Scientific Research Publishing

Journal of Information Security, 2025, 16(1), 1-43
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

# Cybersecurity Guide for SMEs: Protecting Small and Medium-Sized Enterprises in the Digital Era

**Anastasios Papathanasiou[1,2*], George Liontos[3], Athanasios Katsouras[3], Vasiliki Liagkou[2], Euripides Glavas[2]**

[1]Cyber Crime Division, Hellenic Police, Athens, Greece
[2]Department of Informatics and Telecommunications, University of Ioannina, Kostaki Artas, Arta, Greece
[3]Department of Materials Science and Engineering, University of Ioannina, Ioannina, Greece
Email: *anastasios.papathanasiou@gmail.com

**How to cite this paper:** Papathanasiou, A., Liontos, G., Katsouras, A., Liagkou, V. and Glavas, E. (2025) Cybersecurity Guide for SMEs: Protecting Small and Medium-Sized Enterprises in the Digital Era. *Journal of Information Security*, **16**, 1-43.
https://doi.org/10.4236/jis.2025.161001

**Received:** October 9, 2024
**Accepted:** November 16, 2024
**Published:** November 19, 2024



## Abstract

Small and Medium-sized Enterprises (SMEs) are considered the backbone of global economy, but they often face cyberthreats which threaten their financial stability and operational continuity. This work aims to offer a proactive cybersecurity approach to safeguard SMEs against these threats. Furthermore, to mitigate these risks, we propose a comprehensive framework of practical and scalable cybersecurity measurements/protocols specifically for SMEs. These measures encompass a spectrum of solutions, from technological fortifications to employee training initiatives and regulatory compliance strategies, in an effort to cultivate resilience and awareness among SMEs. Additionally, we introduce a specially designed a Java-based questionnaire software tool in order to provide an initial framework for essential cybersecurity measures and evaluation for SMEs. This tool covers crucial topics such as social engineering and phishing attempts, implementing antimalware and ransomware defense mechanisms, secure data management and backup strategies and methods for preventing insider threats. By incorporating globally recognized frameworks and standards like ISO/IEC 27001 and NIST guidelines, this questionnaire offers a roadmap for establishing and enhancing cybersecurity measures.

## Keywords

Cybersecurity, Cybercrime, SMEs (Small and Medium-Sized Enterprises), Risk Management, Ransomware, Phishing, Social Engineering, Malware

## 1. Introduction

In an era dominated by digital advancements and interconnected technologies, small and medium enterprises (SMEs) stand at the forefront of economic growth

and innovation. These businesses are often referenced as the backbone of economies worldwide due to their contribution to job creation, wealth generation and community development. The diversity of SMEs is vast, encompassing a wide array of industries and business models, each with unique challenges and opportunities. At one end of the spectrum, SMEs include local shops, family-owned businesses and retail stores-businesses that are deeply rooted in their communities and focused on providing essential services. On the other end, there are highly specialized SMEs such as defense industry contractors, innovative tech startups and one-person cybersecurity consultancies, which operate in complex, highly regulated environments and often serve specialized markets. This broad spectrum highlights the versatility of SMEs, demonstrating their ability to thrive in various sectors, from traditional trades to cutting-edge technology, each requiring different approaches to management, growth, and, notably, cybersecurity.

According to the World Bank SMEs represent about 90% of businesses and more than 50% of employment worldwide [1], and according to the Annual Report on European SMEs for 2022, SMEs represent over 99% of enterprises in the European Union. In accordance with EU Recommendation 2003/361, SMEs are classified as micro, small and medium-sized enterprises based on staff headcount and turnover or balance sheet total, as illustrated in **Table 1** [2].

**Table 1.** Classification of SMEs.

| Company Category | Staff Headcount | Turnover |
|---|---|---|
| Medium-sized | <250 | ≤€43 m |
| Small | <50 | ≤€10 m |
| Micro | <10 | ≤€2 m |

In 2023, the global average cost of a data breach was USD 4.45 million, marking a 15% increase over the past three years. Consequently, 51% of organizations are planning to increase their security investments, focusing on areas such as incident response planning and testing, employee training, and threat detection and response tools. Notably, organizations that extensively utilize security AI and automation save an average of USD 1.76 million compared to those that do not, highlighting the financial benefits of advanced cybersecurity measures [3].

However, as SMEs are in a continuous effort to exploit the power of technology and expand their market reach, they often find themselves exposed to an escalating and complex web of cyber threats and cybersecurity challenges. Research indicates a significant lack of cybersecurity awareness and resources among Small and Medium Enterprises (SMEs), making them vulnerable to cyber threats [4].

Due to budget constraints, small and medium enterprises often lack specialized departments such as those dedicated to social engineering, blue and red teams and extensive IT infrastructure, as seen in larger enterprises. It is crucial for these businesses to comprehend the risks associated with ineffective cybersecurity practices. This paper aims to highlight not just the prevailing cybersecurity threats, including social engineering, ransomware, BEC attacks, malware and insider threats, but

also intends to provide a practical survival guide. This guide incorporates both technical and non-technical measures, serving to assist enterprises in crafting a robust risk management plan. Such a plan not only enhances their resilience against cyber threats but also ensures compliance with ISO and data protection standards. SMEs often struggle with limited budgets, insufficient expertise, and inadequate security practices [5]. Key challenges include a lack of awareness of cybersecurity risks, limited cybersecurity literacy, and constrained financial resources [6].

SMEs face several common cybersecurity threats that can severely impact their operations and reputation. These include network hacking, leading to data breaches, data theft of sensitive information and malware, such as viruses, ransomware, and spyware, which disrupt operations and cause financial losses. Mobile device compromise and phishing attacks, where employees are deceived into revealing sensitive information, are also critical risks. These threats emphasize the need for SMEs to adopt strong cybersecurity measures to protect their digital assets and maintain customer trust [7] [8].

As SMEs grapple with evolving cyber threats and limited resources, next-generation solutions, including artificial intelligence (AI) and machine learning (ML), present transformative opportunities. AI-driven tools offer advanced threat detection, predictive analytics, and automated response capabilities, which can significantly enhance cybersecurity posture without requiring extensive human oversight. Machine learning algorithms can analyze vast amounts of data to identify patterns and anomalies that may indicate potential security breaches, enabling SMEs to respond more swiftly and accurately. By integrating AI and machine learning, SMEs can bridge some of the gaps caused by limited budgets and expertise, effectively leveling the playing field with larger enterprises [9].

In this paper, our contribution is centered around addressing the critical cybersecurity challenges faced by small and medium-sized enterprises (SMEs). Recognizing the unique vulnerabilities of SMEs—such as limited resources, lack of specialized expertise, and an increasing reliance on digital technologies—we present a multifaceted approach aimed at bolstering their cybersecurity resilience. A key component of this contribution is the development of a Java-based cybersecurity evaluation tool, which is designed to offer an initial assessment of an SME's cybersecurity posture. This tool, structured around a 30-question questionnaire, provides SMEs with an accessible, free resource to evaluate their cybersecurity readiness and identify areas for improvement. The questions within the tool were carefully selected based on internationally recognized frameworks such as ISO/IEC 27001:2022, the NIST Cybersecurity Framework, and ISO/IEC 27701:2019, ensuring that the tool adheres to best practices and industry standards.

Our work also includes a detailed analysis of both technical and non-technical measures that SMEs can adopt to enhance their cybersecurity defenses. These measures cover key areas such as malware protection, network security, data backup and encryption, physical security, and regular policy reviews. By addressing these fundamental aspects, we provide a practical guide for SMEs to strengthen their

security practices in line with their operational needs and constraints.

In our research, a systematic search strategy was employed across various academic search engines, such as Google Scholar, Core, Scopus, etc., to conduct the literature review (Figure 1). This search process is grounded in systematic literature review (SLR) methodologies, which emphasize transparency and replicability. SLR methods are widely used in academic research to comprehensively explore existing literature, ensuring the inclusion of relevant studies and eliminating biases in the review process.


Figure 1. Steps of the research methodology.

Following SLR principles, multiple keywords and key phrases such as "cybercrime," "phishing attacks," "social engineering," "ransomware," "malware," "cyberthreats for enterprises," and "NIS directives" were used to retrieve pertinent studies. A pilot search was conducted, after which we implemented an inclusion/exclusion procedure based on predefined criteria to ensure the selection of studies directly relevant to our research objectives. Furthermore, we employed the snowball sampling technique to identify additional relevant sources by exploring the references of the initial studies selected.

Once the literature was gathered, we applied thematic analysis, a qualitative research method that allows for the identification of patterns, themes, and concepts within the data. This method helped categorize the literature into major themes related to cyber threats, NIS directives, and enterprise security measures.

Subsequently, a critical evaluation was conducted, grounded in research methods, to assess the validity and reliability of the identified studies. This process involved a thorough analysis of the methodologies, evidence bases, and theoretical frameworks employed in each study, ensuring that only high-quality, credible sources were included in our review.

While this methodology has been employed in various systematic literature studies, it comes with certain constraints. One limitation is its capacity to narrow

the scope of the review or study, possibly leaving readers with an incomplete grasp of the subject matter. Moreover, our data collection was confined to just four scientific search engines, which might restrict the range of publications included in our review. Although these sources are deemed reliable, the limitation arises from not exploring all potential sources to identify articles relevant to our study objectives.

## 2. Main Cybersecurity Threats and Attacks against SMEs

Small and medium-sized enterprises are increasingly becoming prime targets for cybercriminals, largely due to their often limited cybersecurity resources and defenses. The rapidly evolving digital landscape exposes these businesses to a wide range of cyber threats, including social engineering, phishing, malware, ransomware, and insider attacks. These attacks exploit both technical vulnerabilities and the human factor, leading to significant financial losses, operational disruptions, and reputational damage. This section explores the main cybersecurity threats facing SMEs, analyzing their characteristics, attack methods, and the potential consequences for businesses. By understanding the nature of these threats, SMEs can better prepare and implement effective countermeasures to safeguard their digital assets and ensure long-term security.

### 2.1. Social Engineering

According to ENISA (European Union Agency for Cybersecurity), the term social engineering refers to "all the techniques aimed at talking a target into revealing specific information or performing a specific action for illegitimate reasons" [10]. Social engineering doesn't stop only at talking to a target in order to deceive him, but it can also be combined with other techniques described in later chapters like phishing attacks, ransomware attacks and others.

Social engineering is defined as the psychological manipulation of human behavior with the aim of influencing people to act in certain ways or to divulge confidential information. It is a technique that exploits our cognitive biases and fundamental instincts, such as trust, authority, urgency, familiarity and others, in order to gather information, deceive, or gain access to systems. Social engineering is the "favorite" tool of cybercriminals, who, in several cases, use social networking platforms and emails for its execution [11].

Executing social engineering successfully requires a detailed gathering of information about the target, aiming to enhance the persuasiveness or deceitfulness of the approach. This information-gathering process, referred to as doxing, is facilitated through a technique known as OSINT (Open-Source Intelligence). OSINT encompasses both non-technical methods, such as observation skills, and technical methods involving the extraction of information from sources like social media, search engines, websites and general data derived from both the visible web and the dark web. It's noteworthy that tools designed for this purpose are increasingly accessible and user-friendly in the present day, exemplified by the

likes of Kali Linux tools including Maltego, Social Engineering Toolkit (SET), Ratoll and others, meaning that social engineering doesn't require expertise in technical skills and can be performed by any malicious actor with limited to high technical skills.

The next step after gathering information about the target is establishing an emotional relationship with the victim through the following basic social engineering principles:

• Claiming Authority: This technique is notably effective as individuals are more prone to respond to figures of authority. Attackers may assert authority through various means, such as verbal communication or email spoofing.

• Intimidation: Often stemming from authority, intimidation involves leveraging authority, confidence, or even threats of harm to motivate a person to carry out actions on behalf of the attacker.

• Consensus: Exploiting a person's natural inclination to mimic the actions of others or those perceived as having done something in the past characterizes the consensus technique.

• Familiarity: This principle capitalizes on a person's inherent trust in the familiar, meaning individuals are more inclined to trust someone with common contacts or relationships, *i.e.*, a known entity.

