Journal of Engineering Science *Vol. XXXII, no. 2 (2025), pp. 75 - 86*
Fascicle *Electronics and Computer Science* *ISSN 2587-3474*
Topic *Computers and Information Technology* *eISSN 2587-3482*

https://doi.org/10.52326/jes.utm.2025.32(2).07
UDC 004.056.5:334.72(478)

SECURING MOLDOVAN SMALL AND MEDIUM-SIZED BUSINESSES: STRATEGIES BASED ON IT INFRASTRUCTURE DOMAINS

Anatol Alexei *, ORCID: 0000-0002-0570-4854,
Victor Moraru, ORCID: 0000-0002-5454-8341,
Arina Alexei, ORCID: 0000-0003-4138-957X

Technical University of Moldova, 168, Stefan cel Mare Blvd., Chisinau, Republic of Moldova
* Corresponding author: Anatol Alexei, *anatolie.alexei@adm.utm.md*

Received: 03. 28. 2025
Accepted: 05. 04. 2025

Abstract. The digitization of small and medium-sized enterprises (SMEs) has accelerated in recent years, increasing their reliance on information systems to support core business operations. ENISA's 2021 report showed an important growth in SME dependence on IT, while the World Economic Forum ranked cybersecurity failure among the top five global risks. Although digital transformation brings competitive advantages, it also exposes SMEs to cyber threats. A comparative analysis of scientific studies from the UK, Australia, the EU, Malaysia, and the USA identified social engineering, Denial of Service (DoS) / Distributed Denial of Service (DDoS), and Man-in-the-Middle (MitM) attacks as the most frequent threats. This article analyzes the main barriers preventing SMEs from implementing information security frameworks and identifies the lack of national-level regulations in the Republic of Moldova. Based on a structured model developed by the authors, the paper proposes tailored recommendations for improving information system security in Moldovan micro-enterprises. The findings emphasize the need for contextualized, cybersecurity solutions and public policy support targeting risk management and awareness.

Keywords: *cybersecurity, information system; framework, risk, SME.*

Rezumat. Digitalizarea întreprinderilor mici și mijlocii (IMM-uri) s-a accelerat în ultimii ani, crescând dependența acestora de sistemele informaționale pentru susținerea operațiunilor esențiale. Raportul ENISA din 2021 a evidențiat o creștere semnificativă a dependenței IMM-urilor de tehnologiile IT, iar Forumul Economic Mondial a clasat eșecul în materie de securitate cibernetică printre primele cinci riscuri globale. Deși transformarea digitală aduce avantaje competitive, ea expune IMM-urile la amenințări cibernetice. O analiză comparativă a studiilor științifice din Regatul Unit, Australia, Uniunea Europeană, Malaysia și Statele Unite a identificat ingineria socială, atacurile DoS/DDoS și atacurile de tip MitM drept cele mai frecvente amenințări. Acest articol analizează principalele bariere care împiedică IMM-urile să implementeze cadre de securitate informațională și evidențiază lipsa unor reglementări naționale în Republica Moldova. Pe baza unui model structurat elaborat de autori, lucrarea propune recomandări specifice pentru îmbunătățirea securității sistemelor informaționale în

micro-întreprinderile din Moldova. Concluziile subliniază necesitatea unor soluții de securitate cibernetică adaptate contextual, precum și sprijinul politicilor publice orientate spre gestionarea riscurilor și creșterea nivelului de conștientizare.

Cuvinte-cheie: *securitate cibernetică, sistem informațional, cadru, risc, IMM.*

1. Introduction

Small and medium-sized enterprises (SMEs) play a very important role in the global economy, accounting for 90% of businesses worldwide [1]. In Australia, for example, SMEs represent 98% of all Australian enterprises, generate one-third of the total Gross Domestic Product (GDP), and employ 4.7 million people, while in the United Kingdom, SMEs account for approximately 99.9% of all businesses [1]. In the Republic of Moldova, it was reported in 2020 that 98.6% of the enterprises active in the national economy are SMEs [2].

The digitization of SMEs is no longer regarded as an option, but rather as a key driver of sustainable development in the context of a global digital economy. Digital transformation can enhance the competitiveness, efficiency, and adaptability of SMEs to emerging challenges, offering benefits such as:

- improved operational efficiency and reduced costs through the automation of various processes, minimization of human errors, and time savings;
- expanded access to new markets and customers, regardless of the company's geographical location, through digital marketing and e-commerce;
- the ability to make informed decisions based on the analysis of large volumes of data using a variety of Business Intelligence tools;
- increased innovation and market competitiveness through the implementation of new business models and personalized services based on customer behavior analysis.

