SCIREA Journal of Information Science and Systems Science
ISSN: 2995-3936
http://www.scirea.org/journal/ISSS
August 31, 2024
Volume 8, Issue 4, August 2024
https://doi.org/10.54647/isss120360

Enhancing Information Security for Businesses and Organizations: Practical Controls and Systems Frameworks

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

[1]Cyber Crime Division, Hellenic Police, 173 Alexandras Avenue, 11522 Athens, Greece

[2]Department of Materials Science and Engineering, University of Ioannina, 45110 Ioannina, Greece

[3]Department of Informatics and Telecommunications, University of Ioannina, Kostaki Artas, 47150 Arta, Greece

*Authors to whom correspondence should be addressed.

Abstract

Businesses and Organizations or Small and Medium-sized Enterprises (SMEs) are pivotal to the global economy, yet they frequently encounter cyber threats that jeopardize their financial stability and operational continuity. This paper presents a proactive approach to cybersecurity designed to protect SMEs from such threats. We propose a comprehensive and scalable cybersecurity framework tailored specifically for SMEs, integrating a range of practical measures and protocols. These measures span technological defenses, employee training programs, and regulatory compliance strategies, all aimed at enhancing resilience and fostering greater cybersecurity awareness among SMEs. By adopting this holistic framework, SMEs can better safeguard their assets and ensure their continued operational success in the face of evolving cyber risks.

Keywords: Information security, cybersecurity, Businesses and Organizations, SMEs (Small and Medium-sized Enterprises), risk management, information security measurements and controls, cybersecurity frameworks

1. Introduction

In a time when digital advancements and interconnected technologies dominate, small and medium enterprises (SMEs) are pivotal to economic growth and innovation. Often regarded as the backbone of global economies, these businesses play a crucial role in job creation, wealth generation, and community development.

In 2023, the global average cost of a data breach reached USD 4.45 million, reflecting a 15% rise over the last three years. In response, 51% of organizations are planning to boost their security investments, with a focus on incident response planning and testing, employee training, and tools for threat detection and response. Interestingly, companies that make extensive use of security AI and automation save an average of USD 1.76 million compared to those that do not, underscoring the financial advantages of advanced cybersecurity strategies and measures [1].

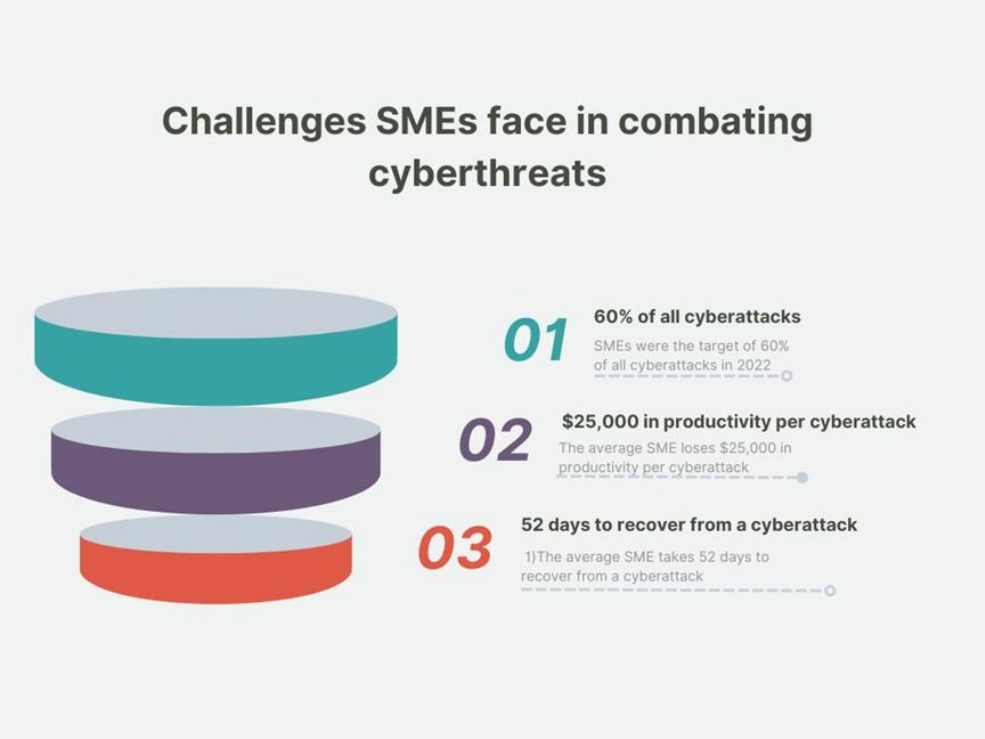

Figure 1: Challenges SMEs face in combating cyberthreats.

