IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/46ISM/2025/4646725/
Vol. 2025 (29), Article ID 4646725

Cybersecurity Threats and IT Infrastructure in SMEs: An Analysis and Practical Implications*

Mateusz KRAUZE and Mariusz ZAL

Poznan University of Technology, Chair of Communication and Computer Networks, Poznań, Poland,

Correspondence should be addressed to: Mariusz ZAL, mariusz.zal@put.poznan.pl

* Presented at the 46th IBIMA International Conference, 26-27 November 2025, Ronda, Spain

Abstract

Small and medium-sized enterprises (SMEs) are increasingly exposed to sophisticated cybercriminal campaigns while lacking the financial and human resources available to large corporations. At the same time, market pressure forces SMEs to digitalize their operations, making core business processes directly dependent on IT infrastructure that is often neither highly available, nor redundant, nor easily scalable. This paper analyses the specific context of the SME sector by first clarifying the formal EU classification of micro, small, and medium-sized enterprises, and then examining their typical level of digital maturity, organizational structures, and IT budgeting practices. Based on recent national and international reports, the study characterizes the prevailing IT landscape in SMEs, including the dominance of basic communication tools and office suites, the widespread use of Windows-based workstations, the popularity of NAS platforms and affordable server solutions, as well as the reliance on Gigabit Ethernet and WLAN as core networking technologies. The paper also reviews major external and internal cyber threats affecting SMEs, with particular emphasis on software vulnerabilities, compromised credentials, ransomware, Trojans, spyware, and self-replicating malware, as well as insider threats and social engineering attacks that exploit the human factor as the weakest link. Building on this analysis, the paper proposes a concept of a low-budget, corporate-class IT infrastructure tailored to SMEs, focusing on security, performance, redundancy, scalability, and ease of administration, while remaining as hardware-agnostic as possible. The approach combines technical measures-such as patch management, network segmentation, and the deployment of next-generation firewalls-with organizational controls and security awareness initiatives. The ultimate goal is to enable SMEs to achieve a significantly higher level of cyber resilience without requiring enterprise-scale resources.

Keywords: small and medium-sized enterprises, SME, IT infrastructure, cybersecurity, risk assessment, digital transformation

Introduction

The contemporary small and medium-sized enterprise (SME) sector faces increasingly serious challenges related to digitalization and cybersecurity. These challenges are often defined with large corporations in mind and strongly depend on their capabilities, which places smaller organizations at a disadvantage due to limited human and material resources. Cybercriminals frequently use exactly the same tools against both large and small entities, while the latter have significantly smaller budgets dedicated to protection. At the same time, today's market effectively forces SMEs to undergo digital transformation, making their business processes directly dependent on IT infrastructure, without facilitating access to infrastructure that is sufficiently efficient, reliable, scalable, and adequately redundant.

This paper assumes a detailed analysis of market requirements and the design of a low-budget, corporate-class IT infrastructure. The goal is to enable effective protection of company resources while providing modern support

Cite this Article as: Mateusz KRAUZE and Mariusz ZAL, Vol. 2025 (29) "Cybersecurity Threats and IT Infrastructure in SMEs: An Analysis and Practical Implications " Communications of International Proceedings, Vol. 2025 (29), Article ID 4646725, https://doi.org/10.5171/2025.4646725

for business processes, regardless of the organization's financial capacity. The design assumptions focus on security, performance, redundancy, scalability, and ease of administration. An important advantage of the proposed approach is its universality and template-based nature, aimed at minimizing dependence on specific hardware platforms and allowing implementation on a wide range of devices. The sources used will be a combination of scientific literature, reports from reputable companies, conference presentations, and online resources, with the intention of employing the most up-to-date and trustworthy data in each case.