The digitization of small and medium-sized enterprises (SMEs) has been progressing in recent years. SMEs carry out various business processes that rely on information systems [3], such as: e-commerce; the exchange of information between employees, business partners, and customers [4]; as well as informing and promoting companies through websites and social media platforms. Information systems are defined as the complete set of software, hardware, data, people, and procedures that enable the use of a company's informational resources [5]. The 2021 report of the European Union Agency for Cybersecurity (ENISA) indicated a growing dependence of small and medium-sized business operations on information technology systems [6].

What is certain is that technological progress adds competitiveness and can contribute to the increase of annual business revenues, but it also leads to heightened cyber risks associated with information systems security. In the 2019 report published by the World Economic Forum, cyber risks were ranked among the top 10 global risks [7], while in the 2021 report, cybersecurity failure was assessed as the 4th major global risk [4]. The analysis of scientific studies revealed that SMEs are frequently targeted by cyberattacks. For instance, 39% of SMEs in the United Kingdom reported having been targeted by cyberattacks in the past 12 months [8], while in Australia, statistics indicated that 66% of SMEs had fallen victim to cyberattacks [1]. In developing countries such as Malaysia, the percentage of SMEs affected by cyberattacks is even higher, reaching 85% [4]. In the Republic of Moldova, such statistics are lacking due to the immaturity of the field, making it very difficult to assess the real state of affairs [9].

The main challenges SMEs face in ensuring the security of information systems stem from insufficient allocated budgets, lack of awareness regarding information security issues, lack of support from top management who are unaware of the consequences of cyberattacks, the absence of processes and tools to improve security practices [8], and, of course, the employees' cybersecurity culture, with the human factor representing the greatest vulnerability in the information system [10].

According to a survey conducted by ENISA in 2021 [11], which involved 16 SMEs from 14 European Union countries, European SMEs face the following issues: low staff awareness of information security, inadequate protection of critical and sensitive data, budget limitations, a shortage of Information and Communication Technologies (ICT) cybersecurity specialists, lack of appropriate cybersecurity guidelines tailored to SMEs, poor IT management, ICT-related work shifting beyond SME control, and low support from company management [7].

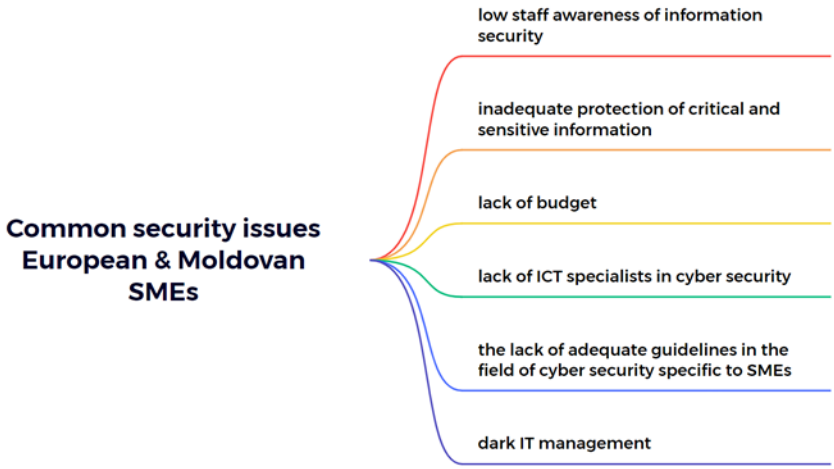

Figure 1. Common security issues in European and Moldovan SMEs – synthesized from ENISA 2021 survey data and national context.

The scope is to analyze the current state of cybersecurity readiness among SMEs, identify common vulnerabilities, and propose tailored security measures that are both effective and feasible within the specific constraints of small and medium-sized businesses. The central hypothesis explored in this study is that the implementation of a structured, cost-effective cybersecurity framework adapted to the SME context can reduce exposure to cyber threats, even in environments with limited institutional maturity in the field. To support this analysis, a review of key academic and institutional publications was conducted, including reports from ENISA, the World Economic Forum, Ponemon Institute, Check Point Research, Verizon and various country-specific studies focused on cybersecurity in the SME sector.

2. Materials and Methods

This research was conducted based on a systematic review of specialized literature, with a focus on both international and national studies concerning information security in small and medium-sized enterprises (SMEs). Primary sources included ENISA reports [12-14], studies by Verizon [15,16], Ponemon Institute [17], Check Point Research [18], as well as peer-reviewed scientific articles and governmental reports relevant to the context of the Republic of Moldova.

The methodology consisted of the following steps:

- Thematic bibliographic analysis, which allowed the identification of key threats, vulnerabilities, and reported security practices in SMEs at both international and national levels. Reference management and citation consistency were ensured using Mendeley Reference Manager.
- Identification and systematization of IT infrastructure domains in SMEs, structured into seven core components: users, workstations, LAN (local area network), LAN-to-WAN, WAN (wide area network), remote access, and system/application domains. This structure was based on the security framework proposed by Kim & Solomon [19], which provides a logical mapping of organizational IT assets for targeted risk analysis and protection strategies.
- Logical risk modelling, by correlating identified threats and vulnerabilities with the seven IT infrastructure domains, a domain-specific exposure. The conceptual design of this correlation process was supported using Xmind (version 25.01.01061) for visual mapping and clarity.