• Trust: As a social engineering principle, trust involves the effort an attacker makes to cultivate a relationship with a victim.

• Urgency: This technique exerts pressure on the victim to act swiftly, denying them the time needed for careful consideration of their actions.

• Phishing: A form of social engineering attack that focuses on stealing credentials or identity information.

Salahdine *et al.* [12] categorize social engineering techniques into three distinctive categories:

1) Technical based: Technical based attacks can be launched remotely with the use of malicious software like malware in email attachment or SMS. Characteristic examples are phishing, smising, ransomware, etc.

2) Social based: Social based attacks are carried out via the internet, targeting social networks and online service websites. These endeavors aim to collect specific information, such as passwords, credit card details, and other sensitive data.

3) Physical based: Physical based attacks are conducted with the physical presence of the attacker who tries to steal desired information and data by interacting with the victim. Examples of this category include shoulder surfing, impersonation, social engineering via phone, or gaining physical access to data within the victim's working environment.

Social engineering serves as the common factor in the majority of cyberattacks on SMEs, as the gathering of information for a target and the application of key psychological techniques are essential components of nearly every major cyberattack scheme. The success of social engineering techniques lies in their exploitation of the weakest link of all—the human factor.

## 2.2. Phishing

One of the most prevalent threats that SMEs face is phishing attacks. These deceptive tactics involve malicious actors posing as trustworthy entities to manipulate individuals into divulging sensitive information. SMEs, with their diverse workforce and sometimes limited resources for extensive cybersecurity training, can be particularly vulnerable to phishing schemes. A successful phishing attack can lead to unauthorized access to critical systems, compromising sensitive data and potentially causing irreparable damage to the business.

According to Hadnagy [13], phishing attacks can be classified into six categories:

• Spear Phishing: These attacks often involve extensive research on the target. Spear phishing involves crafting highly personalized and convincing emails in order to deceive the recipient and act on the attacker's behalf.

• Whaling Phishing: A variation of spear phishing, this attack specifically targets high-profile individuals. In whaling phishing attacks, cybercriminals impersonate a senior executive or trusted authority figure within the organization and send fraudulent emails to employees, suppliers or business partners. These emails typically request urgent action, such as wire transfers or the disclosure of sensitive information. Whaling attacks are often sophisticated and carefully crafted to mimic the communication style and authority of the targeted individual, thus making them difficult to detect.

• Vishing Phishing: This term pertains to phone phishing, wherein phishing attempts are conducted through voice communication. In these schemes, cybercriminals usually impersonate trusted entities like banks or government agencies, exploiting social engineering tactics to manipulate victims.

• Smishing: Referring to phishing via SMS communication, this method is commonly employed to deliver malware to mobile devices or to steal credentials. These messages often contain urgent requests or offers designed to prompt recipients to click on malicious links, call fraudulent phone numbers or provide sensitive information like account credentials or personal details.

• Interactive Voice Response Phishing (IVR): In IVR phishing attacks, victims receive automated phone calls that impersonate legitimate organizations such as banks, government agencies, or other enterprises. These calls typically prompt recipients to follow voice orders in order to enter personal information such as account numbers, passwords, etc., using their smartphones.

• Business Email Compromise Phishing: This term encompasses scams that typically involve the compromise of legitimate business email accounts. The aim is to deceive the victim into authorizing unauthorized fund transfers, divulging confidential information and, in some instances, installing malware such as keyloggers. This kind of scheme often needs extensive research on an enterprise communication system in order to effectively mimic the communication between a high-profile individual—like a CEO or CFO—making urgent requests for wire transfers or sensitive information to a department employer.

### 2.3. Malware

Malware is defined as a software that is designed to create disturbances within a computer, server, client, or computer network. Its malicious context usually proceeds to unauthorized acquisition of sensitive information, infiltration of information systems or deliberate denial of access to critical data. This kind of software poses a multifaceted threat, aiming to compromise digital security by not only causing operational disruptions but also compromising the confidentiality and integrity of private information [14].

Saeed *et al.* [15] characterized malware by its capacity for replication, propagation, self-execution and the ability to corrupt computer systems. The corruption of a computer system can have far-reaching consequences, affecting the essential aspects of data security. Replication stands out as a pivotal characteristic for most malware, ensuring its sustained existence. In certain instances, the relentless replication of malware may lead to the depletion of critical computer resources, such as hard disk space and RAM.

The property of invisibility is widely utilized by many types of malwares to elude detection by anti-malware programs. This evasion is often achieved through techniques like polymorphism or metamorphism. Polymorphic or metamorphic malware can alter its code structure, making it challenging for traditional security measures to recognize and combat it effectively.

The common method employed by malware to infect a system involves the transfer of the malicious software from a compromised device to an uninfected one. This transmission occurs through local or network filesystems, affecting data, executable files or consuming network bandwidth. Operating system vulnerabilities and software bugs serve as entry points for malware, exploiting the faults present in a few software programs. Once planted, malware can initiate its lifecycle on the same system or assume remote control, facilitating infection operations on other systems. This intricate analysis underscores the multifaceted nature of malware and the diverse tactics it employs to compromise digital systems.

### 2.4. Ransomware

Ransomware is a type of malicious software that encrypts a user's files and demands payment for their release. According to statistics from OpenText, nearly half of small and medium-sized businesses (SMBs) and enterprises of those surveyed, fell victim to ransomware attacks in 2023 [16]. This alarming figure underscores the pervasive threat that ransomware poses to organizations of all sizes. Ransomware attacks can cause significant disruptions to business operations, leading to financial losses, reputational damage, and even data breaches. As cybercriminals continue to evolve their tactics and target more sophisticated victims, it becomes increasingly crucial for businesses to invest in cybersecurity measures and employee training to mitigate the risk of falling prey to such attacks. The crippling effects of a ransomware attack extend beyond financial losses, often disrupting regular business operations and corrupting customer trust. SMEs, with their reliance

on interconnected systems and digital data and their low cybersecurity level are attractive targets for ransomware operators seeking quick financial gains.

According to Aurangzeb *et al.* [17] a ransomware infiltrates the victim's machine through malicious websites, email attachments and deceitful web links. Upon infecting the system, it establishes communication with a Command and Control (C&C) server. Subsequently, it commences the extraction of the victim's information, forwarding it to the attacker. Simultaneously, the attacker obtains a randomly generated symmetric key from the C&C server. Following this, the ransomware initiates the encryption of files and folders using asymmetric (RSA) encryption, wherein the key employed for encryption lacks the capacity to decrypt the data. The RSA algorithm utilizes two distinct keys—an encryption key (public key) and a decryption key (private key). Concurrently, the malware eradicates all restore points, backup folders and shadow volume copies.

Shopho's report for ransomware attacks [18] states that emails were identified as the primary factor of cyber-attacks. Specifically, 18% were initiated from a malicious email, 13% from phishing attempts, 3% from brute force attacks, a mere 1% from a downloaded source and 36% from exploited vulnerability (**Figure 2**).


**Figure 2.** Shopho's report for ransomware attacks [18].

## 2.5. Business Email Compromise (BEC) Phishing Attacks

The usefulness of email in our daily lives is undeniable, with an estimation of 333.2

billion emails sent and received globally each day in 2022 [19]. While email is an indispensable communication tool, its use has also given rise to an escalation in cyber threats, notably exemplified in the form of Business Email Compromise (BEC) attacks. BEC attacks are sophisticated scams involving email fraud where attackers masquerade as trusted entities to manipulate employees into transferring money or sharing sensitive information. These attacks exploit the trust and routine procedures within organizations, making them particularly dangerous and effective.

Unlike typical phishing scams that may target anyone, BEC schemes are carefully tailored and researched, often involving reconnaissance of the targeted company and its employees. This level of personalization makes BEC attacks not just challenging to detect but also more likely to succeed. Their significance lies in the direct financial losses and potential data breaches they can cause, along with the long-lasting damage to the reputation and trust within and outside the organization. As BEC attacks continue to rise, both in frequency and sophistication, understanding their nature and the importance of vigilance and reporting becomes paramount for businesses of all sizes [20].

In a typical BEC attack, the attacker usually assumes the identity of a legitimate sender (trusted entity) to manipulate the recipient into divulging sensitive information or transferring funds. This sophisticated scheme typically unfolds through carefully designed steps. The attackers, with the use of open-source intelligence techniques (OSINT) gather valuable information and by exploiting this intelligence craft a deceptive email, skillfully adopting the identity of a trusted entity or source.

Within the deceptive email, the attacker often employs social engineering techniques, designed to manipulate, and force the recipient into taking actions that ultimately serve the scammer's interests. Alternatively, the email might bear malicious payloads, such as viruses concealed in various attachments or deceptive links. These actions serve a dual purpose: firstly, compromising the victim's communication channels, potentially enabling the interception of sensitive information, and secondly, seeking to extract money or valuable data from the unsuspecting victim.

In essence, BEC attacks embody a cybersecurity threat that combines target identification, information gathering through OSINT, persuasive impersonation and deployment of malicious software or links. This calculated combination of tactics enables perpetrators to achieve their illicit objectives, making BEC attacks a potent and evolving threat in the realm of cybersecurity by exploiting both technical (malicious payloads) and non-technical (social engineering, OSINT) techniques [21].

### 2.6. Insider Threats

Insider threats, which originate from employees and other insiders within an organization, represent a substantial security challenge. These threats can be particularly

hazardous because insiders possess intimate knowledge of the system and often have access to sensitive data. Detecting and preventing insider threats can be challenging due to these factors. The consequences of insider incidents can be severe, ranging from financial losses to jeopardizing national security. Hence, it is imperative for organizations to establish policies, procedures, and tools specifically designed to tackle insider threats effectively. By implementing comprehensive measures, organizations can better safeguard their systems and sensitive information from insider-related risks.

According to CISA [22] insider threat refers to the risk of an individual with authorized access or knowledge within an organization utilizing that access or information to inflict harm on the organization. This harm may manifest through intentional, negligent, or unwitting actions, all of which can have adverse effects on the organization's integrity, confidentiality and availability.

There are four categories of insider's threat according to Hayden *et al.* [23]:

1) The group of people who have malevolent intent to cause damage to their company (malicious insider threat).

2) The group of people who does not agree with the company's policies and instead they firmly believe that another policy must be enforced (malicious insider threat).

3) The group of people who are characterized by excessive curiosity, frequently breaching the principle of only knowing what is necessary (unintentional insider threat).

4) The group of people who commit violations due to their ignorance (unintentional insider threat).

While external threats are widely acknowledged, the danger posed by insider threats within an organization is equally significant. Employees, whether intentionally or unintentionally can become conduits for cyber threats. Unsecured access credentials, accidental data leaks, or disgruntled employees with malicious intent can compromise the security of SMEs from within [24].

## 3. Risk Management Strategies for Small and Medium Enterprises (SMEs)

Risk management is a critical aspect of business operations for SMEs [25]. While large enterprises often have dedicated risk management departments, SMEs often oversee the need to integrate risk management into their overall business strategy due to limited resources [26]. The fact that SMEs often operate with limited financial and technological resources, makes them attractive targets for cybercriminals seeking vulnerabilities. Effective cybersecurity risk management allows these enterprises to prioritize their defenses, allocating resources strategically to safeguard against the most pertinent threats. By identifying and mitigating cyber risks proactively, SMEs can establish a security analysis and protocol within their operation.

Furthermore, as SMEs increasingly rely on digital platforms, cloud services and

interconnected technologies, the attack surface for potential cyber threats expands. Risk management practices in cybersecurity ensure that SMEs comprehensively assess their digital infrastructure, identifying vulnerabilities and potential points of entry for malicious actors. This approach is crucial for minimizing the risks associated with data breaches, ransomware attacks and other cyber threats that could compromise sensitive information.

Moreover, compliance with data protection regulations like General Data Protection Regulation (GDPR) should be a major concern for SMEs, especially considering the evolving landscape of privacy laws globally. Effective cybersecurity risk management and risk-based approach help SMEs align their digital practices with regulatory requirements, reducing the risk of legal repercussions and financial penalties. This compliance not only ensures the security of sensitive data but also enhances the trust of customers and partners who entrust their information to an enterprise or organization.