As SMEs strive to harness the power of technology and broaden their market presence, they often find themselves vulnerable to an increasingly complex array of cyber threats and security challenges. Due to limited budgets, these businesses frequently lack the specialized departments, such as those focused on social engineering, blue and red teaming, and extensive IT infrastructure, that are common in larger organizations. It is essential for SMEs to understand the risks linked to inadequate cybersecurity practices. This paper seeks to outline key information security controls and measures, offering a practical survival guide. The guide includes both technical and non-technical strategies, aiming not only to bolster their defenses against cyber threats but also to ensure compliance with ISO standards and data protection regulations.

2. Risk Management Methodologies and Frameworks for SMEs

Effective risk management is crucial for SMEs seeking to safeguard their assets and operations from potential threats. Several well-established methodologies and frameworks offer structured approaches to managing risk. These frameworks are chosen based on various factors such as regulatory requirements, alignment with existing risk management programs, or the desire to leverage proven processes. The adoption of a formal risk management standard helps organizations systematically address vulnerabilities and enhance their overall security posture.

ISO/IEC 27005:2022 is a comprehensive international standard that provides guidance on managing information security risks. It is part of the ISO/IEC 27000 family of standards, which focuses on information security management. ISO/IEC 27005:2022 offers a structured approach to identifying, assessing, and mitigating risks related to information security. The standard outlines methods for risk assessment, including risk identification, risk analysis, and risk evaluation, and provides guidance on how to implement appropriate controls to manage identified risks effectively. This framework is particularly useful for SMEs looking to integrate information security risk management into their overall security strategy.

The NIST Standards, developed by the National Institute of Standards and Technology, are widely recognized for their comprehensive and flexible approach to risk management. The NIST Risk Management Framework (RMF) and NIST Special Publication 800-30 offer guidelines for managing information security risks through a structured process that includes risk assessment, control implementation, and continuous monitoring. NIST standards are

adaptable and can be tailored to fit the specific needs of SMEs, providing a robust foundation for building and maintaining an effective risk management program.

Factor Analysis of Information Risk (FAIR) is a quantitative risk management framework that focuses on analyzing and quantifying information risk. FAIR provides a systematic approach to risk assessment by quantifying the potential impact of threats and vulnerabilities in financial terms. This methodology helps SMEs understand the probability and potential impact of different risks, allowing them to prioritize their risk management efforts and allocate resources more effectively. By offering a detailed and quantifiable analysis of risk, FAIR supports informed decision-making and helps organizations manage risks in a more precise and measurable way.

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is a risk assessment methodology designed specifically for small and medium-sized businesses. OCTAVE emphasizes a comprehensive evaluation of critical assets, potential threats, and vulnerabilities within an organization's operational environment. The framework involves identifying and prioritizing critical assets, assessing potential threats and vulnerabilities, and developing strategies to mitigate risks. OCTAVE is particularly beneficial for SMEs as it provides a practical and actionable approach to risk management that is tailored to their operational needs and resource constraints.