Adaptation and refinement of ENISA's recommendations to the national SME context by formulating a set of feasible policies, processes, and technological measures tailored to Moldovan SMEs. These included low-cost yet effective security practices and awareness-building initiatives focused on the human factor, considered the most vulnerability.

The methods applied were predominantly qualitative and descriptive, given the objective of synthesizing existing knowledge and tailoring it to a specific socio-economic and technological environment.

3. Results

The structured analysis of the scientific literature and the synthesis of relevant data for SMEs in the Republic of Moldova have led to the following results, which are described in detail below.

3.1. Aspects of Information Systems in SMEs

From a technical perspective, the implementation of information systems (IS) in SMEs can be structured into seven key domains of IT infrastructure [19]. These domains are summarized in Figure 2 and briefly described below.

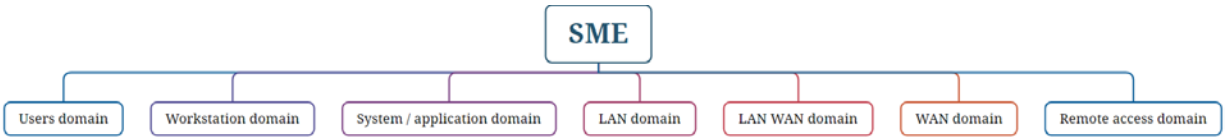

Figure 2. Key domains of the information systems infrastructure in SMEs.

(1) *User Domain* – covers SME personnel who access and operate the organizational IS.
(2) *Workstation Domain* – includes all connected devices (PCs, laptops, tablets, smartphones). It distinguishes between thin clients (limited local resources, rely on network) and thick clients (fully equipped for local processing).
(3) *LAN Domain* – comprises local networks built with Network Interface Cards (Media Access Control - based), Ethernet standards (Institute of Electrical and Electronics Engineers Standard 802.3), Unshielded Twisted Pair cabling (Cat 5/6), switches (Layer 2 and 3), file/print servers, and wireless access points. Logical elements include user authentication, shared directories, IP configurations, and VLANs.

(4) *LAN-WAN Domain* – connects LANs to the Internet via TCP/UDP protocols. Common logical ports include HTTP (80), FTP (20), TFTP (69), Telnet (23), and SSH (22).
(5) *WAN Domain* – enables interconnection between distant sites and Internet access.
(6) *Remote Access Domain* – ensures connectivity for remote users through mobile access, Virtual Private Network (VPN), Wi-Fi, and secure Internet links, used more post-COVID.
(7) *System/Application Domain* – includes mission-critical systems such as Transaction Processing Systems (TPS), Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), and Management Information Systems (MIS) platforms.

This structural view serves as the basis for mapping security vulnerabilities and associated threats across each domain.

3.2. Security Threats Facing SMEs

Analyzing and publishing data on security threats affecting SMEs is important, particularly for raising awareness among top management regarding the importance of securing the information systems they oversee. SMEs are attractive targets for cyber attackers due to the relatively weak security measures they implement—unlike large organizations, which invest in good protection systems to safeguard sensitive business data, including personal, financial, and commercial information [20].

Academic and industry reports identify the most common threats to SMEs as social engineering attacks, credential and data theft, misuse of organizational assets, malicious software - especially ransomware - web application attacks, and e-commerce supply chain breaches [1,17,21,22]. These threats can be grouped into six major categories, as illustrated in Figure 3.

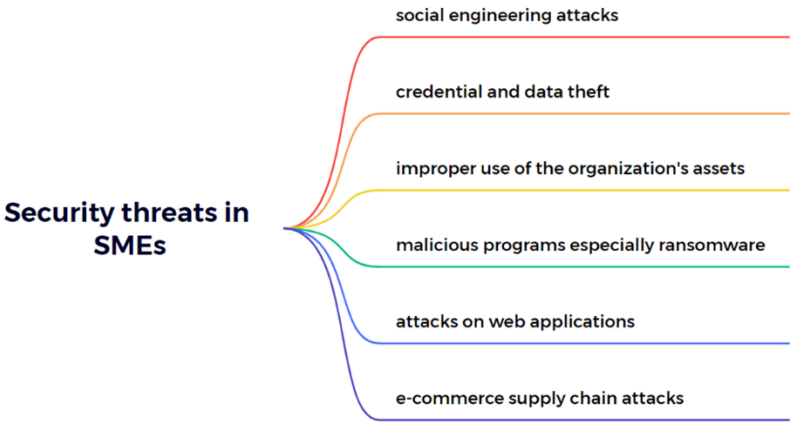

Figure 3. Major categories of security threats in SMEs.