Additionally, the interconnected nature of modern business ecosystems emphasizes the need for SMEs to consider third-party risks in their cybersecurity posture. Effective risk management in this context involves evaluating and mitigating the cybersecurity risks associated with suppliers, service providers, and partners. By extending risk management practices to the broader ecosystem, SMEs can fortify their defenses against potential cyber threats that may originate externally.

The following Risk Management Strategies for small and medium-sized enterprises (SMEs) are proposed through a structured and evidence-based approach. This process involved several key steps, integrating both theoretical frameworks and empirical insights from the literature, as well as practical considerations based on the specific needs and constraints of SMEs.

The foundation of our proposed strategies lies in an extensive review of existing risk management frameworks and guidelines for SMEs, including widely accepted standards such as ISO 27001, NIST Cybersecurity Framework, and the EU NIS Directive. Through the literature, we identified common cybersecurity risks faced by SMEs and explored existing risk management approaches that have been successfully implemented in comparable organizational contexts. Moreover, we conducted an analysis to identify the most prevalent cybersecurity risks affecting SMEs. This analysis considered not only technical vulnerabilities but also the resource and knowledge constraints typical of SMEs. We utilized risk categorization methods such as the risk matrix to prioritize these risks according to their likelihood and potential impact.

### 3.1. Key Considerations for Implementing Effective Risk Management in SMEs (in Line with ISO/IEC 27005:2022)

ISO/IEC 27005:2022 provides a framework for managing information security risks, tailored to the unique characteristics of Small and Medium Enterprises (SMEs). For SMEs, establishing context involves customizing risk management

processes to fit their specific needs, defining the scope and identifying key stakeholders. This ensures a clear understanding of organizational risks within the SME's operational boundaries. Risk identification involves recognizing potential security threats and vulnerabilities pertinent to the SME's resources and technologies. Risk analysis prioritizes these risks based on their likelihood and impact, ensuring the use of appropriate methodologies that fit the SME's scale. Risk evaluation assesses the significance of identified risks, focusing on their impact on confidentiality, integrity, and availability of information assets. Risk treatment involves selecting and implementing measures to mitigate or manage these risks in a cost-effective manner, aligning with the SME's risk appetite. Documentation processes should be streamlined, with a centralized repository for easy access and organization of risk-related information. This approach helps SMEs maintain resilience and protect their information assets effectively.

#### 3.1.1. Context Establishment for SMEs According to ISO 27005/2022

For SMEs following ISO/IEC 27005:2022 guidelines [27] for managing information security risks, establishing context involves customizing the process to suit the organization's specific characteristics and requirements. This entails delineating the scope of risk management activities within the operational boundaries of the SME and creating a streamlined framework with clear policies and processes that mirror the scale and complexity of the business. Identifying key stakeholders, which may entail more direct engagement with a limited team, ensures a focused understanding of their concerns. Every SME should analyze its distinct organizational context, taking into account factors like size, industry, and regulatory environment. It is essential to set practical risk criteria that align with the SME's risk tolerance. Given resource limitations in SMEs, choosing a practical risk assessment methodology and succinctly documenting the established context are crucial considerations. Regular reviews and updates should be seamlessly integrated into the SME's operational routine to uphold relevance and resilience in addressing information security risks [28].

#### 3.1.2. Risk Identification for SMEs According to ISO 27005/2022

For SMEs adhering to ISO/IEC 27005:2022 guidelines in the realm of information security risk management, the process of identifying risks is customized to suit the distinct characteristics of SMEs. SMEs must thoroughly pinpoint and evaluate potential risks to their information security, considering the specific nuances of their business operations, resources, and technologies. This involves staying attuned to the evolving threat landscape, identifying vulnerabilities within the organization, and recognizing potential impacts on information assets. Given the typically constrained resources of SMEs, adopting a pragmatic and targeted approach to risk identification is crucial, focusing on the most significant threats and vulnerabilities. Directly involving key stakeholders engaged in the SME's operations is essential for a precise and efficient identification process. Establishing continuous monitoring and feedback mechanisms is vital to adapt to the dynamic

nature of information security risks in the SME context. Regular reviews and updates to the risk identification process empower SMEs to remain vigilant and responsive to emerging threats within the confines of their operational constraints.

#### 3.1.3. Risk Analysis for SMEs According to ISO 27005/2022

In the context of SMEs adhering to ISO/IEC 27005:2022 for information security risk management, risk analysis is a crucial step tailored to the specific constraints of SMEs. SMEs should systematically evaluate the identified risks by considering the likelihood of occurrence and the potential impact on their information assets. Given resource limitations, a pragmatic and focused approach is essential, prioritizing risks based on their significance to the organization. SMEs should use an appropriate risk analysis methodology that aligns with their operational scale and complexity. Involving key stakeholders intimately familiar with the organization's processes and systems ensures a more accurate and relevant analysis. The output of this analysis guides decision-making on risk treatment strategies, allowing SMEs to allocate their resources effectively and manage information security risks in a manner commensurate with their unique business context. Regular reviews and adjustments to the risk analysis process enable SMEs to adapt to changing circumstances and maintain an effective risk management posture.

#### 3.1.4. Risk Evaluation for SMEs According to ISO 27005/2022

In line with ISO/IEC 27005:2022 for information security risk management, SMEs undertake risk evaluation as a pivotal step customized to their specific circumstances. This process involves assessing the significance of identified risks in terms of their potential impact on the confidentiality, integrity, and availability of information assets within the SME. Considering the constraints typically faced by SMEs, such as limited resources, a focused and pragmatic approach is crucial. The evaluation encompasses determining the risk levels by weighing the likelihood of occurrence against the potential consequences. SMEs should leverage risk criteria established in the earlier stages of the risk management process, aligning them with the organization's risk appetite. This tailored risk evaluation enables SMEs to prioritize and address the most critical information security risks within their operational capacity. Regular reviews ensure the continued relevance of risk assessments in the dynamic landscape of SMEs, fostering a resilient approach to safeguarding information assets.

#### 3.1.5. Risk Treatment for SMEs According to ISO 27005/2022

In accordance with ISO/IEC 27005:2022 guidelines for information security risk management, SMEs engage in risk treatment as a strategic response to identified risks. This involves selecting and implementing appropriate measures to address, mitigate, transfer, or accept the risks based on the outcomes of risk evaluation (**Figure 3**). Given the resource constraints typically encountered by SMEs, a practical and cost-effective approach to risk treatment is essential. SMEs should prioritize actions that align with their risk appetite, aiming to reduce the impact and likelihood of significant risks within the limitations of their operational capacity.

This might involve implementing security controls, enhancing employee awareness, or considering risk transfer mechanisms such as insurance. The effectiveness of risk treatment measures should be monitored and reassessed regularly to adapt to changes in the threat landscape or the organization's internal environment. This dynamic approach enables SMEs to manage information security risks effectively while optimizing the use of available resources.

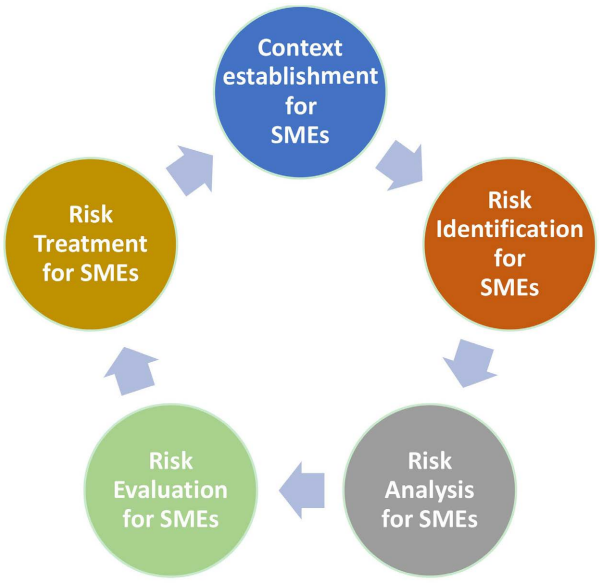


**Figure 3.** Information security risk management process for SMEs according to ISO 27005/2022.

### 3.1.6. Documentation

To enhance efficiency and accessibility in documenting risk management activities and decisions, streamlined procedures should be established. These procedures will ensure clarity and ease of access for stakeholders involved. A centralized repository should also be implemented serving as a unified hub for all risk-related documents. This repository will facilitate seamless storage and retrieval of essential information contributing to a more organized and cohesive approach to risk management.

Moreover, recognizing the distinct characteristics of SMEs, a tailored risk management strategy is strongly encouraged to be developed. This strategy will be practical and adaptable, aligning closely with the specific needs and challenges faced by SMEs. By customizing the approach SMEs can bolster their resilience, safeguard their assets and ultimately contribute to their long-term sustainability and success in a dynamic business environment.

## 3.2. Risk Management Methodologies and Frameworks for SMEs

Various established methodologies exist for organizations seeking to formalize risk management. Entities opt for a particular standard or framework based on diverse factors. These include compliance obligations, such as regulatory or contractual

mandates, alignment with the organization's information risk program or overall business objectives, or a preference for leveraging an established standard process rather than developing one internally.

#### 3.2.1. ISO/IEC 27005:2022 International Standard for Information Security, Cybersecurity and Privacy Protection

ISO/IEC 27005:2022 is an international standard that defines a structured approach to risk assessments and risk management.

ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection. Information Security Management Systems Requirements [29] recommends that organizations and enterprises must establish a risk management process that is appropriate for their context, implement controls to mitigate identified risk and continually monitor and review the effectiveness of these controls.

ISO 27005 is part of the ISO 27000 family of standards, created by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It helps organizations and enterprises to create, monitor, and continually improve an Information Security Management System (ISMS). ISO 27005 focuses specifically on information security risk management. The international standard provides an organized, systematic approach to identifying, assessing, and managing risks related to information security. In October 2022, ISO published an updated version of the standard: ISO 27005:2022. This update replaces the previous version, ISO 27005:2018.

#### 3.2.2. NIST Standards

The National Institute of Standards and Technology (NIST) is responsible for creating standards pertaining to various fields including information security. One such standard, NIST Special Publication (SP) 800-39, outlines the overarching process for managing information security risks by considering the organization's mission and the system's perspective. Additionally, NIST SP 800-30, titled "Guide for Conducting Risk Assessments," offers a comprehensive and thorough framework for conducting risk assessments, providing detailed steps to follow.

- NIST SP 800-39: The methodology described in NIST SP 800-39 consists of multilevel risk management, at the information systems level, at the mission/business process level, and at the overall organization level. Communications up and down these levels ensure that risks are communicated upward for overall awareness, while risk awareness and risk decisions are communicated downward for overall awareness.
- NIST SP 800-30: NIST SP 800-30 provides an in-depth framework for conducting risk assessments, offering structured techniques for the process. It entails creating worksheets to systematically document threats, vulnerabilities, and their respective probabilities of occurrence and potential impacts.
- RMF: The Risk Management Framework (RMF) is a structured process that helps organizations identify, assess, and prioritize risks to their information systems and data [30].

#### 3.2.3. Factor Analysis of Information Risk (FAIR)

Factor Analysis of Information Risk (FAIR) is an analytical approach aiding risk managers in comprehending the elements influencing risk, the likelihood of threat occurrences, and estimating potential losses.

This framework comprises Loss Event Frequency (LEF) and Probable Loss Magnitude (PLM). It can be executed by utilizing data gathered through the ISO/IEC 27005 communication framework. Loss Event Frequency takes into account Threat Event Frequency (TEF) and Vulnerability (Vuln). Meanwhile, Probable Loss Magnitude considers both Primary and Secondary Loss Factors [31].

#### 3.2.4. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) for Small and Medium Businesses

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a risk analysis methodology created by Carnegie Mellon University. The most recent iteration, OCTAVE Allegro, is utilized to evaluate privacy and security risks, enabling organizations to derive meaningful insights from their risk assessments.

The Software Engineering Institute's Networked Systems Survivability (NSS) Program created the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) framework to outline a method for assessing information security risks. OCTAVE guides organizations through a series of steps to help them identify and address their security risks effectively. By adhering to the OCTAVE framework, organizations can conduct thorough evaluations that enable them to recognize the critical information assets relevant to their objectives, identify potential threats to those assets, and pinpoint vulnerabilities that could compromise their security [32]-[35].

