International Journal of
Science, Architecture, Technology and Environment

Cybersecurity in Small and Medium-Sized Enterprises: A Literature Review with a Focus on Slovakia and the European Union

Leoš Šafár[1], Jakub Sopko[2], Michal Mešťan[3*]

[1]*Faculty of Economics, Technical University in Košice, Němcovej 32, 040 01 Košice-Sever, Slovakia*
ORCID: 0000-0001-8466-0644

[1]*Faculty of Economics, Technical University in Košice, Němcovej 32, 040 01 Košice-Sever, Slovakia*
ORCID: 0000-0002-7314-828X

[2]*Faculty of Economics, Matej Bel University in Banska Bystrica, Tajovského 10, 975 90 Banská Bystrica, Slovakia*
ORCID: 0000-0002-4974-2254

[*]*Corresponding author – michal.mestan@umb.sk*

DOI: https://doi.org/10.63680/ijsate0226063.049

Abstract

Small and medium-sized enterprises (SMEs) play a central role in the European and Slovak economies, yet they remain disproportionately exposed to cyber threats amid rapid digitalisation and increasing integration into cross-border value chains. This article presents a structured literature review of cybersecurity in SMEs with a specific focus on Slovakia and a comparative perspective across European Union Member States. The review synthesises peer-reviewed research, EU policy documents, and international threat intelligence reports to examine four interrelated dimensions: i) cybersecurity awareness and organisational preparedness of SMEs, ii) incident reporting practices and the economic impacts of cyber incidents, iii) dominant attack vectors and risk mitigation practices, and iv) governance mechanisms, including NIS2-related supply-chain pressures. The findings identify a persistent awareness–implementation gap, systematic underreporting of cyber incidents (particularly in Central and Eastern Europe), and substantial cross-country heterogeneity in SME cyber resilience. SMEs in digitally advanced EU economies exhibit higher adoption of baseline security controls and faster recovery from incidents than SMEs in less digitally mature ecosystems. The review further highlights emerging intersections between cybersecurity, artificial intelligence, and financial misconduct risks, suggesting that cyber resilience in SMEs should be viewed as part of broader economic governance. The paper concludes with policy implications for targeted capacity-building, improved access to financial support, harmonised reporting mechanisms, and directions for future research.

Keywords: cybersecurity; small and medium-sized enterprises (SMEs); literature review; cyber resilience

1. Introduction

SMEs constitute the backbone of the European and Slovak economies, accounting for most firms and a substantial share of employment and value creation. The rapid digitalisation of business processes—driven by cloud computing, remote work, e-commerce, platformisation, and the increasing integration of SMEs into cross-border value chains—has fundamentally reshaped the risk environment in which SMEs operate. While digital technologies offer significant productivity gains and market opportunities, they simultaneously expose SMEs to an expanding and increasingly sophisticated cyber threat landscape.

The existing literature consistently highlights SMEs as one of the most vulnerable segments of the digital economy in terms of cybersecurity preparedness. Compared to large enterprises, SMEs exhibit lower levels of cybersecurity awareness, weaker internal security governance, and significantly lower adoption rates of both technical and organisational safeguards (ENISA, 2023; European Commission, 2024). These vulnerabilities are not uniform across the European Union. Cross-country evidence suggests substantial heterogeneity in cybersecurity maturity among SMEs, with Nordic and Benelux countries exhibiting higher levels of digital security capabilities, while SMEs in several Central and Eastern European (CEE) and Southern European Member States, including Slovakia, continue to lag behind (European Commission, 2024).

Against this background, the literature increasingly frames cybersecurity not merely as a technical IT issue, but as a core component of enterprise risk management, organisational resilience, and long-term competitiveness. The introduction of the NIS2 Directive further reinforces this shift by extending cybersecurity governance requirements across digital supply chains, indirectly affecting a broad segment of SMEs even when they are not directly regulated entities. However, the empirical and policy-oriented literature on SME cybersecurity remains fragmented, combining academic studies, industry reports, and grey literature, with limited systematic synthesis at the country and EU-comparative levels.