These threats can be analyzed by examining vulnerabilities across five key components: software, hardware, communication networks, data, and users. Among these, the human factor remains the most exploitable - 84% of cyberattacks leverage social engineering to manipulate individuals [7].

Software-related threats include ransomware, which can lock down organizational systems until a ransom is paid. ENISA's 2021 report [13] describes an incident where attackers exploited the Remote Desktop Protocol (RDP) to gain unauthorized access to corporate servers. Other malware types - viruses, trojans, worms, rootkits, and downloaders—pose serious risks. Web applications are also frequently targeted through vulnerabilities such as cross-site scripting (XSS), buffer overflows, XML injection, and SQL injection [3].

Network security is a critical aspect of information system protection. Both wired and wireless networks are vulnerable to attacks such as Denial of Service/Distributed Denial of Service (DoS/DDoS) [11,22,23], man-in-the-middle (MitM) attacks [23,24], and identity spoofing [25], where attackers impersonate legitimate devices to infiltrate networks. Wireless networks, although widely adopted for their convenience, are inherently less secure than wired ones and susceptible to authentication weaknesses and rogue access points [26].

Social engineering attacks, particularly phishing and spear phishing, are increasing in frequency. ENISA reports that 41% of attacks on SMEs fall into this category [11], often targeting top executives. These attacks succeed not by exploiting technical flaws but by manipulating human behavior. The lack of awareness and training in this area is an emerging challenge for effective cybersecurity in SMEs.

Based on this classification, the specific threats and vulnerabilities identified for each IT domain are summarized in Table 1.

Table 1

Security threats and risks in SME IT domains [19]

IT Domain	Security Threats and Risks
User Domain	Unauthorized access; lack of awareness; security policy violations; use of removable media; unauthorized web downloads; system or application damage; sabotage; unauthorized actions
Workstation Domain	Unauthorized access to workstations, systems, applications, or data; OS vulnerabilities; software vulnerabilities; missing updates; malware infections; use of personal devices; use of removable media; unauthorized content downloads
LAN Domain	Unauthorized LAN access; unauthorized access to systems, applications, or data; server OS vulnerabilities; vulnerable server applications; unauthorized WLAN access; compromised wireless transmission; difficult network administration
LAN-WAN Domain	Unauthorized network and port scanning; unauthorized access; DoS/DDoS attacks; router/firewall firmware vulnerabilities; misconfigurations; remote access threats; unverified content downloads; access to malicious URLs; access to unrelated/non-business content
WAN Domain	Open access; unencrypted traffic; malware infections; data corruption; use of insecure protocols
Remote Access Domain	Brute-force and password attacks; multiple unauthorized access attempts; remote data compromise; data loss; theft of remote employees' devices; theft of employee credentials
System/Application Domain	Unauthorized access to data repositories; server unavailability due to maintenance; server OS vulnerabilities; insecure virtual environments; unauthorized access; vulnerable applications; data loss or corruption; loss of backup copies; IT system unavailability

The security risks faced by SMEs are substantial. A previous study showed that approximately 60% of SMEs that suffer a cyberattack go out of business within six months [27]. Several factors contribute to the limited implementation of cybersecurity frameworks, models, or standards in SMEs [1]:

- Underestimation of cyber risk and the complexity of modern threats.
- Lack of expertise and domain knowledge [17,28,29] leading to poor understanding by management regarding the importance of information security.
- Limited financial resources, as managers tend to prioritize product or service development over security investments.
- The steady stream of new digital tools (e.g. Internet of Things, Artificial Intelligence), which further complicate understanding and implementation.
- Excessive and ambiguous information in the field, increasing uncertainty for decision-makers.
- Lack of perseverance due to the indirect or delayed visibility of returns from security investments.

These limiting factors are summarized in Figure 4, which reflects the most common barriers preventing SMEs from adopting cybersecurity frameworks.

