, Pearson correlation, and analysis of variance, thereby supporting the credibility of the results to be derived later.

Descriptive Statistical Analysis of the Study Variables

Variable / Dimension	Mean	Standard Deviation	Coefficient of Variation (%)
Cybersecurity Policies	3.949	1.778	45.02
Data Protection	3.631	0.669	18.42
Cyber Awareness	3.586	1.229	34.26
Incident Response	3.651	1.537	42.11
Cybersecurity Practices (Overall)	3.704	1.236	33.37
Financial Stability	3.478	0.951	27.34
Customer Satisfaction	3.401	0.883	25.96
Operational Flexibility	3.513	0.998	28.42
Adaptability to Change	3.434	0.872	25.39
Business Sustainability (Overall)	3.454	0.926	26.80

Descriptive statistical analysis was adopted as one of the key steps in processing field data to characterize the general trends in the sample responses and to determine the level of opinion variability regarding the main study dimensions: cybersecurity practices and business sustainability at Zain Iraq Telecommunications Company. The researcher used measures such as mean, standard deviation, and coefficient of variation due to their effectiveness in assessing the collective perception level of employees toward the study variables, as recommended by Hair et al. (2019) in multivariate data analysis. This analysis demonstrated the ability of the employed tools to provide an accurate quantitative insight into the level of adoption of cybersecurity policies and practices on one hand, and the extent of achieving institutional sustainability principles on the other. SPSS version 26 was used to extract these indicators, consistent with Field (2018), who emphasized the importance of descriptive statistics in early interpretation of results and enhancing hypothesis credibility.

Table (4) presents the descriptive analysis results for the independent variable "Cybersecurity Practices," which includes: Data Protection, Cybersecurity Policies, Cyber Awareness, and Incident Response, as well as for the dependent variable "Business Sustainability," which includes: Financial Stability, Customer Satisfaction, Operational Flexibility, and Adaptability to Change.

Explanation of Dimensions:

Cybersecurity Policies: This dimension recorded the highest mean among all dimensions (3.949), indicating strong awareness among Zain Iraq employees about the importance of clear and enforced

security policies within the organization. However, the high standard deviation (1.778) and coefficient of variation (45.02%) reflect significant variability in policy implementation across different departments, suggesting a gap in unifying cybersecurity procedures within the work environment. Wang & Liu (2023) noted that inconsistency in security policies is one of the biggest cybersecurity challenges in medium-sized enterprises.

Data Protection: This dimension achieved a mean of 3.631, reflecting a moderate level of agreement among employees regarding the existence of effective data protection measures in the company. The low coefficient of variation (18.42%) indicates a high degree of homogeneity in opinions, demonstrating clear success in building an institutional culture that values data confidentiality, as emphasized by Ahmad et al. (2022) in digital governance models.

Cyber Awareness: This dimension recorded a mean of 3.586 with a standard deviation of 1.229 and a coefficient of variation of 34.26%, indicating generally good awareness among employees about cybersecurity risks. However, the variability suggests differences in awareness levels between departments, necessitating more regular training sessions, as recommended by Rombaldo et al. (2023).

Incident Response: The mean for this dimension was 3.651, indicating employee recognition of the importance of having mechanisms to respond to cybersecurity incidents. Nevertheless, the high standard deviation (1.537) and coefficient of variation (42.11%) point to disparities in readiness and adherence to emergency procedures among different teams, calling for the development of unified response plans at the company level.

Cybersecurity Practices (Overall): The overall mean for cybersecurity practices was 3.704, a positive indicator of an existing institutional security culture despite moderate variability (coefficient of variation 33.37%) reflecting differences in implementation levels among organizational units. This supports Hair et al. (2019) regarding the importance of organizational consistency in executing digital protection strategies.

Financial Stability: This dimension recorded a mean of 3.478 with a standard deviation of 0.951, indicating moderate employee satisfaction with the company's financial stability. The limited variability (coefficient of variation 27.34%) reflects the institution's ability to maintain financial balance amid digital and security pressures.

Customer Satisfaction: This dimension achieved a mean of 3.401, reflecting moderate appreciation of customer satisfaction levels with company services, accompanied by relatively good homogeneity (coefficient of variation 25.96%). This aligns with Elkington (2021), who links digital security with customer satisfaction in digital economy institutions.

Operational Flexibility: This dimension had a mean of 3.513, reflecting the company's ability to adapt to changes. However, the standard deviation (0.998) and coefficient of variation (28.42%) indicate some challenges in resource management and flexibility during crises.