The objective of this paper is therefore to provide a structured literature review of the current state of cybersecurity in SMEs in Slovakia within a broader EU comparative perspective. By synthesising academic research, EU policy documents, and international threat intelligence reports, the paper aims to i) map key patterns in cybersecurity awareness, incident reporting, and economic impacts of cyber incidents among SMEs, ii) identify dominant risk mitigation practices and attack vectors reported in the literature and iii) highlight cross-country differences and policy-relevant gaps in cybersecurity preparedness across EU Member States. In doing so, the paper contributes to the growing body of research on SME digital resilience and provides an evidence-based foundation for future empirical studies and policy interventions in the Slovak and EU contexts.

2. Cybersecurity Awareness, Incident Reporting and Economic Impact of Cyber Incidents in SMEs: A Review of the Current Literature and EU Comparison

The academic and policy-oriented literature consistently identifies SMEs as one of the most vulnerable segments of the digital economy in terms of cybersecurity preparedness. Comparative EU-level evidence shows that SMEs systematically lag behind large enterprises in both cybersecurity awareness and the adoption of basic security controls (ENISA, 2023; European Commission, 2024). According to the Digital Decade Country Reports, countries such as Finland, the Netherlands and Estonia exhibit significantly higher levels of digital security maturity among SMEs compared to CEE economies, including Slovakia, Hungary and Romania, where cybersecurity capabilities remain uneven and fragmented (European Commission, 2024). A large-scale systematic review of SME cybersecurity research confirms that low awareness, limited funding,

and skills shortages are the most persistent structural barriers to cybersecurity adoption across sectors and regions (Rombaldo Junior et al., 2023).

A recurrent theme in the literature is the "awareness–implementation gap" in SMEs. While survey-based studies report that a majority of EU SMEs perceive cybersecurity as a growing concern, actual implementation of technical and organisational safeguards remains limited (Eurobarometer, 2024; ENISA, 2023). In Slovakia, empirical findings indicate that SMEs often lack dedicated cybersecurity personnel and formal security governance structures, a pattern that mirrors evidence from other CEE countries. In contrast, SMEs in Northern and Western Europe report higher levels of internal cybersecurity expertise and greater uptake of structured risk management frameworks, reflecting differences in digital skills ecosystems and institutional support mechanisms (European Commission, 2024).

Empirical research consistently shows that SME cybersecurity behaviour is shaped less by technical constraints alone and more by managerial perceptions of risk, organisational culture, and bounded rationality. Bada and Nurse (2020) demonstrate that SME decision-makers tend to systematically underestimate cyber risks due to optimism bias and limited prior exposure to severe incidents, leading to delayed investments in preventive measures. Renaud and Weir (2016) find that even when SMEs are aware of cybersecurity threats, the absence of formal governance structures and security leadership roles results in fragmented and reactive security practices. Comparative studies across EU Member States suggest that SMEs operating in ecosystems with stronger institutional support for digital skills and cybersecurity awareness campaigns exhibit higher baseline levels of cyber preparedness, while SMEs in less supportive environments display more pronounced gaps between awareness and implementation. These findings reinforce the importance of managerial cognition, organisational routines, and institutional context as key determinants of SME cybersecurity maturity beyond purely technical considerations.

The literature further highlights persistent weaknesses in cyber incident reporting among SMEs. Comparative evidence suggests that underreporting is widespread across the EU but is particularly pronounced in countries with less developed national reporting infrastructures and lower trust in public institutions (ENISA, 2023). For example, regular national surveys in the United Kingdom provide detailed longitudinal data on SME cyber incidents, whereas in several EU Member States, including Slovakia, systematic national-level monitoring remains absent. This data asymmetry limits cross-country comparability and constrains evidence-based policy design.

From an economic perspective, international studies document that cyber incidents impose disproportionate costs on SMEs relative to their size and financial capacity. The IBM Cost of a Data Breach Report (2023) and Verizon DBIR (2023; 2025) consistently show that SMEs face high direct costs of recovery, ransomware payments, and business interruption, alongside substantial indirect losses related to reputational damage and customer churn. Comparative evidence suggests that SMEs in digitally advanced EU economies tend to recover faster from cyber incidents due to higher levels of preparedness, the availability of cyber insurance, and stronger incident response capabilities. In contrast, SMEs in less digitally mature ecosystems face longer recovery times and higher relative losses, increasing the risk of market exit following major cyber incidents. Recent peer-reviewed research further conceptualises cybersecurity in SMEs as an economic and managerial issue rather than merely a technical concern, highlighting market failures and information asymmetries that lead to systematic underinvestment in cybersecurity measures among SMEs (Arroyabe et al., 2024).