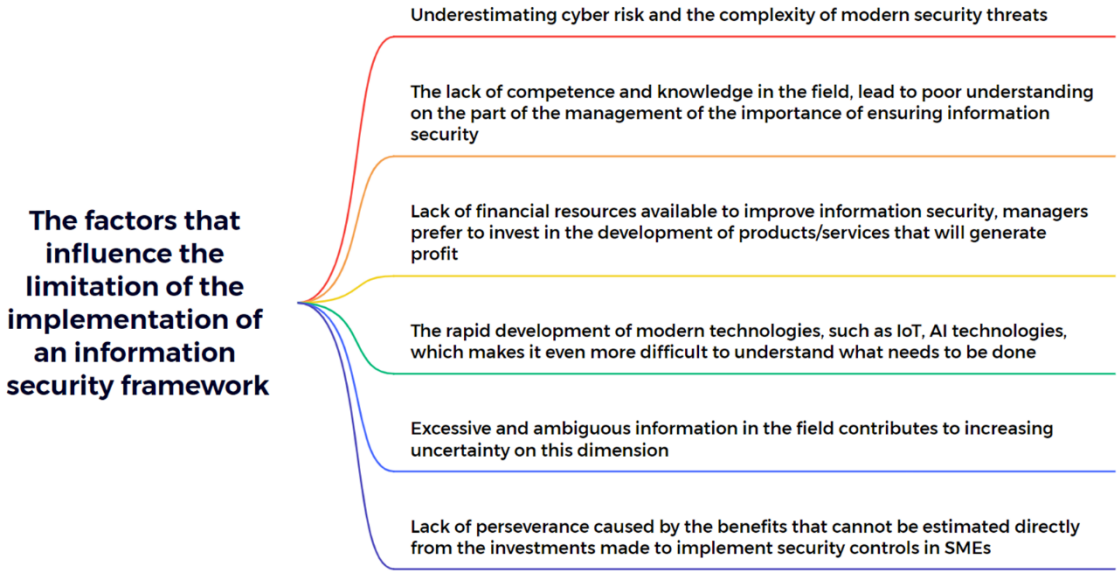

Figure 4. Key factors limiting the implementation of information security frameworks in SMEs.

One of the most critical risks for SMEs is business failure [1], in addition to loss of competitiveness, financial damages, or legal issues resulting from compromised customer data. Moreover, the cost of recovery after a major incident can be extremely high, including equipment upgrades, implementation of security controls, and staff training. An additional concern is the recurrence of attacks - studies show that 28% of SMEs affected by cyberattacks are targeted again within two years. The range and severity of consequences that SMEs face following a cyber incident are illustrated in Figure 5.

Research has shown that most studies on information security in SMEs have focused on developed countries such as the United Kingdom, the United States, Australia, and European Union (EU) member states. However, information security is also highly important for developing countries, such as the Republic of Moldova.

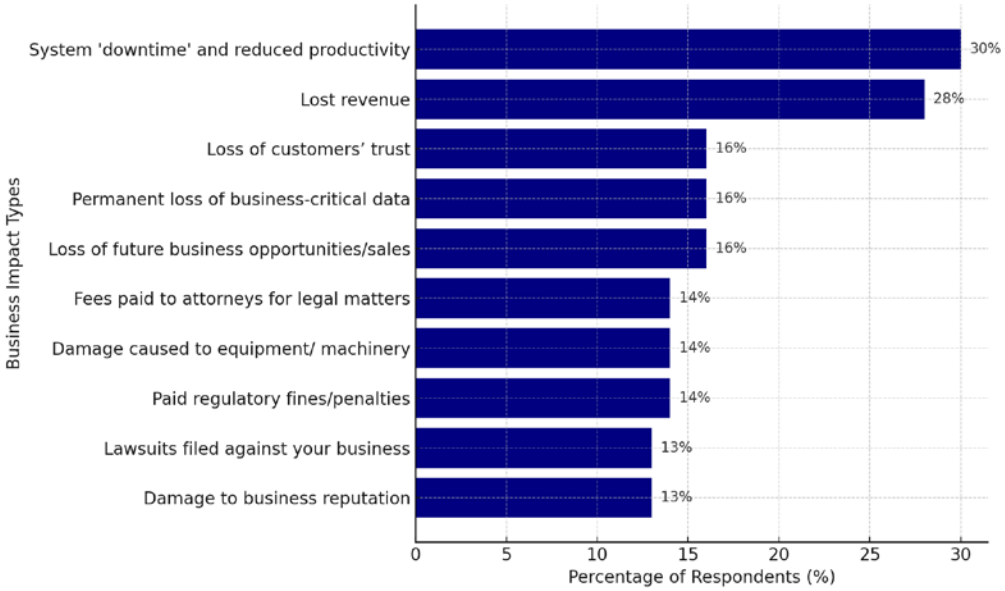

Figure 5. Main consequences of cyberattacks on SMEs.

The analysis of scientific studies revealed that SMEs are frequently targeted by cyberattacks. In the United Kingdom, 39% of SMEs reported being attacked within the last 12 months [8], while in Australia, statistical data showed that 66% had fallen victim to cyberattacks [1]. In developing countries such as Malaysia, the proportion is even higher, reaching 85% [4].

In the Republic of Moldova, such statistics are unavailable due to the immaturity of the field, making it very difficult to assess the actual state of cybersecurity among SMEs [9].