## 4. Cybersecurity Measurements and Controls for SMEs

### 4.1. Employee Training/Education

As highlighted in the Social Engineering section, the human element emerges as the most vulnerable link, constituting a primary threat within the realm of cybersecurity. By recognizing this factor, it becomes essential for companies of all scales (micro, small or medium-sized) to employ comprehensive education and training for each employee, encompassing various aspects of cybersecurity and particularly focusing on the features of social engineering techniques.

A range of studies have highlighted the importance of education and training in cybersecurity. Ion *et al.* [36] emphasize the need for a comprehensive approach to cybersecurity education, covering both theoretical and practical aspects. Kweon [37] provides empirical evidence of the effectiveness of security training in reducing the number of cybersecurity incidents in organizations. He *et al.* [38] further explore the impact of different training methods on employees' cybersecurity risk perception and behavior, with evidence-based malware reports being identified as particularly effective. Finally, Caulkins *et al.* [39] underscores the importance of a human-centric approach in cybersecurity education, with a focus on the National Cybersecurity Workforce Framework and the Department of Homeland Security's

educational framework. These studies collectively highlight the need for ongoing, comprehensive and human-centric education and training in cybersecurity.

To facilitate this crucial undertaking, we formed a guide outlining essential steps for effective employee training and education in the realm of cybersecurity:

1) Identify Threats: employees should participate in ongoing workshops dedicated to cybersecurity threats and potential vulnerabilities, with a particular emphasis on social engineering. Moreover, employees should undergo regular phishing simulations to familiarize themselves with common phishing techniques. This training aims to enable them to identify various tactics employed by attackers, such as phishing, pretexting and baiting.

2) Training modules: Every enterprise is encouraged to develop training modules that are specified to every organization's needs and the potential threats they may encounter. This ensures that employees can relate the training to their daily work.

3) Interactive learning: Enterprises are also encouraged to incorporate interactive elements such as simulations and real-life scenarios to enhance engagement. This helps employees grasp the practical aspects of cyber threats.

4) Basic cybersecurity awareness/education: Each member of a company's workforce should possess a fundamental understanding of essential cybersecurity principles. Specifically, employees must understand the importance of strong, unique passwords and the practice of regularly updating them. Moreover, they should be able to identify suspicious emails, avoid clicking on unknown links and report any phishing attempts. Finally, every enterprise should be educated on the significance of keeping software and devices up-to-date to address potential vulnerabilities.

5) Areas of authorized access: It is of high importance for every company to establish areas of authorized access. In many instances, employees are granted access to sections of the company beyond their designated departments. It is imperative that each staff member is limited to accessing only their specific department to prevent any potential data corruption or theft, whether intentional or unintentional.

6) Encourage Reporting: It is strongly recommended that enterprises should establish a policy where employees ought to report any suspicious activity through dedicated channels for reporting incidents. This policy should stress the need for employees to have a fundamental understanding of the importance of reporting promptly.

7) Cyber Security Gamification Training: A range of studies have explored the use of gamification in cybersecurity training with positive results. Coull [40] developed virtual escape rooms and games to improve user engagement and knowledge acquisition. Similarly, Gonzalez [41] and Steen [42] found that gamification can enhance the learning process and improve attitudes, perceived behavioral control, intentions and behavior. Malone [43] and Rieff [44] further demonstrated the effectiveness of gamified learning platforms and a framework for gamifying cybersecurity awareness training. Jelo [45] and Ashley [46] extended this

work to the field of critical infrastructure, using gamified scenarios and game-based learning to train facility operators in cybersecurity.

### 4.2. Antimalware Software

Antimalware software (also known as antivirus software) is a specialized software designed to detect, prevent and remove malicious software (malware) from computer systems and networks. Malware encompasses a broad category of harmful software, including viruses, worms, trojans, ransomware, spyware and other types of malicious code. Antimalware software employs several key mechanisms. One primary method is signature-based detection, where the software maintains a database of known malware signatures-distinctive patterns or characteristics associated with specific malicious entities. During routine scans or file access events, the software compares these signatures while flagging files that exhibit a match for further investigation. Additionally, antimalware software employs real-time monitoring of the activities of programs and processes and suspicious behavior patterns, such as deviations from normal operations or actions consistent with malware, trigger alerts or further examination. Finally, antimalware runs sets of algorithms in an effort to identify new kinds of malware based on behavioral attributes or code structures [47] [48].

In order to secure cybersecurity defenses, enterprises should always prioritize the adoption and utilization of authentic, up-to-date antimalware software solutions. The critical importance of this practice derives from the dynamic and evolving nature of cyber threats that businesses face daily. By employing original antimalware software, organizations can fortify their digital infrastructure against malicious actors seeking to exploit vulnerabilities and compromise sensitive information.

### 4.3. Updated and Original Software in SMEs

Micro, small, and medium-sized companies cannot compete with big enterprises that have enough funds dedicated to cybersecurity. It has been observed that many companies, in an effort to cut costs, choose not to invest in authentic software. Furthermore, there is a tendency to overlook the importance of updating existing software on multiple occasions.

The choice of original software ensures that your business leverages security protocols designed and endorsed by the software's legitimate developers. These protocols are crafted to address emerging threats, providing a robust shield against evolving cybersecurity challenges. On the other hand, the commitment of software developers extends beyond the initial purchase. Choosing original software guarantees continuous updates and patches, fortifying your systems against vulnerabilities that may arise over time. This proactive approach is instrumental in minimizing potential risks [49]-[51].

Malicious exploitation typically occurs when hackers identify outdated and pirated software. In many instances, these hackers target vulnerabilities that have

already been widely exploited and shared or sold on the darknet.

### 4.4. Network-Attached Storage (NAS) Server

A Network-Attached Storage (NAS) server is a specialized device or software that provides centralized storage and file-sharing capabilities to multiple users and devices within a network. Unlike a traditional server, a NAS is specifically designed for storage-related tasks and is often a dedicated device with integrated storage drives. As businesses increasingly adopt remote work practices, NAS servers often provide secure remote access capabilities. This allows authorized personnel to access critical business data securely from different locations, with proper encryption and authentication measures in place. The importance of a NAS server for security in an SME lies in several key aspects [52] [53]:

1) Data Centralization: NAS allows for the centralization of data storage, meaning that important files and data are stored in one secure location. This reduces the risk of data loss and minimizes the risk of data theft and ransomware attacks.

2) Access Control: NAS devices often come with access control features. This means administrators can regulate and restrict access to sensitive data, ensuring that only authorized personnel can view, modify or delete specific files or directories. This helps prevent unauthorized access and potential data breaches.

3) Data Encryption: A NAS server can offer encryption features to secure data during transmission and while at storage. Encryption is crucial for protecting sensitive information from interception during data transfer or in the event of unauthorized physical access to the storage device. Data encryption is also essential for a company in order to be compliant with data protection law like the General Data Protection Regulation (EU GDPR).

4) Backup and Redundancy: NAS servers commonly support automated backup processes, creating regular copies of data. This procedure is crucial for data recovery in case of accidental deletion, hardware failure, etc. Having a reliable backup strategy enhances data security by ensuring data integrity and availability. Finally, regular backup offers protection against malware and ransomware attacks.

5) Virus and Malware Protection: NAS servers usually come with built-in antivirus and anti-malware features. These security measures add an extra layer of protection against cyberattacks.

### 4.5. Website Security & Protection

In the business landscape, every enterprise depends on a website as a means to promote and communicate its activities to the public. Depending on the nature of the enterprise, a website serves not only as an informational platform but also as a tool for various functions including e-commerce, warehouse management, commercial operations, logistics, work distribution and more.

A website is composed of its domain, which is the name identifying the site, and the platform built using various programming languages such as PHP (Hypertext Preprocessor), CSS (Cascading Style Sheets), SQL (Structured Query Language),

JavaScript, Python and others. Additionally, it incorporates plugins, which are programs providing diverse functions on a website, such as managing cookie policies, facilitating e-commerce transactions, implementing CAPTCHA and more.

The protection of a domain is a critical aspect of cybersecurity as it is a crucial component of a company's online brand identity and unauthorized access or control over a domain can lead to the misuse of a brand's reputation through fraudulent activities or misleading content. Furthermore, domains are often linked to various online services, including email and website hosting. Compromised domains can serve as entry points for cybercriminals to access sensitive data, leading to data breaches and other security incidents. Cybercriminals frequently employ domain spoofing in phishing attacks to deceive users, and thus, protecting a domain helps prevent the creation of websites with similar names, reducing the risk of falling victim to phishing schemes. For many businesses, a domain represents intellectual property. Protecting the domain helps safeguard trademarks, brand names and other proprietary information from being exploited by malicious actors [54].

Moreover, the necessity of regularly updating plugins and programming languages on a website is also critical for cybersecurity. Websites serve as vital interfaces for businesses and individuals, facilitating various online activities and for that reason, plugins, which are additional software components that enhance a website's functionality, play a crucial role in extending features such as e-commerce capabilities, interactive forms and multimedia integration. Regular updates to these plugins are essential as developers often release patches to address security vulnerabilities. Failing to update plugins promptly can expose the website to exploitation by malicious actors seeking to exploit known weaknesses [55]-[57]. Similarly, the programming language used to build a website requires regular updates to address security vulnerabilities and improve overall performance. Outdated programming languages may contain known vulnerabilities that cybercriminals can exploit to compromise the website's integrity and gain unauthorized access to sensitive data.

In summary, the need to keep plugins and programming languages up-to-date and the need to protect the domain of an enterprise is more than ever essential for cybersecurity. Cybercriminals actively exploit vulnerabilities in outdated software, leading to potential compromises of data integrity, injection of malicious code, and disruptions through various attacks.

### 4.6. Clean Desk and Clear Screen Policy of SMEs

Clear guidelines for the management of papers and removable storage media, as well as rules for maintaining clear screens in information processing facilities, are essential for SMEs. The organization should formulate and communicate a specific policy regarding clear desks and screens to all relevant parties involved. In this way, unauthorized access and physical social engineering risk is minimized [58]. More specifically, these guidelines should:

1) Safely storing sensitive or crucial business information, whether in print or electronic format, in a secure location such as a safe, cabinet, or other secure furniture when not in use, especially when the office is empty.

2) Implementing security measures such as key locks to protect user endpoint devices when not in use or left unattended.

3) Ensuring that user endpoint devices are either logged off or secured with a screen and keyboard lock, controlled by a user authentication mechanism when not attended. All computers and systems should be configured with a timeout or automatic logout feature.

4) Print using machines with authentication features so that only the individuals who ordered the print can retrieve their printouts and only when physically present at the printer.

5) Store in a secure way the documents and removable storage media containing sensitive information. Properly dispose of them using secure disposal methods when no longer needed.

6) Establish and communicate rules and guidance for screen pop-ups, such as turning off new email and messaging pop-ups during presentations and screen sharing.

7) Clear sensitive or critical information from whiteboards and other displays when no longer necessary.

### 4.7. Information Backup Policy for SMEs

SMEs should uphold a consistent and tested practice of maintaining backup copies of information, software and systems, aligning with a specific policy on backup. This policy should be tailored to meet the organization's data retention and information security needs.

To ensure effective recovery following an incident, failure, or loss of storage media, adequate backup facilities must be provided. Plans outlining how the organization will back up information, software and systems should be developed and put into action, adhering to the established backup policy. When formulating a backup plan, the following factors should be taken into account:

1) Generating accurate records and documented restoration procedures for backup copies.

2) Aligning with business requirements, security standards and the criticality of information in terms of the extent (e.g., full or differential backup) and frequency of backups.

3) Safely storing backups in a remote location, at a sufficient distance to avoid damage from disasters at the main site.

4) Providing an appropriate level of physical and environmental protection for backup information.

5) Regularly testing backup media to ensure their reliability in emergency situations. Testing the restoration process on a separate system without overwriting the original storage media in order to prevent irreparable data damage or loss in

case of failure.

6) Applying encryption to protect backups based on identified risks, especially in situations where confidentiality is crucial.

