Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Information Technologies

Bachelor Thesis

Impact of Cybersecurity Breaches on Small and Medium-Sized enterprises (SMEs)

Vanessa Flora Igitego Ngirabega

© 2025 CZU Prague

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

BACHELOR THESIS ASSIGNMENT

Vanessa Flora Igitego Ngirabega

Informatics

Thesis title

Impact of Cybersecurity Breaches on Small and Medium-Sized Enterprises (SMEs)

Objectives of thesis

The main objective of this research is to comprehensively analyze the impact of cybersecurity breaches on a sample of small and medium-sized enterprises (SMEs). This will be achieved by exploring the following partial objectives:

- Identify the most common cyberattacks targeting SMEs and vulnerabilities of SMEs.

- Investigate the operational disruptions caused by cyber-attacks on SMEs.

- To develop a strategy aimed at safeguarding the private data of small and medium enterprises (SMEs) against cyber threats, and reducing the economic repercussions of potential data breaches.

Methodology

The methodology for solving the theoretical part of the thesis will be based on the study and analysis of professional information sources and case studies of case studies of cybersecurity breaches that impacted SMEs. Based on the knowledge gained in the theoretical part of the thesis, the practical part will be to develop a strategy to safeguard SMEs' private data and mitigate the economic impacts of breaches.

The proposed extent of the thesis

40

Keywords

Cyber-security, Small and medium-sized enterprises, Vulnerability assessment, Operational disruptions, Risk mitigation strategies

---

Recommended information sources

Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. Risk Analysis, 42(8), 1643-1669.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. Technology innovation management review, 4(10).

] Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. Journal of Information Security and Applications, 58, 102726.

Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. International Journal of Engineering Research and Applications, 2(2), 202-209.

Expected date of thesis defence

2024/25 SS – PEF

The Bachelor Thesis Supervisor

RNDr. Alexander Galba

Supervising department

Department of Information Technologies

Electronic approval: 09. 07. 2024

doc. Ing. Jiří Vaněk, Ph.D.

Head of department

Electronic approval: 04. 11. 2024

doc. Ing. Tomáš Šubrt, Ph.D.

Dean

Prague on 17. 03. 2025

Declaration

I, Vanessa Flora Igitego Ngirabega, declare that I have worked independently on my bachelor thesis titled "Impact of cybersecurity breaches on Small and Medium-Sized Enterprises (SMEs).” All sources used in this thesis have been appropriately referenced at the end of the document.

As the author of the bachelor thesis, I affirm that the thesis does not break any copyrights to the best of my knowledge.

Prague, 13.03.2024 _____

Acknowledgment

First and foremost, I give God all thanks, glory, and praise for His constant wisdom, grace, and strength. I would also like to thank my supervisor, RN Dr. Alexander Galba, for their constructive feedback throughout my thesis. Lastly, I would like to express my heartfelt gratitude to my family and friends for keeping me motivated through all the ups and downs of this journey and for always believing in me, even when I didn't. You all made this journey not only possible but truly memorable

Impact of Cybersecurity Breaches on Small and Medium-Sized Enterprises (SMEs)

Abstract

This bachelor thesis examines the impacts of cybersecurity breaches on small and medium-sized enterprises (SMEs), focusing on both the operational disruptions and financial impacts these businesses face.

The goal of this research is to identify common cyberattacks that target SMEs and the vulnerabilities that make them particularly susceptible, analyse impacts of breaches, and propose a framework for data protection.

In the theoretical part, the thesis reviews existing literature and analyses case studies of real-world cybersecurity incidents affecting SMEs, providing insight into the challenges they encounter.

The practical part uses this knowledge by developing a strategy to protect the private data of SMEs and reduce the economic consequences of potential breaches. This study offers practical recommendations to help SMEs strengthen their cybersecurity measures and better navigate the growing threat of cyberattacks.

Keywords: Cyber security, Small and medium-sized enterprises, Vulnerability assessment, Operational disruptions, Risk mitigation strategies

Dopad narušení kybernetické bezpečnosti na malé a střední podniky (SME)

Abstrakt

Tato bakalářská práce zkoumá dopady narušení kybernetické bezpečnosti na malé a střední podniky (MSP) se zaměřením jak na provozní narušení, tak na finanční dopady, kterým tyto podniky čelí.