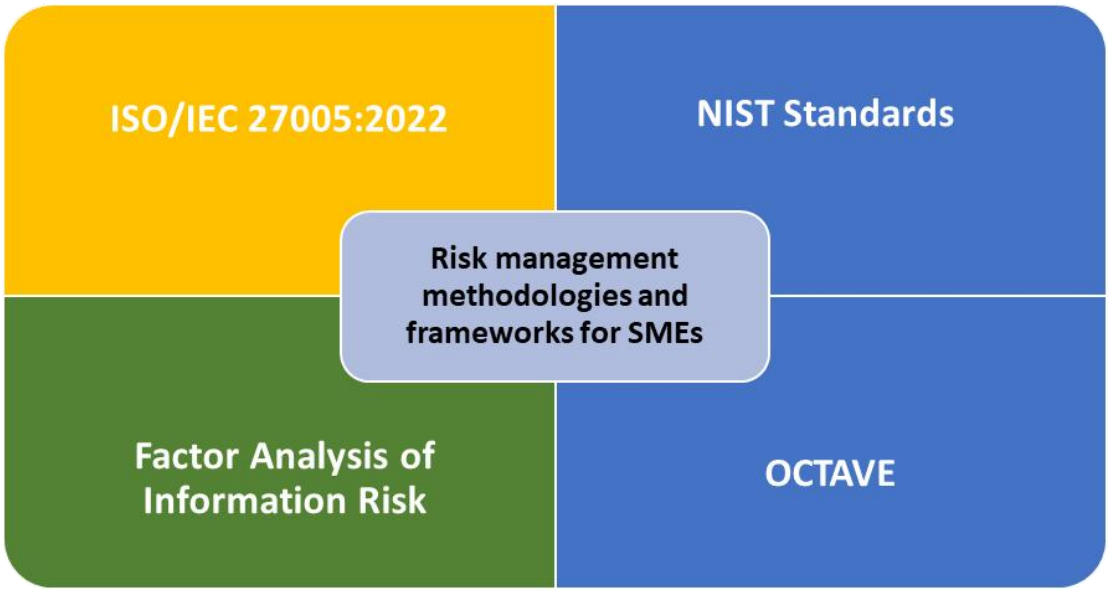

Figure 2: Risk management methodologies and frameworks for SMEs.

In summary, adopting a risk management methodology or framework is essential for SMEs to effectively address and mitigate risks. By choosing from established standards such as ISO/IEC 27005:2022, NIST standards, FAIR, or OCTAVE, organizations can implement structured and proven approaches to managing information security risks. These frameworks offer various benefits, including enhanced risk assessment, improved control implementation, and better resource allocation, ultimately supporting SMEs in maintaining a robust and resilient risk management program.

3. Information Security Measurements and Controls for SMEs

Small and medium enterprises (SMEs) play a vital role in driving economic growth and innovation, but their increasing reliance on digital technologies also exposes them to a growing range of cyber threats. Unlike larger organizations, SMEs often face significant challenges in implementing robust cybersecurity measures due to limited resources and specialized expertise. This section of paper introduces essential information security measurements and controls tailored for SMEs, providing a practical framework to strengthen their defenses against cyber threats while ensuring compliance with industry standards and data protection regulations.

3.1 Employee information security training/education

Numerous studies have highlighted the critical role of education and training in cybersecurity. Ion et al. [2] stress the importance of a comprehensive approach to cybersecurity education, encompassing both theoretical knowledge and practical skills. Kweon [3] presents empirical evidence demonstrating that security training significantly reduces the number of cybersecurity incidents within organizations. He et al. [4] examine how different training methods influence employees' perception of cybersecurity risks and their behavior, with evidence-based malware reports proving to be particularly effective. Additionally, emphasize the necessity of a human-centric approach to cybersecurity education, highlighting the importance of the National Cybersecurity Workforce Framework and the Department of Homeland Security's educational framework. Collectively, these studies underscore the need for continuous, holistic, and human-centered education and training in cybersecurity.

To support this essential endeavor, we have developed a guide that outlines key steps for effective employee training and education in cybersecurity:

Identify Threats: Employees should participate in ongoing workshops focused on cybersecurity threats and potential vulnerabilities, with particular attention to social engineering tactics. Additionally, regular phishing simulations should be conducted to familiarize employees with common phishing techniques. This training aims to equip them with the skills needed to recognize various attack strategies, such as phishing, pretexting, and baiting.

Training Modules: Organizations should develop customized training modules tailored to their specific needs and the potential threats they may face. This approach ensures that employees can directly relate the training to their daily tasks and responsibilities.

Interactive Learning: Incorporating interactive elements, such as simulations and real-life scenarios, is recommended to enhance engagement and help employees better understand the practical implications of cyber threats.

Basic Cybersecurity Awareness: Every employee should have a fundamental understanding of key cybersecurity principles. This includes the importance of using strong, unique passwords and regularly updating them. Employees should also be trained to recognize suspicious emails, avoid clicking on unknown links, and report any phishing attempts. Additionally, companies should educate their workforce on the importance of keeping software and devices up-to-date to mitigate potential vulnerabilities.

Authorized Access Areas: It is crucial for companies to establish clear areas of authorized access. Employees should be restricted to accessing only the sections of the company relevant to their specific roles to prevent potential data breaches or corruption, whether intentional or accidental.

Encourage Reporting: Enterprises should implement a policy that encourages employees to report any suspicious activity through dedicated channels for incident reporting. This policy should emphasize the importance of timely reporting and ensure that all employees understand their role in maintaining the organization's cybersecurity.

3.2 Antimalware and antiransomware software

Antimalware and antiransomware software are essential tools in protecting systems against a wide range of malicious software, including viruses, worms, Trojans, ransomware, and other forms of malware. These software solutions work by detecting, preventing, and removing harmful software before it can cause damage to a system or network.