7) Implementing measures to detect inadvertent data loss before the backup process.

Operational procedures should actively monitor backup execution, addressing any failures in scheduled backups to ensure compliance with the backup policy. Regular testing of backup measures for individual systems and services is essential to meet the objectives of incident response and business continuity plans. Critical systems and services should have comprehensive backup measures covering all necessary system information, applications and data for a complete recovery in the event of a disaster, a data theft or a ransomware attack [59] [60].

### 4.8. Network Security of SMEs

Securing, managing and controlling networks and their devices is crucial for safeguarding information within SMEs systems and applications. To ensure network security and protect connected services from unauthorized access, the following aspects should be considered:

1) Assessing the information types and classification levels supported by the network.

2) Defining responsibilities and procedures for managing networking equipment and devices.

3) Keeping documentation up to date, including network diagrams and configuration files of devices such as routers and switches.

4) Separating operational responsibilities for networks from ICT system operations when necessary.

5) Implementing controls to ensure confidentiality and integrity of data over public, third-party, or wireless networks with additional measures for maintaining network service availability.

6) Logging and monitoring activities to record and detect actions relevant to information security.

7) Coordinating network management activities for consistent control application across the information processing infrastructure.

8) Authenticating systems on the network.

9) Restricting and filtering systems' connection to the network using firewalls.

10) Detecting, restricting and authenticating the connection of equipment and devices to the network.

11) Hardening network devices for increased security.

12) Segregating network administration channels from other network traffic.

13) Temporarily isolating critical subnetworks in case of network attacks.

14) Disabling vulnerable network protocols.

Every enterprise should apply appropriate security controls for virtualized networks, including software-defined networking (SDN, SD-WAN). Virtualized

networks offer security benefits by allowing logical separation of communication over physical networks, especially for systems using distributed computing [61].

Managing the security of large networks can involve dividing them into separate domains, and isolating them from the public network (internet). Domains can be based on trust levels, criticality, sensitivity, organizational units, or a combination thereof. This segregation can be achieved through physically different networks or different logical networks [62].

### 4.9. Use of Cryptography

SMEs should be encouraged to establish and enforce rules for the effective application of cryptography, including cryptographic key management. The objective is to ensure proper and efficient utilization of cryptography, aligning with business and information security requirements while accounting for legal, regulatory and contractual aspects related to cryptography [63]. When employing cryptography, the following factors should be addressed:

1) Development and implementation of an organization-defined policy on cryptography, outlining general principles for information protection. This specific policy is essential to maximize benefits, minimize risks and prevent inappropriate or incorrect cryptographic usage.

2) Determination of the required level of protection and information classification, leading to the specification of the type, strength and quality of cryptographic algorithms needed.

3) Utilization of cryptography for safeguarding information on mobile user endpoint devices, storage media and during transmission over networks to such devices or media.

4) Adoption of an approach to key management, encompassing methods for generating and safeguarding cryptographic keys, along with recovery procedures for encrypted information in case of key loss, compromise or damage.

5) Assignment of roles and responsibilities for implementing effective cryptography rules and key management, including key generation.

6) Adoption of standards, cryptographic algorithms, cipher strength and cryptographic solutions in line with organizational approvals or requirements.

7) Evaluation of the impact of using encrypted information on controls dependent on content inspection such as malware detection or content filtering.

During the implementation of the organization's cryptography rules, it's crucial to consider applicable regulations, national restrictions on cryptographic techniques worldwide and address issues related to the trans-border flow of encrypted information.

### 4.10. Use of Artificial Intelligence (AI)

Artificial intelligence (AI) has emerged as a critical tool in enhancing cybersecurity for enterprises, particularly in the face of increasing cyber threats and the limitations of traditional security systems. AI components such as machine learning, data mining, in-depth learning and expert programs have been identified as key

areas for improving cybersecurity. The use of AI in cybersecurity has been found to offer several benefits, including improved threat detection and response, as well as the ability to counter the evolving tactics of cyber attackers. However, it is important to note that the increasing volume and complexity of cyber-attacks require continuous advancements in AI. Despite the potential of AI in cybersecurity, there are also challenges such as the need for intelligent cybersecurity measures and the potential misuse of AI by cybercriminals. Overall, AI has the potential to significantly enhance cybersecurity capabilities for enterprises, particularly in the areas of threat detection, response and defense mechanisms [64].

The main fields that AI can help enterprises in the area of cybersecurity are:

• Advanced Threat Detection: AI-powered systems can analyze vast amounts of data at an unprecedented speed, enabling them to identify patterns and anomalies that might indicate a security threat. Unlike traditional systems, which rely on known threat signatures, AI algorithms can learn from data, allowing them to detect new and evolving threats. This proactive approach to threat detection ensures that enterprises can respond to attacks more swiftly and effectively.

• Automated Response to Incidents: Once a threat is detected, the speed of response is crucial. AI can automate certain response protocols, immediately isolating infected systems or blocking malicious activities. This not only reduces the window of opportunity for attackers but also alleviates the burden on human security teams, allowing them to focus on more strategic tasks.

• Predictive Analytics: By leveraging machine learning models, AI can predict potential vulnerabilities and threat vectors by analyzing historical data and current trends. This predictive capability enables enterprises to fortify their defenses before an attack occurs, shifting from a reactive to a proactive cybersecurity posture.

• Enhanced Risk Management: AI helps in quantifying and prioritizing risks based on the likelihood and potential impact of threats. This prioritization allows enterprises to allocate their resources more effectively, focusing their efforts on areas of highest risk.

• Phishing Detection and Prevention: Phishing attacks are a common and effective tactic used by cybercriminals. AI can analyze emails and web content in real-time to detect phishing attempts, identifying malicious links and attachments or unusual sender behavior. This significantly reduces the chances of employees inadvertently compromising enterprise security.

• Behavioral Analysis: AI systems can monitor user behavior within an organization's network, learning normal patterns of behavior and flagging deviations that could indicate insider threats or compromised accounts. This level of behavioral analysis goes beyond simple access controls and into the nuanced detection of potential security breaches.

• Streamlining Compliance: AI can also assist enterprises in maintaining compliance with various regulatory requirements. By automating data protection protocols and monitoring compliance in real time, AI reduces the risk of costly violations and ensures that sensitive information remains secure.

### 4.11. Best Security Practices for Remote Work

The organization/business must establish and support specific procedures for teleworking. These procedures should consider the nature and severity of risks regarding the protection of personal data arising from remote work.

The organization should adequately inform, train, and assist employees in implementing these procedures, considering that many users may not be familiar with the technologies supporting telecommuting and related risks. The following best security practices should be implemented for remote work:

• Ensure there is no possibility of insecure remote access to the organization's IT resources, such as internal network computers and files. Secure connection can be achieved, for example, through a Virtual Private Network (VPN) with data encryption and user authentication (e.g., IPSec VPN).

• Define and limit access to resources remotely based on the necessary tasks performed by the telecommuter.

• Connect to the organization's computing systems through a Remote Desktop Protocol (RDP) service only via a secure VPN.

• Use secure WPA2 protocol with a strong password for Wi-Fi connections, even when connecting to the organization's network securely via VPN.

• Avoid storing files with personal data on online storage services (e.g., Dropbox, OneDrive, Google Drive) unless adequate guarantees are provided, such as services provided by the organization with appropriate security measures, or data stored exclusively in appropriately encrypted format.

• Install and regularly update antivirus software and firewall on the device used for telecommuting.

• Ensure the latest software and operating system updates are installed on employees' devices.

• Use up-to-date web browsers (e.g., Firefox, Chrome) and clear browsing history or delete links related to telecommuting at the end of the work session.

• Separate files containing personal data related to work from personal files on the employee's device, using distinct folders with descriptive names. Use a virtual machine exclusively for telecommuting where possible.

• Support appropriate encryption procedures for files containing personal data, especially when stored on portable/removable storage media (e.g., USB stick). Consider encrypting files on the primary device used for telecommuting (e.g., PC, laptop), especially for high-risk data.

• For teleconferencing, the utilization of platforms supporting secure services (encryption) and avoiding teleconferencing software that does not provide end-to-end encryption is of the essence.

### 4.12. Physical & Environmental Security of SMEs

Appropriate measures must be taken to protect buildings, critical areas, computer rooms, staff offices, IT equipment and physical file storage spaces from damages that may result from natural disasters or malicious actions, such as floods, overheating,

fire, earthquakes, explosions, water leaks, power outages, burglary/theft, vandalism, etc.

Indicative measures in this direction include alarms, security doors and windows, fire protection systems, relocating equipment away from water pipes and dust sources, moisture and flood detectors, uninterrupted power supply through stabilizers/generators, etc.

### 4.13. Security and Resilience—Business Continuity Management

The organization must have developed documented policies and implementation procedures concerning ensuring business continuity and recovery from the disruption of critical information systems following an adverse event. In this context, it should have identified its critical systems and functions and conducted an impact assessment of potential adverse events (cyberattacks, natural disasters, etc.).

The organization should have developed and documented a detailed business continuity plan aiming at the immediate restoration and continuity of critical functions and services following an adverse event.

For the above process, it may be certified to apply, maintain, and improve a management system based on which it prepares, responds, and recovers critical functions and continues to provide products and services at an acceptable level in the event of an adverse event. Such an international standard is ISO 22301:2019 Security and Resilience.

### 4.14. Tailoring Cybersecurity Measures Based on Budget Constraints

Cybersecurity is a critical concern for all organizations, irrespective of their size. For small and medium-sized enterprises (SMEs), implementing robust cybersecurity measures is essential to protect against a variety of threats. This unified approach addresses several key areas of cybersecurity relevant to SMEs, including employee training, antimalware software, software updates, network-attached storage (NAS) security, website protection and more, but the implementation may vary based on the size, budget and resources of each SME.

Employee training and education form the cornerstone of an effective cybersecurity strategy. SMEs must invest in comprehensive training programs to educate employees about various cyber threats, including phishing and social engineering tactics. Tailored training should cover fundamental principles such as the creation of strong passwords, the identification of suspicious emails, and the importance of software updates. For small SMEs, cost-effective training options, such as online courses and phishing simulations, can be utilized, while medium-sized SMEs may benefit from more advanced and interactive training modules. Regular updates and ongoing education ensure that employees stay informed about the latest threats and best practices.

Antimalware software is another critical component of cybersecurity. Both small and medium-sized SMEs need reliable antimalware solutions to detect,

prevent, and remove malicious software. This software should be regularly updated to handle new threats and vulnerabilities. Small SMEs should focus on affordable, reputable antimalware solutions, while medium-sized businesses may invest in more comprehensive, enterprise-grade solutions that offer additional features like real-time threat monitoring and advanced threat analytics.

Updated and original software is crucial for maintaining security. SMEs must ensure that all software, including operating systems and applications, is kept up-to-date with the latest patches and updates to protect against known vulnerabilities. This practice not only prevents exploitation by attackers but also ensures compatibility with other security measures. Small SMEs should prioritize regular software updates as part of their basic security hygiene, while medium-sized enterprises can implement automated update management systems to streamline the process.

Network-attached storage (NAS) servers require particular attention to safeguard critical data. For SMEs, securing NAS involves implementing strong access controls, encrypting stored data, and regularly backing up data to prevent loss from ransomware or other attacks. Small SMEs might opt for basic encryption and access controls, while medium-sized enterprises can integrate advanced features such as centralized management and multi-factor authentication.

Website security and protection are essential for SMEs with an online presence. Implementing SSL/TLS certificates to secure data in transit, along with regular vulnerability assessments and updates, helps protect against common web-based attacks. Small SMEs can start with basic security practices like regular software updates and secure login credentials, while medium-sized businesses might adopt more sophisticated solutions such as Web Application Firewalls (WAFs) and comprehensive security monitoring.

A clean desk and clear screen policy helps mitigate the risk of data breaches and unauthorized access. SMEs should enforce policies requiring employees to lock their screens when away from their desks and clear sensitive information from their workspaces. For small SMEs, simple reminders and basic training can suffice, while medium-sized enterprises might implement more formal procedures and regular audits to ensure compliance.