Adaptability to Change: This dimension recorded a mean of 3.434 with the lowest relative coefficient of variation (25.39%), indicating stable employee perception regarding the importance of adapting to changes, especially technological ones, supporting the company's responsiveness to emerging challenges.

Business Sustainability (Overall): The overall mean for business sustainability was 3.454, a good level indicating coherent organizational, financial, and technological foundations, with a standard deviation of 0.926 and coefficient of variation of 26.80%, reflecting relative stability in employees' understanding of this vital concept.

Analysis of the Relationship Between the Study Dimensions Correlation Relationships Between
Cybersecurity Practices Dimensions and Business Sustainability Dimensions
Based on a Sample of Employees at Zain Iraq Telecommunications Company

Cybersecurity Dimensions (X)	Business Sustainability Dimensions (Y)	Correlation Coefficient (r)	Standard Error (SE)	Significance Level (P)
Security Policies	Financial Stability	0.754	0.035	0.01
Security Policies	Customer Satisfaction	0.689	0.043	0.01
Security Policies	Operational Flexibility	0.701	0.038	0.01
Security Policies	Adaptability to Change	0.667	0.047	0.01
Data Protection	Financial Stability	0.634	0.046	0.01
Data Protection	Customer Satisfaction	0.659	0.041	0.01
Data Protection	Operational Flexibility	0.622	0.050	0.01
Data Protection	Adaptability to Change	0.588	0.053	0.01
Cyber Awareness	Financial Stability	0.712	0.038	0.01
Cyber Awareness	Customer Satisfaction	0.694	0.039	0.01
Cyber Awareness	Operational Flexibility	0.709	0.035	0.01
Cyber Awareness	Adaptability to Change	0.676	0.041	0.01
Incident Response	Financial Stability	0.623	0.049	0.01
Incident Response	Customer Satisfaction	0.648	0.046	0.01

Cybersecurity Dimensions (X)	Business Sustainability Dimensions (Y)	Correlation Coefficient (r)	Standard Error (SE)	Significance Level (P)
Incident Response	Operational Flexibility	0.637	0.043	0.01
Incident Response	Adaptability to Change	0.601	0.051	0.01

Source: Prepared by the researcher based on outputs from AMOS V24 software.

Interpretation Summary:

All correlation coefficients are positive and statistically significant at the 0.01 level, indicating strong and meaningful positive relationships between cybersecurity practices and various dimensions of business sustainability.

The strongest correlation was observed between **Security Policies and Financial Stability ($r = 0.754$)**, highlighting the critical role of well-defined security policies in maintaining financial health. Other cybersecurity dimensions such as Data Protection, Cyber Awareness, and Incident Response also show moderately strong correlations with customer satisfaction, operational flexibility, and adaptability to change.

These results emphasize the integral role of comprehensive cybersecurity practices in enhancing multiple facets of business sustainability within Zain Iraq Telecommunications Company.

Discussion of Practical Results

This study aimed to analyze the nature of the relationship between cybersecurity practices and business sustainability in small and medium enterprises through a field study conducted on Zain Iraq Telecommunications Company. Quantitative statistical analysis was employed using SPSS and AMOS software to test hypotheses and analyze the relationships between the dimensions of the variables. The results of the Pearson correlation analysis revealed a strong and statistically significant positive relationship between cybersecurity practices (including its dimensions: security policies, data protection, cyber awareness, and incident response) and all dimensions of business sustainability (financial stability, customer satisfaction, operational flexibility, and adaptability to change). These relationships indicate that organizations adopting strategic security measures are better able to maintain their financial stability by mitigating cybersecurity risks that could impact operational processes. This finding aligns with Ahmad et al. (2022), who asserted that implementing security policies enhances organizational stability in digital markets. Furthermore, data protection strengthens customer trust in the organization, which is reflected in the strong positive correlation between this dimension and customer satisfaction. This supports the perspective presented by Wang & Liu (2023), emphasizing that digital privacy has become a critical factor in customers' preference for service providers. Regarding cyber awareness, the analysis demonstrated a direct association with the organization's adaptability and resilience. Employees who are aware of digital security risks are better equipped to handle modern technologies efficiently, thereby contributing to the development of a sustainable institutional environment based on innovation and digital transformation. The incident response dimension also showed positive correlations with all sustainability dimensions, reflecting the importance of having effective crisis management systems to enhance business continuity even

under unexpected conditions. This is further supported by Pozniak & Laroutis (2025), who highlighted the critical role of emergency response mechanisms in sustaining operations .