Antimalware Software: Antimalware software is designed to detect, block, and remove various types of malicious software, including viruses, spyware, adware, and more. It scans files, emails, and websites to identify known threats using signature-based detection, as well as employing heuristics and behavioral analysis to detect new or unknown malware.

Antiransomware Software: Antiransomware software specifically targets ransomware, a type of malware that encrypts a victim's data and demands payment for its release. These tools focus on preventing ransomware from executing and protecting data from encryption.

Moreover antimalware software, often referred to as antivirus software, is a specialized tool designed to detect, prevent, and remove malicious software (malware) from computer systems and networks. Malware includes a wide range of harmful software, such as viruses, worms, trojans, ransomware, spyware, and other malicious programs. For SMEs, antimalware software utilizes several important techniques to protect their systems. One of the main methods is signature-based detection, where the software uses a database of known malware signatures—unique patterns or characteristics linked to specific threats. During regular scans or when files are accessed, the software compares these signatures against existing files, flagging any suspicious matches for further investigation. Additionally, antimalware software continuously monitors the behavior of programs and processes in real-time. Any unusual behavior, such as deviations from typical operations or actions that resemble malware, triggers alerts or prompts a closer examination. Finally, antimalware software employs advanced algorithms to identify new types of malware by analyzing their behavioral patterns or code structures, ensuring SMEs are protected against emerging threats [5-6].

3.3 Original and updated software in SMEs

Maintaining up-to-date and legitimate software is crucial for small and medium-sized enterprises (SMEs) to ensure security and efficiency. Using original, licensed software guarantees access to regular updates and patches, which are essential for protecting against vulnerabilities and cyber threats. Updated software not only improves performance and compatibility but also helps SMEs comply with industry standards and regulations. Relying on outdated or pirated software can expose SMEs to significant security risks, including malware infections and data breaches, potentially leading to financial losses and reputational damage. Therefore, investing in updated and legitimate software is a key strategy for SMEs to maintain a secure and competitive business environment.

In addition Micro, small, and medium-sized companies often struggle to allocate sufficient funds for cybersecurity, unlike larger enterprises. To cut costs, many of these companies opt not to invest in genuine software. Additionally, the importance of regularly updating existing software is frequently overlooked.

Using authentic software ensures that your business benefits from security protocols designed and supported by the legitimate developers of the software. These protocols are specifically created to combat emerging threats, providing strong protection against evolving cybersecurity risks. Moreover, the commitment from software developers goes beyond the initial purchase. By choosing original software, your business receives continuous updates and patches, strengthening your systems against new vulnerabilities over time. This proactive strategy is essential for reducing potential risks. [7-9].

3.4. Network-Attached Storage (NAS) server in SMEs

A Network-Attached Storage (NAS) server is a critical component for ensuring data security in small and medium-sized enterprises (SMEs). It provides a centralized location for storing, managing, and backing up important business data, which is essential for protecting against data loss due to hardware failures, cyberattacks, or accidental deletion. By using a NAS server, SMEs can implement automated backup routines, ensuring that all critical files are regularly saved and easily recoverable. This not only enhances data security but also ensures business continuity in the event of an unexpected incident.

Moreover, a NAS server offers robust security features that are particularly beneficial for SMEs. These servers typically include encryption, access controls, and user authentication, which help safeguard sensitive data from unauthorized access. By allowing businesses to set user-specific permissions, NAS servers ensure that only authorized personnel can access certain data, reducing the risk of internal data breaches. Additionally, many NAS systems support real-time monitoring and alerting, enabling SMEs to detect and respond to potential security threats promptly. Overall, a NAS server provides a scalable, secure, and efficient solution for managing and protecting valuable business data in SMEs.

The significance of a NAS server for security in an SME is underscored by several key factors [10-11]:

Data Centralization: NAS enables centralized data storage, ensuring that critical files and information are kept in a single, secure location. This approach reduces the risk of data loss and minimizes the chances of data theft or ransomware attacks.

Access Control: NAS devices often feature access control mechanisms, allowing administrators to manage and restrict access to sensitive data. This ensures that only authorized personnel can view, modify, or delete specific files or directories, helping to prevent unauthorized access and potential data breaches.

Data Encryption: NAS servers offer encryption options to secure data both during transmission and while stored. Encryption is vital for protecting sensitive information from being intercepted during data transfers or in the event of unauthorized physical access to the storage device. Moreover, data encryption is essential for compliance with data protection regulations, such as the General Data Protection Regulation (EU GDPR).