Information backup policies are vital for data resilience. Regular backups of critical information should be performed and stored securely, ideally offsite or in a cloud environment. Small SMEs can use basic backup solutions, while medium-sized businesses might invest in more sophisticated backup and recovery systems that offer greater reliability and faster recovery times.

Network security is fundamental to protect against unauthorized access and data breaches. SMEs should employ firewalls, intrusion detection systems, and secure network configurations. Small businesses can implement basic firewall solutions and secure Wi-Fi networks, while medium-sized enterprises might deploy more advanced network security measures, including segmented networks and intrusion prevention systems.

The use of cryptography helps secure sensitive data both at rest and in transit. SMEs should leverage encryption to protect data on devices, during transmission, and in storage. Small SMEs can use basic encryption tools and services, while medium-sized businesses might deploy enterprise-grade encryption solutions with advanced features.

Artificial Intelligence (AI) can enhance cybersecurity by providing advanced threat detection and response capabilities. AI-driven tools can analyze vast amounts of data to identify patterns and potential threats that traditional methods might miss. Small SMEs can explore AI solutions that offer essential threat detection and response features, while medium-sized enterprises may integrate more sophisticated AI systems for comprehensive security analysis and automated responses.

Best security practices for remote work** are increasingly relevant as remote work becomes more common. SMEs should establish clear policies for secure remote access, including the use of Virtual Private Networks (VPNs), secure authentication methods, and regular security updates on remote devices. Small SMEs can adopt basic remote work security measures, while medium-sized enterprises might implement more robust solutions, such as centralized endpoint management and advanced threat detection for remote work environments.

Physical and environmental security ensures that physical access to sensitive areas and equipment is controlled. SMEs should implement access controls, surveillance, and environmental monitoring to protect against physical threats. Small businesses can focus on basic physical security measures, such as locked doors and restricted access, while medium-sized enterprises might invest in more advanced systems, including biometric access controls and comprehensive surveillance systems.

Finally, security and resilience through business continuity management are critical for maintaining operations during and after a cyber incident. SMEs should develop and regularly test business continuity plans to ensure rapid recovery from disruptions. Small SMEs can start with basic continuity planning and testing, while medium-sized businesses might adopt more detailed and formalized plans, including comprehensive risk assessments and recovery strategies.

By addressing these key areas, SMEs can build a robust cybersecurity framework that mitigates risks and ensures resilience against various cyber threats.

## 5. Information Security and Cybersecurity Frameworks for SMEs

Although each organization possesses distinct missions, objectives and risk tolerances, they are not required to develop governance frameworks independently to address security and privacy goals. Some organizations may already possess appropriate control frameworks, while others may not. While opting for an industry-standard control framework is not obligatory, it offers advantages. These frameworks have a track record of implementation across numerous companies and undergo regular updates to adapt to evolving business landscapes, emerging

threats, and technological advancements.

### 5.1. ISO/IEC 27001:2022, Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems

There are several standard security and privacy frameworks, but ISO/IEC 27001:2022 is of the most importance. More specifically:

1) ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection—Information security management systems—Requirements, is the world's best-known standard for information security management systems (ISMS) and defines requirements an ISMS must meet. This standard contains a requirements section that outlines a properly functioning information security management system (ISMS) and a comprehensive control framework.

2) ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection—Information security controls standard is a collection of information security management guidelines that are intended to help an organization implement, maintain and improve its information security management system (ISMS). The standard is published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

3) ISO 27002 is designed to work with ISO 27001 as a code of practice, which provides the requirements for establishing, implementing, maintaining and improving an ISMS. ISO 27002 provides guidelines, general principles and control mechanisms for implementing, maintaining and improving information security management in an organization.

### 5.2. NIST Standards & Cybersecurity Frameworks

NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations: is one of the most well-known and adopted security control frameworks. NIST SP 800-53 many organizations that are not required to employ the framework have utilized it, primarily because it is a high-quality control framework with in-depth implementation guidance and because it is available without cost.

NIST SP 800-53A, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans: is the companion standard to NIST SP800-53 that defines techniques for auditing or assessing each control in NIST SP 800-53.

NIST Cybersecurity Framework (CSF) 2.0: NIST Cybersecurity Framework 2.0: is the latest revision (released in February 2024 in a set of procedures and guidelines developed to help organizations improve cybersecurity measures. The NIST Cybersecurity Framework (CSF) 2.0 provides guidance to industry, government agencies, and other organizations to manage cybersecurity risks. It offers a taxonomy of high-level cybersecurity outcomes that can be used by any organization—regardless of its size, sector, or maturity—to better understand, assess, prioritize,

and communicate its cybersecurity efforts.

### 5.3. ISO/IEC 27701:2019 Security Techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management—Requirements and Guidelines

ISO/IEC 27701:2019, Security techniques—Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management—Requirements and guidelines is an international standard that directs the formation and management of a Privacy Information Management System (PIMS), including the controls and processes to ensure privacy by design and proper ongoing monitoring and management of personal information. The first version of this standard was published in August 2019.

### 5.4. CIS Critical Security Controls (CIS Controls)

The CIS Critical Security Controls (CIS Controls) offer a straightforward and prioritized set of best practices for enhancing cybersecurity resilience. These controls are widely utilized by cybersecurity professionals globally, with contributions from a diverse community.

They serve as safeguards against common cyber-attacks, often referred to as the "SANS 20 Critical Security Controls."

### 5.5. Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is an internationally recognized information security standard mandated by major credit card brands and administered by the Payment Card Industry Security Standards Council. It provides a control framework specifically designed to safeguard credit card information during storage, processing, and transmission across organizational networks. Compliance with PCI DSS is compulsory for entities handling credit card data, with larger volume organizations subject to annual onsite audits. Many organizations extend PCI DSS principles to protect various types of financial and personal data beyond credit card information.

## 6. Proposed Tool for Initial Cybersecurity Assessment for SMEs

As described before, cybersecurity is paramount for organizations of all sizes, but small and medium-sized enterprises (SMEs) often face unique challenges due to limited resources and expertise. To address these challenges, we have developed a Java-based tool designed to provide an initial cybersecurity evaluation for SMEs based on the measurements and policies described in earlier chapters. This tool employs a 30-question questionnaire (Appendix A) aimed at assessing the cybersecurity posture of SMEs and identifying areas for improvement. The tool can be accessed and downloaded in the following Github repository: https://github.com/ZoirosN/SMEs-Questonnaire. More specifically, the above-

mentioned tool focuses on the following areas:

• Comprehensive Policy and Procedures Assessment: The tool begins by evaluating the organization's documentation and implementation of policies and procedures. It examines whether the organization has established appropriate policies for staff training and awareness of information security and cybersecurity issues. By ensuring regular and role-specific cybersecurity awareness training, the tool helps organizations cultivate a culture of security.

• Malware Protection and Management: A significant portion of the questionnaire focuses on the organization's defenses against malware. It checks if the organization uses centrally managed, regularly updated anti-malware software on all workstations and servers. Additionally, it assesses the implementation of automatic malware scans on portable storage devices, ensuring these entry points are not neglected.

• Network Security and Configuration: The tool scrutinizes the organization's network security policies, including the secure configuration of equipment, operating systems and applications. It checks for adherence to internationally accepted standards and guidelines and evaluates whether the organization uses the latest versions of critical applications. Network segmentation and traffic filtering are also reviewed to ensure sensitive areas are adequately protected.

• Data Backup and Encryption: Ensuring data integrity and availability is critical. The questionnaire investigates the organization's backup policies and procedures, including prioritization, data criticality, and retention requirements. It ensures that backups are automated, encrypted during transit, and subject to periodic integrity checks and restoration tests. Additionally, the tool evaluates the use of cryptography to protect sensitive data both in transit and at rest.

• Physical Security and Access Control: The tool also addresses the physical security of the premises hosting the organization's information systems. It checks for control mechanisms at the external perimeter of the computer room, such as barriers, locks, and alarms, to prevent unauthorized physical access. The maintenance of a list of authorized individuals with access to these areas is also evaluated.

• Regular Reviews and Updates: To maintain a cybersecurity posture, the tool ensures that the organization has mechanisms to regularly review and update user access to systems and data. This helps prevent unauthorized access and ensures that only authorized personnel can access critical systems and information.

Navigating the program, the user answers the questionnaire step-by-step. If a response is negative, the program provides an explanatory message detailing the importance of the measure and the necessary actions to address it. At the end of the questionnaire, a score is displayed on the screen, categorized into success rates: 0% - 20%, 21% - 40%, 41% - 60%, 61% - 80%, and 81% - 100%. Additionally, upon completing the questionnaire, a comprehensive report is generated, evaluating the SME's cybersecurity level and offering general recommendations for improvements and further technical measures.

The selection of the 30 questions for the proposed Java-based cybersecurity

assessment tool was guided by a thorough analysis of well-established information security and cybersecurity frameworks, as detailed in Section 6. These questions were carefully chosen to align with the Basic Controls of Information Security and adhere to widely recognized standards such as ISO/IEC 27001:2022, the NIST Cybersecurity Framework, and ISO/IEC 27701:2019, among others. By drawing from these internationally accepted frameworks, the questions are designed to assess key areas of cybersecurity posture, including policy development, risk management, data protection and incident response. This approach ensures that the tool provides a comprehensive evaluation based on industry best practices, allowing SMEs to benchmark their security measures against globally recognized standards.

Our Java-based evaluation tool is a vital and free resource for SMEs looking to assess and enhance their cybersecurity measures. By covering a wide range of essential areas—from staff training and malware protection to data encryption and physical security—the tool provides a detailed and actionable assessment. This enables SMEs to identify vulnerabilities, strengthen their defenses, and ensure the security of their information systems. With this tool, SMEs can take proactive steps to safeguard their digital assets, protect sensitive data and maintain trust with their stakeholders.

## 7. Discussion and Limitations

The study employs a stratified sampling method aimed at ensuring representativeness across different types of SMEs. SMEs are highly diverse, ranging from micro-enterprises with fewer than 10 employees to medium-sized enterprises with up to 250 employees. This broad range is reflected in the participant pool, which was stratified based on the classification outlined by the European Union's SME definition (as presented in Table 1 of the paper). This stratification ensures that the study captures responses from micro, small, and medium-sized enterprises, thereby addressing the varied cybersecurity needs and challenges across different business sizes. The questionnaire, structured around fundamental cybersecurity standards like ISO/IEC 27001:2022 and the NIST Cybersecurity Framework, allows the tool to adapt its evaluation according to the specific profile and resources of each SME type. By stratifying participants this way, the study can more accurately identify how cybersecurity practices and awareness differ among various SME categories.

In evaluating the results of the study, the tool provided a comparative analysis of the cybersecurity posture of different categories of SMEs.

Among the 10 SMEs that completed the questionnaire, the breakdown of results by size category is as follows:

Micro Enterprises (4 SMEs): Of the 4 micro-enterprises, one scored between 0% - 20%, indicating very limited cybersecurity measures. Two of the micro-enterprises scored between 21% - 40%, showing slightly better preparedness, while the final micro-enterprise scored in the 41% - 60% range, reflecting a moderate

level of cybersecurity implementation.

Small Enterprises (4 SMEs): In the small enterprise category, one business scored between 0% - 20%, demonstrating minimal cybersecurity measures. The other three small enterprises, however, scored within the 41% - 60% range, suggesting a noticeable improvement in their cybersecurity efforts compared to the micro-enterprises.

Medium Enterprises (2 SMEs): Both medium-sized enterprises scored within the 61% - 80% range, indicating a higher level of cybersecurity readiness and more robust implementation of protective measures.

Micro-enterprises generally scored lower on the cybersecurity maturity scale (0% - 20%) due to limited financial and human resources. These businesses often lack formal cybersecurity policies, centralized management of malware protection, and robust backup and encryption strategies. Small enterprises, which typically have some dedicated IT resources, displayed moderate improvement in areas such as malware protection, network security, and data backup, often scoring within the 41% - 60% range. However, they still showed gaps in comprehensive policy implementation and encryption measures. Medium-sized enterprises generally performed better, often scoring in the 61% - 80% range. These organizations were more likely to have established formal cybersecurity policies, invested in encryption technologies, and implemented comprehensive network security configurations. Medium-sized SMEs also demonstrated greater adherence to international cybersecurity standards and a stronger overall cybersecurity posture due to their ability to allocate more resources to cybersecurity. Despite these higher scores, gaps were still observed in areas like regular reviews and updates, especially concerning access control and physical security, indicating room for improvement even among the larger participants.