3. Cybersecurity Awareness, Incident Reporting and Economic Impact of Cyber Incidents in SMEs: A Review of the Current Literature and EU Comparison

The literature identifies a consistent pattern of limited adoption of advanced cybersecurity controls among SMEs across the EU. While basic measures such as antivirus software and ad hoc backups are widespread, more sophisticated controls—multi-factor authentication (MFA), systematic patch management, encryption, network segmentation, and formalised incident response planning—remain underutilised, particularly in SMEs operating in traditional sectors and peripheral regions (ENISA, 2023; Center for Internet Security, 2023). Cross-country comparisons indicate that SMEs in Nordic and Benelux countries demonstrate significantly higher uptake of MFA and structured security policies compared to SMEs in Southern and Eastern Europe, where financial constraints and skills shortages remain binding constraints (European Commission, 2024). A socio-technical perspective emphasises that the limited adoption of advanced cybersecurity controls in SMEs reflects not only financial constraints but also organisational culture, leadership, and measurement challenges, which hinder the systematic evaluation of cybersecurity maturity (van Haastrecht et al., 2021).

Empirical studies and threat intelligence reports converge on a common set of attack vectors affecting SMEs across the EU. Phishing campaigns, weak or reused credentials, unpatched software vulnerabilities, exposed remote access services, and misconfigured cloud environments are repeatedly identified as dominant entry points for attackers (ENISA, 2023; Verizon, 2025). Comparative analyses reveal that the relative importance of specific attack vectors varies by country, reflecting differences in digitalisation patterns and technology adoption. For instance, SMEs in highly digitalised economies face higher exposure to cloud-related misconfigurations and SaaS account compromises, whereas SMEs in less digitalised regions are more frequently affected by basic phishing and credential theft.

Literature increasingly emphasises the systemic role of supply-chain vulnerabilities in SME cyber risk exposure. ENISA (2023) and Verizon (2025) document a growing share of incidents originating from compromised third-party providers, a trend that is particularly relevant in the EU context due to the dense integration of SMEs into cross-border value chains. Comparative studies suggest that SMEs embedded in highly regulated supply chains (e.g. manufacturing and healthcare) exhibit higher compliance with minimum cybersecurity standards, driven by contractual requirements imposed by large enterprises. This indirect regulatory channel contributes to a gradual convergence of cybersecurity practices across EU Member States, although significant cross-country heterogeneity persists. Qualitative evidence from SME case studies further shows that time constraints, competing business priorities, and limited internal expertise lead SMEs to prioritise short-term operational goals over proactive cybersecurity investments (Gibb and Bednar, 2024).

From a policy-oriented literature perspective, the effectiveness of public support instruments and standardisation initiatives varies significantly across the EU. Countries with well-established national cybersecurity strategies, decentralised advisory networks for SMEs, and streamlined funding mechanisms report higher uptake of cybersecurity tools and training programmes (European Commission, 2024; ENISA, 2023). In contrast, in countries where support schemes are fragmented or administratively burdensome, SMEs exhibit lower participation rates. The literature therefore points to the importance of institutional design and governance capacity in shaping the real-world impact of cybersecurity policies on SMEs.

The literature increasingly conceptualises the impact of the NIS2 Directive on SMEs as an indirect, supply-chain–mediated governance mechanism rather than as a direct regulatory obligation. Although many SMEs do not fall formally within the scope of NIS2, they are embedded in value chains with regulated large

enterprises and public-sector organisations that are required to comply with stricter cybersecurity governance standards. This regulatory asymmetry generates downstream pressure on SMEs through contractual requirements, supplier audits, security questionnaires, and mandatory compliance with minimum cybersecurity standards imposed by dominant value-chain actors. The resulting supply-chain pressure acts as a behavioural driver that incentivises SMEs to adopt cybersecurity measures primarily for transactional and reputational reasons (e.g. maintaining supplier status, avoiding exclusion from contracts), rather than as a result of intrinsic risk awareness. The literature suggests that this mechanism contributes to a gradual diffusion of cybersecurity practices among SMEs, particularly in sectors with high regulatory intensity and cross-border value-chain integration. However, the effectiveness of this indirect regulatory channel is highly heterogeneous across EU Member States and firm sizes, reflecting differences in institutional enforcement capacity, digital maturity of lead firms, and SMEs' access to financial and advisory support. Consequently, NIS2-related supply-chain pressure can function as a catalyst for improving SME cyber resilience, but only when complemented by targeted capacity-building policies and accessible support instruments that enable SMEs to translate externally imposed requirements into sustainable internal cybersecurity practices (ENISA, 2023; European Commission, 2024).