Backup and Redundancy: NAS servers typically support automated backup processes, regularly creating copies of data. This is crucial for data recovery in cases of accidental deletion, hardware failure, and other issues. A reliable backup strategy enhances data security by ensuring data integrity and availability, while regular backups also provide protection against malware and ransomware attacks.

Virus and Malware Protection: NAS servers are often equipped with built-in antivirus and anti-malware features, providing an additional layer of defense against cyberattacks.

3.5 Website Security

For SMEs, a website is crucial for business operations, serving as a platform for e-commerce, communication, and various other functions. It includes a domain name and is built using programming languages such as PHP, CSS, SQL, JavaScript, and Python, along with plugins that enhance its features, like managing cookies and facilitating transactions.

Protecting the domain is essential for maintaining a company's online identity and preventing misuse, fraud, or phishing attacks. Compromised domains can lead to data breaches and damage to the brand's reputation. Additionally, regularly updating plugins and programming languages is vital for cybersecurity. Updates address security vulnerabilities, preventing exploitation by cybercriminals and ensuring the website remains secure and functional. Keeping these elements current helps safeguard sensitive data and maintain the website's integrity [12-13].

3.6 Implementing Clean Desk and Screen Privacy Policies in SMEs

Clear guidelines for managing physical documents and removable storage media, as well as maintaining clear screens in information processing areas, are crucial for SMEs. Organizations should develop and enforce a policy on clean desks and screens, communicating these standards to all relevant personnel. This approach helps minimize unauthorized access and reduces the risk of physical social engineering attacks [14]. The policy should include the following key practices:

Secure Storage: Store sensitive or important business information, whether in paper or digital format, in a secure place such as a locked safe, cabinet, or other secure storage when not in use, particularly after office hours.

Endpoint Protection: Use key locks or other security measures to protect user devices when they are not in use or left unattended.

Device Security: Ensure that user devices are either logged off or protected with a screen and keyboard lock, using user authentication mechanisms. All computers and systems should be configured with timeout or automatic logout features.

Secure Printing: Use printers with authentication features to ensure that only the individual who requested the printout can retrieve their documents, and only when physically present at the printer.

Secure Storage and Disposal: Store documents and removable media containing sensitive information securely, and dispose of them using secure methods when they are no longer needed.

Screen Management: Establish rules for managing screen pop-ups, such as disabling notifications for new emails and messages during presentations or screen sharing.

Display Maintenance: Remove sensitive or critical information from whiteboards and other displays as soon as it is no longer needed.

Implementing these guidelines helps ensure that information remains secure and minimizes the risk of data breaches or unauthorized access.

3.7 Information backup policy for SMEs

SMEs must adhere to a reliable and well-established practice for maintaining backup copies of their information, software, and systems, following a specific backup policy tailored to

their data retention and security needs. This policy ensures effective recovery in the event of an incident, failure, or loss of storage media. Developing and implementing a backup plan involves several key considerations:

Documentation: Maintain accurate records and detailed restoration procedures for backup copies.

Backup Scope and Frequency: Ensure that backup practices align with business needs, security standards, and the criticality of the information, including the type (e.g., full or incremental backups) and frequency of backups.

Safe Storage: Store backups in a secure, remote location to protect them from potential disasters at the primary site.

Protection: Provide adequate physical and environmental safeguards for backup data.

Testing: Regularly test backup media to confirm their reliability in emergencies. Perform restoration tests on separate systems to avoid damaging the original data.

Encryption: Apply encryption to backup data based on identified risks, particularly when confidentiality is critical.

Pre-Backup Checks: Implement measures to identify inadvertent data loss before initiating the backup process.

Operational procedures should include monitoring backup activities and addressing any failures in scheduled backups to ensure adherence to the backup policy. Regular testing of backup measures for various systems and services is crucial to support incident response and business continuity plans. Comprehensive backup strategies should cover all essential system information, applications, and data to ensure full recovery in the event of a disaster, data theft, or ransomware attack. [15-16].

3.8 Network security of SMEs

Securing and managing networks and their devices is critical for safeguarding information within SMEs. To ensure robust network security, SMEs must assess the types of information and their classification levels that the network supports. This involves defining clear responsibilities and procedures for managing networking equipment and maintaining up-to-date documentation, including network diagrams and device configurations. It is also important to separate network management from ICT system operations when necessary and

implement controls to protect data confidentiality and integrity across public, third-party, and wireless networks, with additional measures to ensure service availability. Logging and monitoring network activities, authenticating systems, and using firewalls to restrict and filter network connections are essential practices. Furthermore, detecting and managing connections of devices, hardening network devices, and segregating network administration from other traffic enhance overall security.