A corporate-class solution is characterized by careful attention to detail, which is particularly important in the context of cyber threats. Therefore, the initial part of the work focuses on analysing the potential adversary, relevant statistics, and the actual threat landscape for the SME sector. This is followed by an overview of detection mechanisms that actively participate in security incident management. Equal weight is given to preventive measures that offer administrators a realistic chance of responding quickly enough. Once the required safeguards have been identified, the next stage of analysis addresses the services that organize and build the infrastructure and its resources in practice. Virtualization, data storage, and monitoring are treated as the absolute minimum for an efficient implementation. Appropriate competences should enable the deployment of the proposed objectives in a newly created infrastructure; consequently, the subsequent sections of the paper successively refine the assumptions, describe the practical implementation, and present extensive testing. The final solution is intended to be resilient to all forms of disregard for both data and physical equipment..

Cyber Threat Analysis in the IT Infrastructure of Small and Medium-Sized Enterprises

Further analysis in the context of SME cybersecurity requires a precise specification of the size of these entities. This makes it possible to determine both the scale of the threats they face and the amount of resources available to them for mitigating cyber risks. The basic classification criteria are the number of employees and the annual turnover or balance sheet total. According to the definition adopted by the European Union [1]:

- micro-enterprises employ fewer than 10 people and have an annual turnover or balance sheet total not exceeding 2 million euro;
- small enterprises employ between 10 and 49 people and have an annual turnover or balance sheet total not exceeding 10 million euro;
- medium-sized enterprises employ between 50 and 249 people and have an annual turnover not exceeding 50 million euro or a balance sheet total not exceeding 43 million euro.

The difference between the largest and smallest entities within the SME category is therefore substantial, amounting in some cases to several dozen-fold discrepancies in the level of available resources.

In the context of SME resources, a key factor determining both efficiency and resilience to operational risks is the level of digitalization and the quality of the IT infrastructure. The sector's limited capabilities do not translate into a reduced demand for high service availability (uptime). A report by Organisation for Economic Co-operation and Development (OECD) notes that the current state of digitalization in enterprises leaves much to be desired, which directly affects the risk assessment associated with maintaining high availability of IT services [2]. Any unplanned interruption in the operation of services essential for day-to-day business may result in disruptions to the execution of core business processes.

The analysis presented in the report indicates that the level of digital maturity among SMEs is relatively low[15]. Many enterprises rely solely on basic technological solutions used in everyday operations, which is often linked to the absence of dedicated organizational structures for the deployment of modern technologies. It turns out that only 18.4% of companies maintain dedicated units responsible for IT services, while the remaining enterprises assign these tasks to employees in other roles. This prevents the effective and consistent development of a stable infrastructure capable of adapting to changing market conditions.

In addition, budgeting for the development and maintenance of IT infrastructure constitutes a further factor that increases the overall risk level in SMEs. The report shows that investments in digital technologies often focus solely on the purchase of basic equipment such as computers, peripheral devices, and telecommunications hardware. The lack of funds for the development of advanced IT systems and for building employees' digital competences again results in a situation where achieving high service availability is practically impossible. IT budgets in most SMEs are limited and concentrated mainly on ensuring the minimum infrastructure necessary for day-to-day operations.

Against this background, the fact that insufficient funds are allocated to IT resources compares unfavourably with the statistics presented by the Union of Entrepreneurs and Employers and the company Symfonia in their report on the level of digitalization in the SME sector [3]. We learn that only 32% of company owners declare that they do not use any digital tools. In addition, 14% of respondents use cloud solutions, while 13% have implemented Enterprise Resource Planning (ERP) systems. At the same time, only 9% state that they definitely do not intend to continue digitalizing their company.

As shown by the Polish Agency for Enterprise Development in its report, the most widespread work tools are various communication programs and office suites, primarily Microsoft Office [4]. This is linked to the dominance of the Windows operating system and traditional desktop and laptop computers. Entrepreneurs in the SME sector often choose solutions that offer a good price-to-performance ratio. Maciej Urbanek, writing for the CRN Polska portal, identifies Network Attached Storage (NAS) servers as a frequent choice [5]. Platforms such as those offered by QNAP are popular among SMEs due to their ease of use, competitive pricing, and functionality. They are used for data storage, backup creation, and as file servers. Modern models provide features such as support for virtualization, data encryption, power redundancy, and various expansion options. The report cites a statement by Kornelia Szlósarczyk, a sales specialist at Action, who emphasizes that “In smaller enterprises there is still a belief that a server is a complicated machine and that to use it you have to be an IT specialist. People look at NAS devices completely differently. A user-friendly interface and easy configuration make them as simple to use as a computer or smartphone. Attractive prices also encourage their purchase.” At the same time, server vendors continue to report sustained demand for their products in the SME sector. A universal server platform offers greater flexibility, but here too significant attention is paid to hyperconverged configurations, which in a sense represent a nod towards NAS solutions.