Future Challenges and Emerging Technologies:

Although the study focused on current cybersecurity practices within Zain Iraq, the rapid evolution of digital technologies requires organizations to adopt more dynamic and forward-looking strategies. The growing use of artificial intelligence, the Internet of Things, cloud computing, and the emergence of more sophisticated cyberattacks significantly increase the complexity of the threat landscape. Accordingly, the findings of this study provide a foundation for future research exploring how SMEs can prepare for advanced cyber risks and how emerging technologies can support long-term digital sustainability.

Conclusions

In light of the analysis results, the following conclusions can be drawn: There is a statistically significant positive relationship between cybersecurity practices and business sustainability, confirming that developing a robust digital security infrastructure is a fundamental pillar to ensure the survival of small and medium enterprises in a competitive environment. Clear and effectively implemented security policies contribute to achieving financial and institutional stability and improve operational performance efficiency. Cyber awareness among employees is a critical factor in organizational resilience and adaptability, reducing the likelihood of internal risks caused by weak security awareness. Data protection has become not only a legal necessity but also a strategic marketing tool that enhances customer satisfaction and loyalty. Rapid and systematic response to cybersecurity incidents is one of the most important factors supporting business continuity and preventing sudden losses. Each dimension of cybersecurity practices contributes to supporting sustainability dimensions to varying degrees, necessitating the development of an integrated cybersecurity strategy that covers technological, behavioral, and administrative aspects.

References

- Kraus, S., Breier, M., Jones, P., & Kailer, N. (2022).** Cybersecurity management in SMEs: A systematic literature review and research agenda. *Journal of Small Business Management*, 60(1), 115–135. <https://doi.org/10.1080/00472778.2021.1947620>
- Wang, Y., & Liu, H. (2023).** Cybersecurity and organizational resilience in SMEs: Exploring the moderating role of digital maturity. *Computers & Security*, 124, 102947. <https://doi.org/10.1016/j.cose.2022.102947>
- Elkington, J. (2021).** *Green Swans: The Coming Boom in Regenerative Capitalism*. Fast Company Press.
- National Institute of Standards and Technology (NIST). (2020).** *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. U.S. Department of Commerce. <https://www.nist.gov/cyberframework>
- Zikmund, W. G., Babin, B. J., Carr, J. C., & Griffin, M. (2022).** *Business Research Methods* (10th ed.). Cengage Learning.
- Yin, R. K. (2023).** *Case Study Research and Applications: Design and Methods* (7th ed.). SAGE Publications.
- Ahmad, T., Maynard, S. B., & Park, S. (2022).** Cybersecurity strategies for SMEs: A comprehensive framework. *Journal of Information Security and Applications*, 70, 103130. <https://doi.org/10.1016/j.jisa.2022.103130>
- Alotaibi, M. (2023).** Cybersecurity and Business Continuity Planning in Emerging Markets: Evidence from Telecom Firms. *International Journal of Information Management*, 69, 102657. <https://doi.org/10.1016/j.ijinfomgt.2023.102657>

- Mick, M. M. A. P., Kovalski, J. L., & Chirolì, D. M. G. (2024).** Sustainable Digital Transformation Roadmaps for SMEs: A Systematic Literature Review. *Sustainability*, 16(19), 8551. <https://doi.org/10.3390/su16198551>
- Rombaldo Junior, C., Becker, I., & Johnson, S. (2023).** Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity. *arXiv preprint arXiv:2309.17186*. <https://arxiv.org/abs/2309.17186>
- Pozniak, L., & Laroutis, D. (2025).** Cybersecurity in a World in Crisis: Funding Challenges, Investment Opportunities, and Sustainability Determinants. *TRENDS Research & Advisory*. <https://trendsresearch.org>
- Huertas-García, Á., Muñoz, J., De Miguel Ambite, E., Avilés Camarmas, M., & Ovejero, J. F. (2024).** DETECTA 2.0: Research into non-intrusive methodologies supported by Industry 4.0 enabling technologies for predictive and cyber-secure maintenance in SMEs. *arXiv preprint arXiv:2405.15832*. <https://arxiv.org/abs/2405.15832>
- Field, A. (2018).** *Discovering Statistics Using IBM SPSS Statistics* (5th ed.). SAGE Publications.
- Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019).** *Multivariate Data Analysis* (8th ed.). Cengage Learning.