For virtualized networks, such as those using software-defined networking (SDN) and SD-WAN, applying appropriate security controls leverages their benefits by allowing logical separation of communications over physical networks. Managing the security of large networks may require dividing them into distinct domains based on trust levels, sensitivity, or organizational units. This segregation, achieved through physically separate networks or logical network divisions, helps protect against vulnerabilities and ensures comprehensive security across the entire infrastructure. [17-18]

3.9 Use of cryptography in SMEs

SMEs should establish and enforce robust cryptographic practices, including effective cryptographic key management, to ensure the secure and compliant use of encryption technologies. This involves developing a comprehensive policy that outlines general principles for protecting information and specifies the required level of cryptographic protection based on information classification. The policy should detail the type, strength, and quality of cryptographic algorithms needed and ensure the use of cryptography for securing data on mobile devices, storage media, and during network transmission. Key management practices should include secure key generation, protection, and recovery procedures in case of key loss or compromise.

Additionally, SMEs must assign clear roles and responsibilities for implementing cryptographic rules and managing keys, and ensure that adopted cryptographic standards and solutions meet organizational requirements and approvals. It is also important to assess how encryption impacts other security controls, such as malware detection and content filtering. Compliance with relevant regulations, including national restrictions on cryptographic techniques and considerations for the trans-border flow of encrypted information, must be integrated into the cryptographic policy to address legal and regulatory aspects effectively. [19]

3.10 Use of artificial intelligence (AI)

Artificial intelligence (AI) is rapidly becoming essential for enhancing cybersecurity in small and medium-sized enterprises (SMEs) due to its ability to address the limitations of traditional security systems and cope with increasing cyber threats. AI technologies, such as machine learning and data mining, offer substantial benefits by improving threat detection and response. Unlike conventional systems that depend on pre-defined threat signatures, AI algorithms can analyze large volumes of data to recognize patterns and anomalies, enabling the identification of new and evolving threats. This proactive approach allows SMEs to detect and mitigate potential attacks more swiftly and effectively.

AI also enhances the speed and efficiency of incident response through automation. When a security threat is detected, AI can immediately execute response protocols, such as isolating infected systems or blocking malicious activities, thereby reducing the time attackers have to exploit vulnerabilities. This automation not only helps in managing threats more quickly but also alleviates the workload on human security teams, allowing them to focus on more strategic aspects of cybersecurity. Additionally, AI's predictive analytics capabilities enable SMEs to foresee potential vulnerabilities and adjust their defenses before an attack occurs, shifting from a reactive to a proactive cybersecurity posture [20].

Moreover, AI contributes to improved risk management and compliance for SMEs. It helps quantify and prioritize risks based on their likelihood and impact, allowing for more effective allocation of resources. AI systems can also detect phishing attempts and monitor user behavior to identify potential insider threats. Furthermore, AI assists in maintaining regulatory compliance by automating data protection processes and monitoring adherence to legal requirements. This comprehensive approach ensures that SMEs can better protect sensitive information and manage their cybersecurity measures efficiently.

3.11 Best Practices for Secure Teleworking in SMEs

Organizations and SMEs must implement and support robust procedures for teleworking to safeguard personal data and mitigate risks associated with remote work. Employees should be well-informed and trained on these procedures, given that many may be unfamiliar with the technologies and potential vulnerabilities of telecommuting. Key practices include ensuring secure access to IT resources through technologies like Virtual Private Networks (VPNs) with encryption and user authentication. Access should be restricted based on job requirements, and Remote Desktop Protocol (RDP) connections should only occur via secure VPNs. Secure

Wi-Fi protocols, such as WPA2, should be used, and files containing personal data should not be stored on untrusted online services unless they offer adequate security.

It is crucial to maintain the security of telecommuting devices by regularly updating antivirus software, firewalls, operating systems, and web browsers. Employees should also clear browsing history after work sessions and keep work-related files separate from personal ones. Encrypting files containing sensitive data, especially when using portable storage media or a primary device, is essential. Virtual machines dedicated to work tasks can further enhance security.

For teleconferencing, it is important to use platforms that offer secure services with end-to-end encryption to protect sensitive discussions. By adopting these practices, SMEs can better manage the risks associated with remote work, ensuring that personal data and organizational resources remain secure.