A similar situation can be observed in the area of computer networks. The most commonly chosen standard is Gigabit Ethernet, due to its favourable price-to-performance ratio. Mariusz Kochański, a board member of Veracomp, a company specializing in cybersecurity, stated in CRN Polska that this does not constitute a technological debt [6]. Gigabit Ethernet is fully sufficient for the needs of most SMEs. The same article also highlights the growing interest in WLAN networks and the satisfactory speeds offered by the latest IEEE 802.11 standards defining Wi-Fi operation. Computer networks are no longer just a gateway to the Internet, but increasingly form the foundation of all digitalized business processes. This is associated with the large volume of confidential data processed by IT infrastructures and the growing need to ensure their security. Although, as long as an enterprise does not use cloud services, the Internet may not be the single most critical service, it remains relatively crucial. Returning to the data provided by Symfonia, broadband Internet access is becoming increasingly widespread in Poland and is no longer a major issue in urban areas [3]. Consequently, the edge device of the network must not become a bottleneck in any of the aforementioned aspects.

A common and practical solution in this context is the use of Next Generation Firewalls (NGFW), which go far beyond basic packet routing and simple filtering. NGFWs extend beyond Layer 3 of the Open Systems Interconnection Reference Model (OSI RM) defined by the International Organization for Standardization (ISO) and may operate up to Layer 7, offering such functions as routing, firewalling and filtering of specific services or applications, VPN services, and protection against malware, among others. The Grand View Research report entitled “Next-generation Firewall Market Size & Share Report, 2030” indicates a growing interest in such solutions and forecasts that this market in the SME sector will grow by 12.3% year-on-year until 2030 [7]. This confirms the increasing demand for cybersecurity and for controlling data flows even among the smallest enterprises.

Classification of Cyber Threats

Enterprises are increasingly becoming targets of sophisticated cybercriminal campaigns. SMEs, which lack extensive resources, redundant systems, and specialized IT staff, find themselves at a significant disadvantage in the fight against cybercriminals. The most effective response in such conditions is the proactive management of IT infrastructure, with a focus on prevention so as not to enter an inherently unequal struggle. A key prerequisite for this approach is understanding the mechanisms against which one is defending. Each year, Sophos conducts research and publishes a report entitled The State of Ransomware, presenting key statistics on cyberattacks against enterprises. Based on the 2024 edition of this report, it is possible to identify the main cybersecurity challenges faced by SMEs [8].

The most common initial access vector in external attacks-accounting for 32% of all cases-is software vulnerabilities resulting from the use of outdated technologies or simple negligence in regularly updating the software in use. Virtually no application is perfectly secured and most contain code fragments or functionalities that attackers can exploit to achieve their objectives. Cybercriminals continuously search for new security flaws,

and developers respond by fixing these weaknesses. This makes patch management and monitoring the quality of vendor support for hardware and software critically important. Another major attack vector is the compromise of user credentials within organizational systems (29%), most frequently caused by data theft and data leaks. It is worth emphasizing that brute-force password attacks account for only 3% of all incidents. In addition, social engineering attacks-such as phishing or downloading malware from e-mail messages and the Internet-also play a significant role. These statistics are summarized in Figure 1.