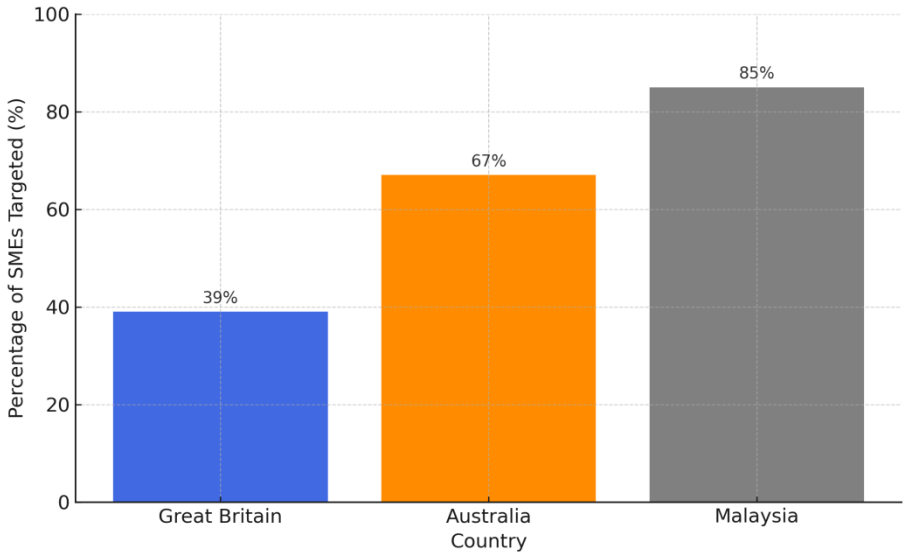

Figure 6. Percentage of SMEs targeted by cyberattacks in selected countries – United Kingdom, Australia, and Malaysia [1, 4, 8].

These results demonstrate not only the widespread nature of cyber threats across SMEs but also the pressing need for structured, context-aware cybersecurity policies - especially in underregulated environments like the Republic of Moldova.

4. Discussion

The results of this study confirm that SMEs are exposed to a wide range of cybersecurity threats across all layers of their IT infrastructure, from end-users to remote access and core applications. These vulnerabilities are not isolated or accidental but systemic, reflecting both structural weaknesses and a lack of organizational preparedness.

Compared to large enterprises, SMEs face disproportionate risks due to limited financial and human resources, minimal formalization of security processes, and low awareness at the management level. These findings are consistent with prior studies conducted in the UK [8], Australia [1], and Malaysia [4], which emphasize the lack of cybersecurity culture as a critical barrier.

In the case of Moldovan SMEs, the situation is more severe due to the immaturity of national cybersecurity frameworks, a low adoption rate of digital technologies, and the absence of structured support mechanisms. Although international bodies such as ENISA provide valuable recommendations, this study shows that global guidelines must be contextualized to meet local needs.

According to 2020 statistics, EU countries and the UK have mostly implemented security measures such as network access control, regular backups, software updates, and strong password policies. However, they show a low level of implementation of risk management practices, security testing, and secure remote access [7,8]. In a study referring to security practices among SMEs in the United States [30], several issues were identified regarding information system security: although SMEs use antivirus software, updates - considered a key element - are performed by only a portion of respondents. Firewall programs used both at endpoint devices [31,32] and at network nodes are deployed by only one-third of the respondents and are updated even less frequently. Problems with password usage and management were also observed.

As for employee education, organizations in the UK implement awareness activities to a limited extent [8], which may be due to a lack of commitment from top management in this area. As shown in a study conducted in France [33], managers are typically occupied with entrepreneurial tasks and dedicate little time to data protection concerns.

The ENISA report outlines the EU's recommendations for implementation within SMEs, as well as priority areas in this domain (Figure 7).

Figure 7. EU recommandations for SMEs [3].

As demonstrated in Table 1 and Figures 5 - 6, the impact of cyberattacks is huge and recurring, while the mitigation efforts remain fragmented.

A notable limitation of this research is the lack of empirical data from Moldovan SMEs, caused by low transparency and reluctance to report incidents. This constrained the analysis to secondary sources and comparative literature. Future research should focus on empirical

validation through surveys, interviews, or incident analysis to assess the actual implementation of cybersecurity measures.

Nevertheless, the findings show the urgent need for tailored, low-cost, and effective cybersecurity solutions that can be adopted even by microenterprises. Public-private partnerships, state-backed education programs, and regulatory incentives are needed for improving cyber resilience across the SME sector.

These recommendations build upon a prior study by the authors [3], where a framework aligned with ENISA principles was adapted to the specific needs and constraints of SMEs in the Republic of Moldova. The proposed framework structures security measures into three categories: People, Processes, and Technology. It shows the need for security policies, staff training, and managerial involvement (People); incident response planning, password and patch management (Processes); and antivirus, encryption, access control, and secure backups (Technology).