Moreover, the indirect regulatory pressure exerted through the NIS2 Directive and supply-chain governance mechanisms highlights the need for integrated policy frameworks that simultaneously strengthen cybersecurity resilience and address emerging risks such as AI-enabled financial fraud and market conduct issues, creating an opportunity for cross-sectional research at the intersection of cybersecurity, compliance, and digital economic governance.

Recent literature increasingly points to the dual role of artificial intelligence in the context of SME cybersecurity and broader economic risks, including tax evasion and financial fraud. On the one hand, AI-based tools enhance cyber defence capabilities by enabling automated threat detection, anomaly identification in network traffic, and early warning systems against phishing and ransomware attacks. On the other hand, the same technologies lower entry barriers for sophisticated cybercrime and financial fraud by enabling the automation and personalisation of social engineering attacks, the generation of deepfake identities, and the large-scale exploitation of compromised digital infrastructures. In the SME context, weak cybersecurity practices and fragmented digital governance can facilitate not only cyber incidents but also financial irregularities, including VAT fraud, false invoicing, and cross-border tax evasion schemes conducted through compromised or manipulated accounting and e-commerce systems. The growing integration of AI-driven accounting, invoicing, and compliance tools into SME operations further increases systemic interdependencies between cybersecurity and tax compliance. Consequently, the literature suggests that strengthening cyber resilience in SMEs should be viewed not only as a matter of information security, but also as a component of broader economic governance and tax compliance frameworks, where improved cybersecurity can indirectly reduce the risks of AI-enabled financial fraud and tax evasion (e.g. OECD, 2023; ENISA, 2023).

4. Conclusion

This literature review demonstrates that cybersecurity risks represent a structural and growing challenge for SMEs across the European Union, with particularly pronounced vulnerabilities in less digitally mature ecosystems, including Slovakia. The reviewed literature converges on several core findings. First, SMEs systematically lag behind large enterprises in cybersecurity awareness, governance structures, and the adoption of technical and organisational safeguards. Second, cyber incident reporting remains fragmented and incomplete, especially in countries without established national monitoring frameworks, leading to

significant underestimation of the true scale and economic impact of cyber incidents affecting SMEs. Third, the economic consequences of cyber-attacks are disproportionately severe for SMEs due to limited financial buffers, weak recovery capacities, and high dependence on continuous business operations.

The EU-level comparative perspective highlights persistent cross-country heterogeneity in SME cybersecurity maturity. SMEs in Nordic and Benelux countries benefit from stronger digital skills ecosystems, more developed institutional support mechanisms, and higher uptake of cybersecurity standards and practices. In contrast, SMEs in parts of Central and Eastern and Southern Europe face binding constraints related to skills shortages, limited financial resources, and lower institutional trust, which collectively hinder the effective implementation of cybersecurity measures. These structural differences underscore the importance of contextualised policy design rather than one-size-fits-all regulatory approaches.

The literature further indicates that technological solutions alone are insufficient to address SME cybersecurity vulnerabilities. Effective cyber resilience requires the integration of cybersecurity into broader enterprise risk management, business continuity planning, and organisational culture. Supply-chain dependencies and third-party risks emerge as increasingly important drivers of SME cyber exposure, reinforcing the relevance of indirect regulatory channels, such as contractual cybersecurity requirements imposed by larger enterprises under NIS2-related compliance regimes.

From a policy and research perspective, the findings point to several priorities. Policymakers should focus on reducing adoption barriers for basic cybersecurity controls through targeted financial incentives, simplified access to support schemes, and decentralised advisory services for SMEs. At the same time, greater emphasis should be placed on building managerial and employee-level cybersecurity competencies, as human factors remain a dominant vulnerability across Member States. The absence of harmonised and systematic incident reporting mechanisms for SMEs represents a critical knowledge gap that limits evidence-based policymaking and cross-country benchmarking within the EU.