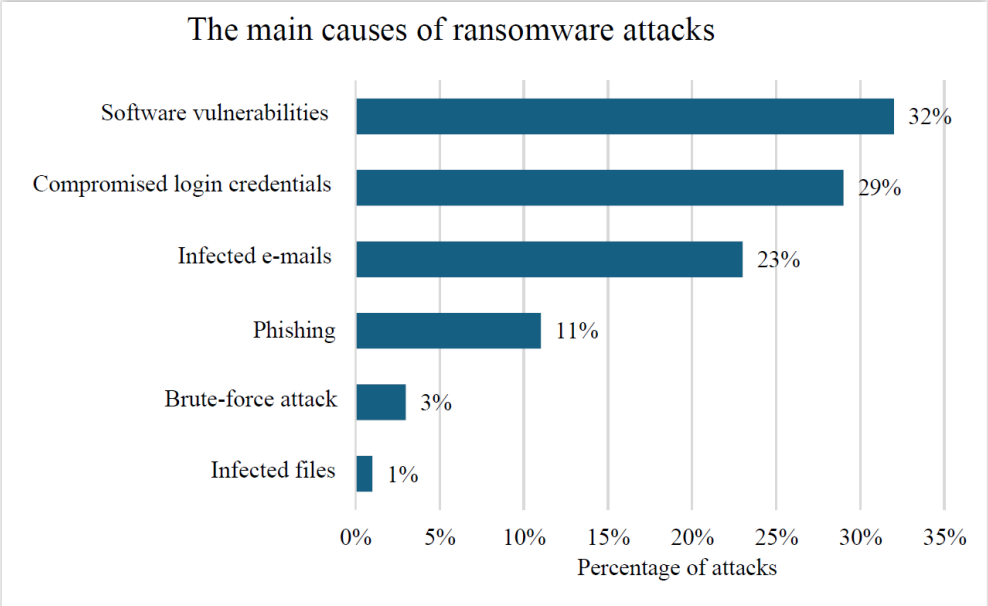

Figure 1. Initial access vectors of attacks [14]

A successful external attack most often results in the encryption of the victim's data-this occurs in 70% of cases-while in 32% of incidents the attackers also exfiltrate data. The encryption process is carried out by ransomware, which, once it infiltrates the infrastructure, gradually reconnoitres the environment and encrypts the data it encounters. The attackers then demand a ransom in exchange for providing a decryption method, often additionally threatening to disclose the stolen information if the requested amount is not paid [9].

Another prevalent and critically dangerous class of malware is the Trojan horse (hereafter: Trojan), which masquerades as legitimate software in order to infect systems and enable cybercriminals to gain unauthorized access to a company's data or resources. Trojans are frequently used to install additional malicious software or to monitor user activity. Their operation may lead to data theft, espionage, or facilitate further infections with other types of malware. A related example is spyware-dedicated surveillance tools used to track users and obtain sensitive information such as passwords, financial data, or trade secrets. Less common, but still highly dangerous, are viruses and self-replicating worms that spread within the infrastructure. These can significantly affect the performance and reliability of services, causing numerous anomalies in the operation of IT systems [10].

No system can be secure if its users are not aware of the consequences of their actions; hence it is crucial to develop competencies not only among IT staff, but also among the rest of the workforce. This also explains the popularity of attacks that exploit human vulnerability rather than weaknesses in hardware or software. Malicious e-mails, spoofed websites, distribution of infected files, and the deliberate use of removable storage media are only some of the methods employed by cybercriminals. The Verizon 2024 Data Breach Investigations Report (DBIR) reveals that 35% of security breaches result from internal activities, 73% of which are unintentional errors, such as misconfiguration of systems or accidental data disclosure [11]. DBIR suggests that investment in training programmes and support mechanisms that help employees detect and report incidents could potentially improve security outcomes in more than two-thirds of cases where the human factor plays a role. The revolution in IT should not be limited to investments in corporate-grade solutions, but must also involve building a strong security culture within the organization.