Building on this foundation, the underlying research problem addressed by the authors is the identification of security policies and practices that are both effective and realistically implementable in the SME environment, particularly within the Republic of Moldova. The study was guided by three core objectives:

(1) to analyze the current challenges, security behaviors, and managerial attitudes within national SMEs;
(2) to design a sustainable information system model aligned with SME capabilities; and
(3) to develop a support platform with implementation guidelines, risk management tools, and clearly defined mappings of vulnerabilities, threats, and controls.

These components form the basis for a cybersecurity reference model tailored to the needs of local SMEs.

5. Conclusions

This study emphasizes the need to strengthen information system security in small and medium-sized enterprises, especially in countries such as the Republic of Moldova. The analysis showed that SMEs are exposed to a wide variety of cybersecurity threats affecting multiple layers of IT infrastructure, from users and devices to networks and business applications.

Despite their economic importance, SMEs in developing countries often give priority to immediate business needs, while information security remains a secondary concern. This approach increases exposure to cyber threats, especially in the context of digitalized and technology-driven operations. Security should not be seen as optional, but as a necessary component of business continuity.

The results indicate that SMEs are limited by reduced financial and human resources, insufficient awareness at the managerial level, and the absence of a coordinated approach to risk. While international recommendations, such as those from ENISA, provide useful guidance, they need to be adapted to local conditions to be effective in practice.

Further research is needed to collect empirical data from SMEs in the Republic of Moldova. A national-level survey would help assess the current state of information security, including:

- security measures applied in practice;
- types of threats encountered;
- employee and manager awareness levels;

- and how risks are perceived and managed.

The long-term objective is to design a support platform tailored to the local SME environment, offering practical tools and guidance for improving resilience against cyber incidents.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Chidukwani, A.; Zander, Z.; Koutsakis, P. A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations. *IEEE Access* 2022, 10, pp. 85701–85719. DOI: 10.1109/ACCESS.2022.3197899.
2. NBSRM. The activity of small and medium enterprises in the Republic of Moldova in 2020. Available online: https: // statistica. gov.md /ro/activitatea-intreprinderilor-mici-si-mijlocii-in-republica-moldova-in-anul-9557_ 50055.html (accessed on 05.04.2025).
3. Alexei, An.; Alexei, Ar. The problem of information systems security in SME. In: *Central and Eastern European eDem and eGov Days 2023*, ACM, NY, USA, 2023, pp. 101–105.
4. Wallang, M.; Shariffuddin, M. D. K.; Mokhtar, M. Cyber security in small and medium enterprises (SMEs). *Journal of Governance and Development* 2022, 18(1), pp. 75–87.
5. Whitman, M. E.; Mattord, H. J. Principles of Information Securit, 7th ed. Cengage Learning, Boston, SUA, 2021, 658 p.
6. ENISA. Threat Landscape 2021. Available online: https://www.enisa. europa. eu/publications/ enisa-threat-landscape-2021 (accessed on 05.05.2025).
7. Falch, M.; Olesen, H.; Skouby, K. E.; Tadayoni, R.; Williams, I. Cybersecurity Strategies for SMEs in the Nordic Baltic Region. *Journal of Cyber Security and Mobility* 2023, 11(6), 727–754. https://doi.org/10.13052/jcsm2245-1439.1161.
8. Erdogan, G.; Halvorsrud, R.; Boletsis, R.; Tverdal, S.; Pickering, J. Cybersecurity Awareness and Capacities of SMEs. In: *Proceedings of the 9th International Conference on Information Systems Security and Privacy, SCITEPRESS - Science and Technology Publications* 2023, pp. 296–304.
9. Bolun, I.; Ciorbă, D.; Zgureanu, A.; Bulai, R. Informatics security assessment in the Republic of Moldova. *Journal of Engineering Science* 2020, 27(4), pp. 103–119.
10. Boletsis, C.; Halvorsrud, R.; Pickering, J.; Phillips, S.; Surridge, M. Cybersecurity for SMEs: Introducing the Human Element into Socio-technical Cybersecurity Risk Assessment. In: *Proceedings of the 16th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications, SCITEPRESS - Science and Technology Publications* 2021, pp. 266–274
11. Sarri, A.; Paggio, V.; Bafoutsou, G. *Cybersecurity for SMEs – Challenges and Recommendations*. Heraklion, European Union Agency for Cybersecurity, Greece, 2021, 61 p.
12. ENISA threat landscape for ransomware attacks 2022. Available online: https://www.enisa. europa.eu/ publications/enisa-threat-landscape-for-ransomware-attacks/@@download/fullReport (accessed on 06.05.2025).
13. ENISA. Cybersecurity for SMES Challenges And Recommendations, 2021. Available online: https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes (accessed on 08.05.2025).
14. ENISA. Cybersecurity Maturity Assessment for Small and Medium Enterprises. Available online: https://www.enisa.europa.eu/cybersecurity-maturity-assessment-for-small-and-medium-enterprises#/ (accessed on 08.05.2025).
15. Verizon. Data Breach Investigations Report, 2024. Available online: https://www.verizon.com/business/resources/reports/dbir/2024/industries-intro/healthcare-data-breaches/ (accessed on 09.05.2025).
16. Verizon. Data Breach Investigations Report, 2023. Available online: https://www.verizon.com/business/resources/reports/dbir/2023/small-business-data-breaches/?mkt_tok= MTU3LUlQVy04NDYAAAGP51ZU5rx9mZgDjn1I6bznDT1j-OutdGDM2wlWO_wNe3RNqr87MTdVGu_Pn LvBiUFzCodL2mCHf9cRYDk7zNfejzmKlZe_bcHGhu9bR339nWz0NKSG /(accessed on 09.05.2025).
17. Cost of a Data Breach Report 2021. Available online: https://www.ibm. com /downloads/cas/3R8N1DZJ (accessed on 06.05.2025).
18. Check Point Research. Cyber Security Report, 2022. Available online: https://www.checkpoint.com (accessed on 06.05.2025).