3.12 Physical Security Strategies and Measures for SMEs

To safeguard buildings, critical areas, computer rooms, staff offices, IT equipment, and physical file storage from potential damage caused by natural disasters or malicious actions, SMEs should implement effective protective measures. These threats include floods, fires, earthquakes, explosions, water leaks, power outages, burglary, theft, and vandalism. Recommended strategies include installing alarms, security doors, and windows, as well as deploying fire protection systems. Equipment should be positioned away from risks such as water pipes and dust sources. Additionally, employing moisture and flood detectors and ensuring an uninterrupted power supply with stabilizers or generators are essential steps to enhance resilience and maintain operational continuity.

3.13 Enhancing Business Continuity and Resilience for SMEs

The SMEs must establish and maintain documented policies and procedures to ensure business continuity and recovery from disruptions to critical information systems caused by adverse events. This includes identifying critical systems and functions and performing an impact assessment to evaluate potential risks from events such as cyberattacks or natural disasters.

The organization should develop a comprehensive business continuity plan designed to restore and maintain critical functions and services promptly following an adverse event. To support this process, the organization may seek certification to a management system that

prepares, responds to, and recovers from such events, ensuring the continued delivery of products and services at an acceptable level. An example of an international standard for this purpose is ISO 22301:2019, which focuses on security and resilience.

4. Information security and cybersecurity frameworks for SMEs

While each organization has unique missions, objectives, and risk tolerances, they are not necessarily required to create their own governance frameworks from scratch to address security and privacy goals. Some organizations may already have suitable control frameworks in place, while others may not. Although adopting an industry-standard control framework is not mandatory, it can be highly beneficial. These frameworks are proven through widespread implementation across various companies and are updated regularly to address evolving business needs, emerging threats, and technological advancements.

4.1. 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 27002:2022** 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.

4.2 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.

4.3 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.

4.4 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."

4.5. Payment Card Industry Data Security Standard (PCI DSS)

The **Payment Card Industry Data Security Standard (PCI DSS)** is a globally recognized information security standard, established by major credit card brands and managed by the Payment Card Industry Security Standards Council. This standard offers a control framework specifically aimed at protecting credit card information throughout its storage, processing, and transmission within organizational networks. Compliance with PCI DSS is mandatory for all entities that handle credit card data, with larger organizations required to undergo annual onsite audits. Many organizations and SMEs also apply PCI DSS principles more broadly to safeguard other types of financial and personal data beyond just credit card information.

Figure 3: Information security and cybersecurity controls and frameworks for SMEs.

5.Conclusions

Small and Medium-sized Enterprises (SMEs) play a crucial role in the global economy, representing approximately 90% of all businesses and employing over half of the workforce worldwide. Despite their economic significance, SMEs often struggle with limited resources for addressing cybersecurity challenges, making them particularly vulnerable to cyberattacks. As cybercriminals increasingly target these businesses, it is imperative for SMEs to adopt comprehensive strategies to protect their information systems and ensure their continued operation.

This paper has explored various risk management methodologies and frameworks suitable for SMEs. We examined established standards such as ISO/IEC 27005:2022, NIST Standards, Factor Analysis of Information Risk (FAIR), and Operationally Critical Threat, Asset, and

Vulnerability Evaluation (OCTAVE). These frameworks offer structured approaches for identifying and mitigating cybersecurity risks, allowing SMEs to build a solid foundation for their information security efforts. By selecting and implementing these frameworks, SMEs can better align their risk management practices with industry standards and improve their ability to manage and respond to emerging threats.

In addition to risk management frameworks, effective information security measures and controls are essential for safeguarding SME operations. Key strategies include implementing comprehensive employee training programs to enhance cybersecurity awareness, regularly updating software to protect against evolving threats, ensuring timely backups of critical data to mitigate ransomware risks, and applying strict access controls to prevent insider threats. These measures collectively strengthen an SME's defenses against cyber threats and reduce potential vulnerabilities.

Beyond preventive measures, developing robust cyber resilience strategies is critical for maintaining business continuity in the face of cyber incidents. SMEs must establish well-defined incident response and recovery plans that enable swift and effective responses to security breaches. This involves preparing for various types of cyber threats, ensuring rapid recovery from disruptions, and adapting to new and emerging risks. By focusing on resilience, SMEs can minimize the impact of cyber incidents and maintain operational stability.