The most common topic in cybersecurity training for end users concerns aspects related to social engineering. Defending against attacks that target people rather than systems remains an external threat only as long as it is possible to filter out contact attempts-which is never feasible in 100% of cases. At that point, the administrator

must ultimately rely on the end user. Social engineering attacks, constitute a form of manipulation that targets humans as the weakest link in the information security system [12]. A particularly significant threat is posed by various forms of phishing, whose aim is cognitive manipulation leading to the disclosure of sensitive data, such as authentication credentials, or to the installation of malicious software. The differences between these attacks boil down to the communication channel used; e-mail, SMS messages, and voice calls are all observed in practice. According to the authors, the effectiveness of such attacks is based on psychological mechanisms of social influence, such as authority, time pressure, reciprocity, and trust building. Moreover, in some scenarios the contact with the attacker is initiated by the victim, which significantly reduces their vigilance and critical scrutiny [13]. This highlights the need to treat the end user as an integral component of the security architecture, primarily exposed to attacks at the behavioural layer.

Conclusions

he analysis presented in this paper confirms that SMEs operate under a structural imbalance: they are targeted by many of the same tools, techniques, and procedures as large enterprises, yet they typically lack comparable budgets, redundant infrastructure, and specialized security staff. Digitalization is no longer optional for maintaining competitiveness, but the current level of digital maturity in the SME sector remains relatively low. Many organizations confine themselves to basic IT solutions and ad hoc responsibilities for IT operations, which makes it difficult to systematically build and maintain a stable, adaptable, and secure infrastructure.

A key finding is that IT infrastructure in SMEs is usually shaped by price–performance considerations. This explains the widespread use of NAS platforms, commodity servers, Gigabit Ethernet, and WLAN technologies. While these choices are rational from a cost perspective and, in many cases, sufficient in terms of raw capacity, they are rarely complemented by an architectural approach that takes availability, redundancy, and security into account from the outset. Similarly, investments tend to focus on visible hardware rather than on advanced systems, monitoring, or the development of digital competences among staff.

The threat analysis highlights that the main external entry points for cyberattacks against SMEs are software vulnerabilities, compromised credentials, and social engineering. Ransomware remains the most impactful form of attack, often combining data encryption with data exfiltration. Additional risks are posed by Trojans, spyware, viruses, and worms. At the same time, a substantial proportion of incidents is caused or facilitated by internal actors, with unintentional errors-such as misconfigurations and accidental data disclosure-playing a dominant role. This underscores the dual nature of SME cyber risk: it is driven both by technical weaknesses and by human factors.

From these observations, several practical conclusions emerge:

- Balanced investment into SME infrastructure is essential. Focusing solely on hardware procurement is insufficient. SMEs need to combine basic infrastructure spending with targeted investments in security controls, monitoring, and staff competences.
- Patch and vulnerability management must be prioritized. Given that software vulnerabilities represent a leading initial access vector, systematic updating of systems and applications, as well as active vendor support monitoring, should be treated as a core security process rather than an optional task.
- Network and perimeter security should be modernized. Gigabit Ethernet and contemporary WLAN standards offer adequate capacity for most SMEs, but must be complemented by robust security measures. Next-generation firewalls, network segmentation, and secure remote access are particularly important for controlling traffic flows and mitigating the impact of successful attacks.
- Human factors cannot be treated as secondary. Training, awareness programmes, and clear procedures for reporting incidents are necessary to reduce the likelihood and impact of both social engineering attacks and accidental errors. Users should be explicitly recognized as integral components of the security architecture, especially at the behavioural level.
- A reference, hardware-agnostic architecture is feasible. The concept of a low-budget, corporate-class infrastructure-built around virtualization, reliable storage, backup mechanisms, monitoring, and centrally managed security controls-offers a realistic path for SMEs to increase cyber resilience without adopting overly complex or vendor-specific solutions.

In summary, improving cybersecurity in SMEs is not solely a matter of purchasing more advanced technology. It requires combining a carefully designed, cost-conscious infrastructure with organizational maturity and a security-oriented culture. The proposed approach demonstrates that, even under tight budget constraints, SMEs can significantly enhance their resilience to cyber threats by aligning technical measures, processes, and user

behaviour within a coherent security strategy.