19. Kim, D.; Solomon, M. Fundamentals of Information Systems Security (4th ed.). Jones & Bartlett Learning, Burlington, MA, USA, 2023, 550 p.
20. Alexei, A; Platon, N.; Bolun, I.; Alexei, A. Smart and Digital Healthcare. Advanced Technologies and Security Issues. In: *Proceedings of the Central and Eastern European eDem and eGov Days 2024,* New York, USA, 2024, pp. 288–294.
21. Keller, S.; Powell, A.; Horstmann, B.; Predmore, C.; Crawford, M. Information Security Threats and Practices in Small Businesses. *Information Systems Management* 2005, 22(2), pp. 7–19.
22. Alexei, A. Network security threats to higher education institutions. *CEE e|Dem and e|Gov Days* 2021, pp. 323–333. DOI: 10.24989/ocg.v341.24.
23. Alexei, A.; Alexei A. Cyber Security Threat Analysis in Higher Education Institutions as a Result of Distance Learning. *International Journal of Scientific & Technology Research* 2021, 10(3), pp. 128–133.
24. Javeed, D.; Mohammedbadamasi, U.; Ndubuisi, C. O.; Soomro, F.; Asif, M. Man in the Middle Attacks: Analysis, Motivation and Prevention. *International Journal of Computer Networks and Communications Security* 2020, 8(7), pp. 52–58.
25. Ramesh, P.; Bhaskari, D.L. A Comprehensive Analysis of Spoofing. *International Journal of Advanced Computer Science and Applications* 2010, 1(6), pp. 157–162. DOI: 10.14569/IJACSA.2010.010623.
26. Wu, D.; Hu, G. Research and improve on secure routing protocols in wireless sensor networks. In: *International Conference "Circuits and Systems for Communications 2008, IEEE",* 2008, pp. 853–856.
27. Galvin, J. 60 Percent of Small Businesses Fold Within 6 Months of a Cyber Attack Here's How to Protect Yourself. Available online: https://www.Inc.com/joe-galvin/60-percent-of-smallbusinesses- fold-within-6-months-of-a-cyber-attack-heres-how-to-protectyourself. html (accessed on 17.05.2025).
28. What's New in the 2019 Cost of a Data Breach Report. Security Intelligence. Available online: https://securityintelligence.com/posts/whats-new-in-the-2019-costof-a-data-breach-report/ (accessed on 20.05.2025).
29. Cost of a Data Breach Report 2020. Available online: https://www.ibm. com /downloads/cas/3R8N1DZJ (accessed on 16.05.2025).
30. Berry, C. T.; Berry, R. L. An initial assessment of small business risk management approaches for cyber security threats. *International Journal of Business Continuity and Risk Management* 2018, 8(1), pp. 1-10.
31. Alexei, A. Laboratory Guidelines for the Course "Information Security Technologies". Tehnica-UTM, Chisinau, Republic of Moldova, 2024, 94 p.
32. Alexei, A. Course Support "Fundamentals of Cybersecurity". Tehnica-UTM, Chisinau, Republic of Moldova, 2024, 120 p. ISBN 978-9975-64-464-8.
33. Barlette, Y.; Gundolf, K.; Jaouen, A. CEOs' information security behavior in SMEs: Does ownership matter? *Systèmes d'information & management* 2017, 22(3), pp. 7–45.

Citation: Alexei, A.; Moraru, V.; Alexei, A. Securing Moldovan small and medium-sized businesses: strategies based on it infrastructure domains. *Journal of Engineering Science*. 2025, XXXII (2), pp. 75-86. https://doi.org/10.52326/jes.utm.2025.32(2).07.

Submission of manuscripts: jes@meridian.utm.md