Future research should move beyond predominantly descriptive assessments of SME cybersecurity and explore causal relationships between specific cybersecurity interventions and firm-level outcomes such as operational resilience, productivity, financial performance, and survival rates following cyber incidents. Comparative longitudinal studies across EU Member States would be particularly valuable in assessing whether recent regulatory and policy initiatives, including NIS2-related measures, national digital strategies, and public support schemes for SMEs, translate into measurable improvements in cyber resilience over time. In addition to outcome-oriented analyses, future research should examine the behavioural and organisational mechanisms underlying cybersecurity decision-making in SMEs, including managerial risk perception, organisational culture, learning from cyber incidents, and the role of external advisors and supply-chain partners in shaping security practices.

Further work should also focus on the development of harmonised firm-level datasets and reporting frameworks that would enable systematic cross-country benchmarking of SME cybersecurity maturity and the evaluation of policy effectiveness. Mixed-method research designs combining large-scale surveys, administrative data, and in-depth case studies could provide richer insights into the constraints and enabling factors affecting cybersecurity adoption in SMEs. By situating the Slovak experience within a broader EU comparative framework, future studies can contribute to more targeted empirical analyses and support the design of context-sensitive cybersecurity policies aimed at strengthening the digital resilience and long-term competitiveness of SMEs.

Declaration of Conflicting Interests

The authors declare no potential conflicts of interest with respect to the research, authorship and publication of this article.

Funding

This work was supported by the Slovak Research and Development Agency under the contract no. VV-MVP-24-0272 and by Slovak Scientific Grant Agency (VEGA) under the contract No.1/0714/26.

References

[1] B. Bada, J. R. C. Nurse, The social and psychological impact of cyber-attacks on organizations. Edited by V. Benson and J. Mcalaney: Emerging cyber threats and Cognitive Vulnerabilities ISBN 978-0-12-816203-3 (2020). 73-92. URL: https://doi.org/10.1016/B978-0-12-816203-3.00004-6

[2] Center for Internet Security, CIS Controls v8, Center for Internet Security (2023).

[3] ENISA, ENISA Threat Landscape 2023, European Union Agency for Cybersecurity (2023). URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

[4] ENISA, Threat Landscape for AI and Emerging Technologies, European Union Agency for Cybersecurity (2023).

[5] Eurobarometer, Cybersecurity in EU Enterprises, European Commission (2024). URL: https://europa.eu/eurobarometer

[6] European Commission, Digital Decade Country Report 2024 – Slovakia, European Commission (2024). URL: https://digital-strategy.ec.europa.eu/en/library/digital-decade-2024-country-reports

[7] European Commission, Digital Economy and Society Index (DESI) 2024 – Country Report Slovakia, European Commission (2024). URL: https://digital-strategy.ec.europa.eu/en/policies/desi

[8] European Commission, NIS2 Directive (Directive (EU) 2022/2555), Official Journal of the European Union (2022).

[9] IBM Security, Cost of a Data Breach Report 2023, IBM Security (2023).

[10] K. V. Renaud, G. R. S. Weir, Cybersecurity and the Unbearability of Uncertainty. Cybersecurity and Cyberforensics Conference (CCC) (2016): 137-143.

[11] OECD, Building a Skilled Cyber Security Workforce in Europe, OECD iLibrary (2023).

[12] Verizon, Data Breach Investigations Report 2023, Verizon (2023).

[13] Verizon, Data Breach Investigations Report 2025, Verizon (2025).

[14] M. F. Arroyabe, C. F. A. Arranz, I. F. De Arroyabe, J. C. F. de Arroyabe, Exploring the economic role of cybersecurity in SMEs: A case study of the UK, In Technology in Society, Volume 78 September 2024 102670 (2024). URL: https://www.sciencedirect.com/science/article/pii/S0160791X24002185

[15] M. van Haastrecht, B. Y. Ozkan, M. Brinkhuis, M. Spruit, Respite for SMEs: A Systematic Review of Socio-Technical Cybersecurity Metrics, Applied Sciences 11(15) (2021) 6909. URL: https://www.mdpi.com/2076-3417/11/15/6909

[16] A. Gibb, P. Bednar, Cybersecurity Best Practices in SMEs: A Socio-Technical Perspective, OISI Workshop 2024 (2024) 1. URL: https://aisel.aisnet.org/oisiworkshop2024/1

[17] C. Rombaldo Junior, I. Becker, S. Johnson, Unaware, Unfunded, and Uneducated: A Systematic Review of SME Cybersecurity, Journal of CyberSecurity, 2025, 1–31 arXiv (2023). URL: https://arxiv.org/abs/2309.17186