Acknowledgement

This research was funded by the Polish Ministry of Science and Higher Education (No. 0313/SBAD/1311).

Bibliography

- European Commission, *Commission Regulation (EU) No 651/2014 of 17 June 2014 declaring certain categories of aid compatible with the internal market in application of Articles 107 and 108 of the Treaty Text with EEA relevance*, 2014. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2014/651/oj, [Accessed: 20.11.2025]
- OECD (2021), *The Digital Transformation of SMEs, OECD Studies on SMEs and Entrepreneurship*, OECD Publishing, Paris, https://doi.org/10.1787/bdb9256a-en.
- Union of Entrepreneurs and Employers, Report by the Union of Entrepreneurs and Employers and Symfonia on the 2023 SME digitisation level "Digitisation of the SME sector in Poland", [Online]. Available: https://zpp.net.pl/en/report-by-the-union-of-entrepreneurs-and-employers-and-symfonia-%E2%80%A8on-the-2023-sme-digitisation-level-digitisation-of-the-sme-sector-in-poland/, [Accessed: 20.11.2025]
- Polish Agency for Enterprise Development. (2023). *The IT/ICT Sector in Poland – report 2023*. Warsaw: PARP.
- M. Urbanek, "Małe firmy w świecie wielkich danych," CRN Polska, Sep. 30, 2019. [Online]. Available: https://crn.pl/artykuly/male-firmy-w-swiecie-wielkich-danych/. [Accessed: 20.11.2025]
- European Commission. (2024). Poland 2024 Digital Decade Country Report. Brussels: European Commission. [Online]. Available: https://digital-strategy.ec.europa.eu/en/factpages/poland-2024-digital-decade-country-report [Accessed: 20.11.2025]
- Grand View Research. (2024). *Next-generation Firewall Market Size, Share & Trends Analysis Report, 2022–2030*. San Francisco, CA: Grand View Research. [Online]. Available: https://www.grandviewresearch.com/industry-analysis/next-generation-firewall-market-report [Accessed: 20.11.2025]
- Sophos, *The State of Ransomware 2024*, Oxford, UK, 2024. [Online]. Available: https://news.sophos.com/en-us/2024/04/30/the-state-of-ransomware-2024/ [Accessed: 20.11.2025]
- Check Point, Ransomware Attack – What Is It and How Does It Work? (section: "Why Are Ransomware Attacks Emerging?"), 2025. [Online]. Available: https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/ [Accessed: 20.11.2025]
- Elsevier, "Computer Worms – an overview," in ScienceDirect Topics: Computer Science, 2025. [Online]. Available: https://www.sciencedirect.com/topics/computer-science/computer-worms. [Accessed: 20.11.2025]
- Verizon, 2024 Data Breach Investigations Report (DBIR), 2024. [Online]. Available: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf [Accessed: 20.11.2025]
- A. A. Abubaker, D. Eleyan, A. Eleyan, T. Bejaoui, N. Katuk and M. Al-Khalidi, "Social Engineering in Social Network: A Systematic Literature Review," 2023 International Symposium on Networks, Computers and Communications (ISNCC), Doha, Qatar, 2023, pp. 1-7, doi: 10.1109/ISNCC58260.2023.10323826.
- C. Lekati, "Psychological Exploitation of Social Engineering Attacks," Cyber Risk GmbH, [Online]. Available: https://www.cyber-risk-gmbh.com/Psychological_Exploitation_of_Social_Engineering_Attacks.html. [Accessed: 20.11.2025]
- DeepStrike. Ransomware Statistics 2025: Trends, Costs, and Key Threats [Online]. Available: https://deepstrike.io/blog/ransomware-statistics-2025 [Accessed: 20.11.2025]
- ASM – Centre for Research and Market Analysis Ltd. (2023). *On the road to digital excellence*. (In Polish) Ministry of Digital Affairs. [Online]. Available: https://ai.gov.pl/media/2023/06/Raport_koncowy_z_badania_malych_srednich_przedsiebiorstw__MC_2023__06__19.pdf [Accessed: 20.11.2025]