Finally, understanding and applying information security and cybersecurity frameworks specifically designed for SMEs is fundamental for creating a secure environment. These frameworks provide actionable guidelines tailored to the unique needs and constraints of smaller organizations. Fostering a culture of cybersecurity within SMEs—emphasizing ongoing education, compliance with standards, and resilience—ensures that businesses are well-prepared to protect their assets and secure their future. By adopting a comprehensive approach to cybersecurity, SMEs not only enhance their own security but also contribute to the broader stability of the global economy.

References

[1] IBM, IBM Cost of a Data Breach Report, **2023;** Available online: https://www.ibm.com/reports/data-breach (accessed on 12 April 2024).

[2] Ion, B., Rodica, B., Dumitru, C; *Support of education in cybersecurity*; Pro Publico Bono–Public Administration; **2021**; 9(1), 128-147.

[3] Kweon, E., Lee, H., Chai, S., Yoo, K; *The utility of information security training and education on cybersecurity incidents: An empirical evidence*; **2021**; Information Systems Frontiers, 23; 361-373.

[4] He, W., Ash, I., Anwar, M., Li, L., Yuan, X., Xu, L., Tian, X.; *Improving employees' intellectual capacity for cybersecurity through evidence-based malware training*; **2020**; Journal of intellectual capital; 21(2), 203-213.

[5] Majthoub, M., Qutqut, M. H., Odeh, Y.; *Software re-engineering: An overview;* **2018**; In 2018 8th International Conference on Computer Science and Information Technology (CSIT); (pp. 266-270), IEEE.

[6] Ali, M., Hussain, S., Ashraf, M., Paracha, M. K.; *Addressing Software Related Issues On Legacy Systems–A Review;* **2020**; International Journal of Scientific & Technology Research; 9(03), 3738-3742.

[7] Santos, B. M., de Guzmán, I. G. R., de Camargo, V. V., Piattini, M., Ebert, C.; *Software refactoring for system modernization*; **2018**; IEEE Software; 35(6), 62-67.

[8] Badhon, A. J., Aggarwal, S.; *Cybersecurity in Networking Devices;* **2021**; Journal of Cybersecurity and Information Management (JCIM); Vol, 8(1), 35-41.

[9] Mueller, P., Huang, C. T., Yu, S., Tari, Z., Lin, Y. D.; *Cloud security*; **2016**; IEEE Cloud Computing; 3(5), 22-24.

[10] Laksmiati, D.; *Vulnerability Assessment with Network-Based Scanner Method for Improving Website Security*; **2023**; Journal of Computer Networks; Architecture and High Performance Computing; 5(1), 38-45.

[11] Walden, J., Doyle, M., Lenhof, R., Murray, J., Plunkett, A.; *Impact of plugins on the security of web applications*; **2010**; In Proceedings of the 6th International Workshop on Security Measurements and Metrics; (pp. 1-8).

[12] Da Fonseca, J. C. C. M., Vieira, M. P. A.; *A practical experience on the impact of plugins in web security;* **2014**; In 2014 IEEE 33rd International Symposium on Reliable Distributed Systems; (pp. 21-30), IEEE.

[13] Cernica, I., Popescu, N.; *Security evaluation of wordpress backup plugins*; **2019**; In 2019 22nd International Conference on Control Systems and Computer Science (CSCS); (pp. 312-316), IEEE.

[14] Jin, Y., Tomoishi, M., Matsuura, S., Kitaguchi, Y.; *A secure container-based backup mechanism to survive destructive ransomware attacks. In 2018 International Conference on Computing*; **2018**; Networking and Communications (ICNC); (pp. 1-6); IEEE.

[15] Alharbi, T., Portmann, M.; *The (in) security of virtualization in software defined networks*; **2019**; IEEE Access; 7, 66584-66594.

[16] Dabbagh, M., Hamdaoui, B., Guizani, M., Rayes, A.; *Software-defined networking security: pros and cons;* **2015**; IEEE Communications Magazine; 53(6), 73-79.

[17] Barker, E., Barker, W.; *Recommendation for key management, part 2: best practices for key management organization;* **2018**; National Institute of Standards and Technology.

[18] Abrham, T., Kaddoura, S., Al Breiki, H.; *Artificial intelligence applications in cybersecurity*; **2023**; In Handbook of Research on AI Methods and Applications in Computer Engineering; (pp. 179-205), IGI Global.

[19] Barker, E., Barker, W.; Recommendation for key management, part 2: best practices for key management organization; **2018**; National Institute of Standards and Technology.

[20] Abrham, T., Kaddoura, S., Al Breiki, H.; Artificial intelligence applications in cybersecurity; **2023**; In Handbook of Research on AI Methods and Applications in Computer Engineering; (pp. 179-205), IGI Global.