This comparative analysis underscores the diverse needs and capabilities of SMEs across different sizes and emphasizes the importance of tailored cybersecurity strategies that reflect the specific challenges faced by different types of enterprises.

While our Java-based cybersecurity evaluation tool offers a significant step forward in assisting SMEs with their cybersecurity needs, it does have several limitations that should be acknowledged. Firstly, the tool provides an initial assessment based on a predefined 30-question questionnaire, which, although comprehensive, may not fully capture the security requirements of every SME. This limitation arises from the inherent complexity and variability in cybersecurity needs across different industries and business models. While the tool covers key areas such as policy assessment, malware protection, network security, data backup, encryption, physical security, and access control, it may not address all the unique threats or compliance requirements specific to certain sectors.

Another notable limitation is the tool's reliance on self-reported data. The effectiveness of the assessment largely depends on the accuracy and honesty of the responses provided by users. Given that the tool does not include real-time

validation or auditing capabilities, there is a risk that organizations may overestimate their security posture or underreport their vulnerabilities. This limitation underscores the need for SMEs to complement the tool's findings with more detailed internal audits or external expert evaluations.

Additionally, while the tool provides detailed feedback and recommendations based on user responses, it may not always offer tailored solutions or in-depth technical guidance. The recommendations are designed to be general and applicable to a broad range of SMEs, which means that organizations with more complex or specialized needs might find the advice less actionable. This could be particularly challenging for SMEs in highly regulated industries or those with advanced cybersecurity requirements.

Furthermore, while the tool is designed to be user-friendly and accessible, it may still pose challenges for SMEs with limited technical expertise. The complexity of some cybersecurity concepts and the necessity for periodic reviews and updates might be daunting for users who are not well-versed in the field. This limitation highlights the need for supplementary educational resources or support services to help SMEs effectively interpret and act on the tool's findings.

Lastly, the tool's effectiveness in addressing emerging cybersecurity threats is constrained by its static nature. As the cybersecurity threat landscape evolves, the tool's content and assessment criteria may need to be updated regularly to reflect new threats and best practices. While the tool provides a valuable snapshot of an SME's current security posture, it may not fully account for the dynamic nature of cyber threats and the corresponding need for continuous adaptation.

In conclusion, while our Java-based tool represents a significant advance in providing SMEs with a structured approach to evaluating their cybersecurity measures, it is important to recognize its limitations. The tool serves as a valuable starting point for assessing and improving cybersecurity practices but should be used in conjunction with other resources, expert consultations, and ongoing vigilance to ensure comprehensive and effective security management.

## 8. Conclusions

Small and Medium-sized Enterprises are considered the backbone of the global economy, and for good reason, as they occupy about 90% of businesses and more than 50% of employment worldwide. However, SMEs often lack the necessary resources to address cybersecurity aspects, especially in comparison with large enterprises, which makes them increasingly targeted by cybercriminals.

In this work, we examined key cyber threats such as social engineering, ransomware, malware, BEC attacks, and insider threats to guide SMEs on the multifaceted nature of cybersecurity challenges they may face.

To combat these threats, several measures have been identified as critical, such as implementing comprehensive employee training programs on cybersecurity awareness to counteract social engineering tactics, adopting and regularly updating software to protect against malicious software threats, ensuring timely backups of

critical data to minimize damage from ransomware attacks, applying strict access controls and monitoring to mitigate insider threats, establishing cybersecurity frameworks and standards such as ISO/IEC 27001 and NIST guidelines, and adopting innovative technologies.

Beyond preventative measures, SMEs must develop cyber resilience strategies to ensure business continuity in the event of a cyber incident. This involves planning for incident response, recovery, and adaptation in the face of evolving cyber threats. Ultimately, fostering a culture of cybersecurity within SMEs, focused on education, compliance, and resilience, is essential for safeguarding their future and, by extension, the global economy.

We proposed a comprehensive cybersecurity questionnaire intended to provide SMEs with a valuable tool to assess and enhance their cybersecurity level. The questionnaire is designed to guide users through critical areas such as social engineering, antimalware strategies, data management, and insider threat prevention. The detailed feedback and scoring system aim to highlight areas of strength, identify vulnerabilities, and provide actionable recommendations for improvement. By aligning with globally recognized guidelines like ISO/IEC 27001 and NIST standards, the tool offers a structured and scalable approach to cybersecurity that is both practical and effective.

However, it is important to note that the effectiveness of the questionnaire is currently based on its design principles and theoretical alignment with established standards. Its real-world efficacy has yet to be validated through empirical research. As such, while the tool provides a valuable first look at potential vulnerabilities and strengths, SMEs are encouraged to consult with a cybersecurity task force for a more in-depth analysis and tailored solutions.

In future work, we plan to integrate an AI module that can deliver real-time updates and responses, tailoring its recommendations to the specific cybersecurity needs of each company. This enhancement will enable SMEs to receive continuous, customized guidance, helping them to strengthen their defenses against evolving cyber threats. Additionally, we aim to collect feedback and gather statistical data from SMEs that utilize the questionnaire. This data will be crucial for refining the tool, providing improvements based on real-world usage, and enabling a comprehensive statistical analysis of cybersecurity trends and challenges within the SME sector.

## Author Contributions

Conceptualization, A.P. and G.L.; writing—original draft preparation, A.P. and G.L.; writing—review and editing, A.P., G.L., A.K., V.L., and E.G.; supervision V.L. and E.G. All authors have read and agreed to the published version of the manuscript.

## Data Availability Statement

Data sharing is not applicable.

## Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

## References


[1] World Bank (2024) Small and Medium Enterprises (SMEs) Finance. https://www.worldbank.org/en/topic/smefinance

[2] European Commission (2024) SME Definition. https://single-market-economy.ec.europa.eu/smes/sme-definition_en

[3] IBM (2024) IBM Cost of a Data Breach Report. https://www.ibm.com/reports/data-breach

[4] Chaudhary, S., Gkioulos, V. and Katsikas, S. (2023) A Quest for Research and Knowledge Gaps in Cybersecurity Awareness for Small and Medium-Sized Enterprises. *Computer Science Review*, **50**, Article ID: 100592. https://doi.org/10.1016/j.cosrev.2023.100592

[5] Erdogan, G., Halvorsrud, R., Boletsis, C., Tverdal, S. and Pickering, J. (2023) Cybersecurity Awareness and Capacities of SMEs. *Proceedings of the 9th International Conference on Information Systems Security and Privacy*, Lisbon, 2003, 296-304. https://doi.org/10.5220/0011609600003405

[6] Junior, C.R., Becker, I. and Johnson, S. (2023) Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity. arXiv: 2309.17186.

[7] Wilson, M., McDonald, S., Button, D. and McGarry, K. (2022) It Won't Happen to Me: Surveying SME Attitudes to Cyber-security. *Journal of Computer Information Systems*, **63**, 397-409. https://doi.org/10.1080/08874417.2022.2067791

[8] Alahmari, A. and Duncan, B. (2020) Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. 2020 *International Conference on Cyber Situational Awareness, Data Analytics and Assessment* (*CyberSA*), Dublin, 15-19 June 2020, 1-5. https://doi.org/10.1109/cybersa49311.2020.9139638

[9] Pleshakova, E., Osipov, A., Gataullin, S., Gataullin, T. and Vasilakos, A. (2024) Next Gen Cybersecurity Paradigm Towards Artificial General Intelligence: Russian Market Challenges and Future Global Technological Trends. *Journal of Computer Virology and Hacking Techniques*, **20**, 429-440. https://doi.org/10.1007/s11416-024-00529-x

[10] European Union Agency for Cybersecurity (ENISA) (2024) What Is Social Engineering. https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering

[11] Agazzi, A. (2020) Business Email Compromise (BEC) and Cyberpsychology. https://arxiv.org/abs/2007.02415

[12] Salahdine, F. and Kaabouch, N. (2019) Social Engineering Attacks: A Survey. *Future Internet*, **11**, Article 89. https://doi.org/10.3390/fi11040089

[13] Hadnagy, C. (2018) Social Engineering: The Science of Human Hacking. 2nd Edition, Wiley. https://doi.org/10.1002/9781119433729

[14] Kramer, S. and Bradfield, J.C. (2009) A General Definition of Malware. *Journal in Computer Virology*, **6**, 105-114. https://doi.org/10.1007/s11416-009-0137-1

[15] Saeed, I.A., Selamat, A. and Abuagoub, A.M.A. (2013) A Survey on Malware and Malware Detection Systems. *International Journal of Computer Applications*, **67**, 25-31. https://doi.org/10.5120/11480-7108

[16] (2024) Opentext Cybersecurity. https://www-cdn.webroot.com/8916/9999/2485/Ransomware_Survey_2023_Final.pdf

[17] Aurangzeb, S., Aleem, M., Iqbal, M.A. and Islam, M.A. (2017) Ransomware: A Survey and Trends. *Journal of Information Assurance & Security*, **6**, 48-58.

[18] SOPHOS (2024) The State of Ransomware, 2023. https://www.sophos.com/en-us/content/state-of-ransomware

[19] OBERLO (2024) How Many Emails Are Sent Per Day. https://www.oberlo.com/statistics/how-many-emails-are-sent-per-day

[20] Cyberspace Project (2024) Business Email Compromise BEC Attacks. https://cyberspaceproject.eu/wp-content/uploads/2024/03/CYBERSPACE_T2.3_Topic-15_PN_Business-Email-Compromise-BEC-Attacks.pdf

[21] Papathanasiou, A., Liontos, G., Paparis, G., Liagkou, V. and Glavas, E. (2024) BEC Defender: QR Code-Based Methodology for Prevention of Business Email Compromise (BEC) Attacks. *Sensors*, **24**, Article 1676. https://doi.org/10.3390/s24051676

[22] Cisa.gov (2024) Defining Insider Threats. https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats

[23] Hayden, M.V. (1999) The Insider Threat to US Government Information Systems. National Security Telecommunications and Information Systems Security Committee (NSTISSAM) INFOSEC, 1-99.

[24] Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y. and Ochoa, M. (2019) Insight into Insiders and It: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Counter-Measures. *ACM Computing Surveys*, **52**, 1-40. https://doi.org/10.1145/3303771

[25] Mthiyane, Z.Z.F., van der Poll, H.M. and Tshehla, M.F. (2022) A Framework for Risk Management in Small Medium Enterprises in Developing Countries. *Risks*, **10**, Article 173. https://doi.org/10.3390/risks10090173

[26] ENISA (2024) Risk Management for SMEs. https://www.enisa.europa.eu/topics/risk-management/approaches-for-smes/infosec-smes

[27] The International Organization for Standardization (ISO) (2024) ISO/IEC 27005: 2022 Information Security, Cybersecurity and Privacy Protection. Guidance on Managing Information Security Risks. https://www.iso.org/standard/80585.html

[28] Ferreira de Araújo Lima, P., Crema, M. and Verbano, C. (2020) Risk Management in Smes: A Systematic Literature Review and Future Directions. *European Management Journal*, **38**, 78-94. https://doi.org/10.1016/j.emj.2019.06.005

[29] The International Organization for Standardization (ISO) (2024) ISO/IEC 27001: 2022 Information Security, Cybersecurity and Privacy Protection Information Security Management Systems Requirements. https://www.iso.org/standard/27001

[30] NIST (2024) NIST Special Publication 800-37 Risk Management Framework for Information Systems and Organizations. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

[31] Lee, J.J., Go, M., Kim, Y., Joo, M., Seo, J., Oh, H., *et al.* (2020) A Multi-Component Analysis of CPTED in the Cyberspace Domain. *Sensors*, **20**, Article 3968. https://doi.org/10.3390/s20143968

[32] ENISA (2024) Octave v2.0 (and Octave-S v1.0 for Small and Medium Businesses).

https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_octave.html

[33] Alberts, C.J., Behrens, S.G., Pethia, R.D. and Wilson, W.R. (2024) Operationally Critical Threat, Asset, and Vulnerability Evaluation SM (OCTAVE SM) Framework, Version 1.0. https://insights.sei.cmu.edu/documents/1210/1999_005_001_16769.pdf

[34] Barraza de la Paz, J.V., Rodríguez-Picón, L.A., Morales-Rocha, V. and Torres-Argüelles, S.V. (2023) A Systematic Review of Risk Management Methodologies for Complex Organizations in Industry 4.0 and 5.0. *Systems*, **11**, Article 218. https://doi.org/10.3390/systems11050218

[35] AL-Dosari, K. and Fetais, N. (2023) Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach. *Electronics*, **12**, Article 3629. https://doi.org/10.3390/electronics12173629

[36] Bolun, I., Bulai, R. and Ciorbă, D. (2021) Support of Education in Cybersecurity. *Pro Publico Bono—Magyar Közigazgatás*, **9**, 128-147. https://doi.org/10.32575/ppb.2021.1.8

[37] Kweon, E., Lee, H., Chai, S. and Yoo, K. (2019) The Utility of Information Security Training and Education on Cybersecurity Incidents: An Empirical Evidence. *Information Systems Frontiers*, **23**, 361-373. https://doi.org/10.1007/s10796-019-09977-z

[38] He, W., Ash, I., Anwar, M., Li, L., Yuan, X., Xu, L., *et al.* (2019) Improving Employees' Intellectual Capacity for Cybersecurity through Evidence-Based Malware Training. *Journal of Intellectual Capital*, **21**, 203-213. https://doi.org/10.1108/jic-05-2019-0112

[39] Caulkins, B.D., Badillo-Urquiola, K., Bockelman, P. and Leis, R. (2016) Cyber Workforce Development Using a Behavioral Cybersecurity Paradigm. 2016 *International Conference on Cyber Conflict* (*CyCon U.S.*), Washington DC, 21-23 October 2016, 1-6. https://doi.org/10.1109/cyconus.2016.7836614

[40] Coull, N., Donald, I., Ferguson, I., Keane, E., Mitchell, T., Smith, O.V., *et al.* (2017) The Gamification of Cybersecurity Training. In: Tian, F., Gatzidis, C., El Rhalibi, A., Tang, W. and Charles, F., Eds., *E-Learning and Games*, Springer, 108-111. https://doi.org/10.1007/978-3-319-65849-0_13

[41] Gonzalez, H., Llamas, R. and Ordaz, F. (2017) Cybersecurity Teaching through Gamification: Aligning Training Resources to Our Syllabus. *Research in Computing Science*, **146**, 35-43. https://doi.org/10.13053/rcs-146-1-4

[42] van Steen, T. and Deeleman, J.R.A. (2021) Successful Gamification of Cybersecurity Training. *Cyberpsychology, Behavior, and Social Networking*, **24**, 593-598. https://doi.org/10.1089/cyber.2020.0526

[43] Malone, M., Wang, Y. and Monrose, F. (2021) An Online Gamified Learning Platform for Teaching Cybersecurity and More. *Proceedings of the 22nd Annual Conference on Information Technology Education*, SnowBird, 6-9 October 2021, 29-34. https://doi.org/10.1145/3450329.3476859

[44] Rieff, I. (2018) Systematically Applying Gamification to Cyber Security Awareness Trainings: A Framework and Case Study Approach. https://www.semanticscholar.org/paper/Systematically-Applying-Gamification-to-Cyber-A-and-Rieff/20887d51c26bd70860482d3d2c92d217e2dfde46

[45] Jelo, M. and Helebrandt, P. (2022) Gamification of Cyber Ranges in Cybersecurity Education. 2022 20*th International Conference on Emerging eLearning Technologies and Applications* (*ICETA*), Stary Smokovec, 20-21 October 2022, 280-285. https://doi.org/10.1109/iceta57911.2022.9974714

[46] Ashley, T.D., Kwon, R., Gourisetti, S.N.G., Katsis, C., Bonebrake, C.A. and Boyd, P.A.

(2022) Gamification of Cybersecurity for Workforce Development in Critical Infrastructure. *IEEE Access*, **10**, 112487-112501. https://doi.org/10.1109/access.2022.3216711

[47] Hsu, F., Wu, M., Tso, C., Hsu, C. and Chen, C. (2012) Antivirus Software Shield against Antivirus Terminators. *IEEE Transactions on Information Forensics and Security*, **7**, 1439-1447. https://doi.org/10.1109/tifs.2012.2206028

[48] Patil, B.V. and Jadhav, R.J. (2014) Computer Virus and Antivirus Software a Brief Review. *International Journal of Advances in Management and Economics*, **4**, 1-4.

[49] Majthoub, M., Qutqut, M.H. and Odeh, Y. (2018) Software Re-Engineering: An Overview. 2018 8*th International Conference on Computer Science and Information Technology* (*CSIT*), Amman, 11-12 July 2018, 266-270. https://doi.org/10.1109/csit.2018.8486173

[50] Ali, M., Hussain, S., Ashraf, M. and Paracha, M.K. (2020) Addressing Software Related Issues on Legacy Systems—A Review. *International Journal of Scientific & Technology Research*, **9**, 3738-3742.

[51] Santos, B.M., de Guzman, I.G., de Camargo, V.V., Piattini, M. and Ebert, C. (2018) Software Refactoring for System Modernization. *IEEE Software*, **35**, 62-67. https://doi.org/10.1109/ms.2018.4321236

[52] Badhon, A.J. and Aggarwal, D.S. (2021) Cybersecurity in Networking Devices. *Journal of Cybersecurity and Information Management*, **8**, 35-41. https://doi.org/10.54216/jcim.080104

[53] Mueller, P., Huang, C., Yu, S., Tari, Z. and Lin, Y. (2016) Cloud Security. *IEEE Cloud Computing*, **3**, 22-24. https://doi.org/10.1109/mcc.2016.117

[54] Laksmiati, D. (2023) Vulnerability Assessment with Network-Based Scanner Method for Improving Website Security. *Journal of Computer Networks, Architecture and High Performance Computing*, **5**, 38-45. https://doi.org/10.47709/cnahpc.v5i1.1991

[55] Walden, J., Doyle, M., Lenhof, R., Murray, J. and Plunkett, A. (2010) Impact of Plugins on the Security of Web Applications. *Proceedings of the 6th International Workshop on Security Measurements and Metrics*, Bolzano, 15 September 2010, 1-8. https://doi.org/10.1145/1853919.1853921

[56] Fonseca, J.C.C.M.D. and Vieira, M.P.A. (2014) A Practical Experience on the Impact of Plugins in Web Security. 2014 *IEEE* 33*rd International Symposium on Reliable Distributed Systems*, Nara, 6-9 October 2014, 21-30. https://doi.org/10.1109/srds.2014.20

[57] Cernica, I., Popescu, N. and Tiganoaia, B. (2019) Security Evaluation of Wordpress Backup Plugins. 2019 22*nd International Conference on Control Systems and Computer Science* (*CSCS*), Bucharest, 28-30 May 2019, 312-316. https://doi.org/10.1109/cscs.2019.00056

[58] Cram, W.A., Proudfoot, J.G. and D'Arcy, J. (2020) Maximizing Employee Compliance with Cybersecurity Policies. *MIS Quarterly Executive*, **19**, Article 5.

[59] Thomas, J.E. and Galligher, G.C. (2018) Improving Backup System Evaluations in Information Security Risk Assessments to Combat Ransomware. *Computer and Information Science*, **11**, 14-25. https://doi.org/10.5539/cis.v11n1p14

[60] Jin, Y., Tomoishi, M., Matsuura, S. and Kitaguchi, Y. (2018) A Secure Container-Based Backup Mechanism to Survive Destructive Ransomware Attacks. 2018 *International Conference on Computing, Networking and Communications* (*ICNC*), Maui, 5-8 March 2018, 1-6. https://doi.org/10.1109/iccnc.2018.8390376

[61] Alharbi, T. and Portmann, M. (2019) The (in)security of Virtualization in Software

Defined Networks. *IEEE Access*, **7**, 66584-66594.
https://doi.org/10.1109/access.2019.2918101

[62] Dabbagh, M., Hamdaoui, B., Guizani, M. and Rayes, A. (2015) Software-defined Networking Security: Pros and Cons. *IEEE Communications Magazine*, **53**, 73-79.
https://doi.org/10.1109/mcom.2015.7120048

[63] Barker, E. and Barker, W. (2018) Recommendation for Key Management, Part 2: Best Practices for Key Management Organization. National Institute of Standards and Technology.

[64] Abrham, T., Kaddoura, S. and Al Breiki, H. (2023) Artificial Intelligence Applications in Cybersecurity. In: Kaddoura, S., Ed., *Handbook of Research on AI Methods and Applications in Computer Engineering*, IGI Global, 179-205.
https://doi.org/10.4018/978-1-6684-6937-8.ch009

## Appendix A

**Table A1.** Detailed questionnaire with 30 cybersecurity-related questions for small- and medium-sized Enterprises (SMEs).

| |
|---|
| 1. Has the organization developed an appropriate documented policy and implementation procedures for the necessary training and awareness of staff on information security and cybersecurity issues? |
| 2. How does the organization recognize social engineering attacks such as phishing emails, impersonation phone calls, etc.? |
| 3. Have good authentication practices been developed such as creating strong passwords and multi-factor authentication? |
| 4. Does the organization periodically conduct a cybersecurity awareness training program for staff based on distinct roles such as active & experiential learning? |
| 5. Does the organization periodically conduct cybersecurity incident simulation exercises and tests to simulate phishing incidents and their consequences? |
| 6. Has the organization developed a documented policy and implementation procedures on the security and protection of its information systems against malware infection? |
| 7. Does the organization implement technologies to protect against spam at all entry and exit points of its infrastructure? |
| 8. Has the organization developed a documented policy including implementation procedures on the secure configuration of equipment, operating systems, and applications? |
| 9. Does the organization implement an approved secure configuration procedure based on internationally accepted standards and guidelines? |
| 10. Does the organization have an approved procedure for the disposal of equipment, operating systems, and applications for which support has expired? |
| 11. Does the organization use only the latest and most up-to-date versions for critical customer applications? |
| 12. Has the organization developed a documented policy as well as implementation procedures regarding the secure architecture of its networks? |
| 13. Has the organization divided its internal network into distinct sub-networks based on the level of sensitivity of its business areas (network segmentation)? |
| 14. Does the organization apply traffic filtering between subnets to limit the flow of information to that which is strictly necessary for its business needs? |
| 15. Does the organization ensure that remote users access its internal network via VPN (Virtual Private Network) using two-factor authentication and the latest encryption algorithms? |

**Continued**

16. Is there a recorded Clean Desk Policy and clear screen?

17. Has the organization developed a documented policy as well as implementation procedures regarding the backup of its information systems?

18. Has the organization ensured that backups are obtained in an automated manner from all its major information systems daily?

19. Has the organization ensured that the received backups are protected by encryption in transit?

20. Does the Organization conduct a periodic integrity check of the backups?

21. Does the Organization conduct a periodic data restoration test with the aim of validating that the backup taking process works correctly?

22. Has the Organization developed a recorded policy as well as implementation procedures concerning the use of cryptography in its information systems?

23. Does the Organization ensure that data classified as critical/sensitive are encrypted during their transmission (encryption in transit)?

24. Does the Organization ensure that data classified as critical/sensitive are encrypted during their storage (encryption at rest)?

25. Does the organization ensure that the VPNs and firewalls have the latest version of operating systems, are kept up to date, and receive security updates and software upgrades at regular intervals in an automated manner?

26. Has the Agency developed a documented policy including implementation procedures on the physical security of the premises hosting its information systems?

27. Has the organization ensured that the building facilities hosting its servers have control mechanisms at the external perimeter for protection against unauthorized physical access?

28. Does the organization keep a list of individuals with authorization for access to the computer room?

29. Are there measures in place for tracking and recording user activities across the organization's network to ensure accountability?

30. Does the organization have procedures for regularly reviewing and updating its cybersecurity policies and systems?