Cílem tohoto výzkumu je identifikovat běžné kybernetické útoky, které se zaměřují na malé a střední podniky, a zranitelná místa, která je činí zvláště náchylnými, analyzovat dopady porušení a navrhnout rámec pro ochranu údajů.

V teoretické části práce reviduje existující literaturu a analyzuje případové studie skutečných incidentů kybernetické bezpečnosti, které ovlivňují malé a střední podniky, a poskytuje vhled do výzev, s nimiž se potýkají.

Praktická část využívá těchto znalostí při vývoji strategie ochrany soukromých dat malých a středních podniků a snížení ekonomických důsledků potenciálních narušení. Tato studie nabízí praktická doporučení, která malým a středním podnikům pomohou posílit jejich opatření v oblasti kybernetické bezpečnosti a lépe se vypořádat s rostoucí hrozbou kybernetických útoků.

Klíčová slova: Kybernetická bezpečnost, Malé a střední podniky, Hodnocení zranitelnosti, Provozní narušení, Strategie zmírňování rizik

Table of Content

1. Introduction **11**
1.1 Cybersecurity 11
1.2 Small and Medium Enterprises 12
1.3 Background on Cybersecurity in SMEs 13
2. Objectives and methodology **15**
2.1. Objectives 15
2.2. Methodology 15
3. Literature review **16**
3.1 Defining Cybersecurity in the Context of SMEs 16
3.1.1 Multidisciplinary Definitions of Cybersecurity 16
3.1.2 Cybersecurity Risk in SMEs 17
3.1.3 The Role of Cybersecurity Culture in SMEs 20
3.1.4 The Economic Implications of Cybersecurity for SMEs 21
3.1.5 Future Directions and Recommendations 22
3.2. Common Cyberattacks and Vulnerabilities Targeting SMEs 23
3.2.1 Types of Cyberattacks 23
3.2.2 Conclusion 26
3.3 Vulnerabilities of SMEs 27
3.3.1 Limited Resources 27
3.3.2 Lack of Cybersecurity Expertise 28
3.3.3 Lower Security Budgets 29
3.3.4 Insufficient Security Policies 29
3.3.5 Challenges Posed by Remote Work 30
3.3.6 Influence on Cybersecurity Readiness 30
3.3.7 Conclusion 31
3.4. Operational Disruptions Caused by Cyber-Attacks on SMEs 31
3.4.1 Impact on Operations 31
3.4.2 Financial Consequences 32
3.4.3 Damage to Reputation 32
3.4.4 Case Studies 33
3.4.5 Conclusion 36

4. Practical part **37**
4.1. Introduction 37
4.2. Hypothetical profile 37
4.2.1 Simulated cyberattack: Ransomware attack 39
4.3. Strategy 40
4.4 Implementation Phase 46
4.5 Cost-Benefit Analysis 47
4.5.1 Introduction 47
4.5.2 Cost-Benefit Analysis of Cybersecurity Implementation Table 47
4.5.3. Conclusion of Cost-Benefit Analysis 49
5. Conclusion and future research directions **51**
5.1 Summary of Key Findings 51
5.2 Gaps in the Literature and Future Research 51
5.3 Conclusion 52
6. References **53**
7. List of pictures, tables, and abbreviations **57**
7.1 List of pictures 57
7.2 List of tables 57
7.3 List of abbreviations 57

1. Introduction

1.1 Cybersecurity

For many small and medium business owners, cybersecurity feels like a distant concern until the moment they find themselves locked out of their own systems, facing ransom demands.

Cybersecurity is the practice of safeguarding computers, networks, and data from unauthorised access, damage, or theft. It involves a comprehensive set of processes, technologies, and strategies designed to protect digital assets from a wide array of threats. As our reliance on digital systems grows, the importance of cybersecurity becomes even more critical [1].

At its essence, cybersecurity aims to protect the confidentiality, integrity, and availability of information. Confidentiality ensures that sensitive information is only accessible to those who are authorised to see it. Integrity involves maintaining the accuracy and trustworthiness of data and ensuring that it is not altered or tampered with by unauthorised parties. Availability ensures that information is accessible to authorised users when needed, without unnecessary delays or disruptions [2].

In practical terms, cybersecurity encompasses a wide range of activities. These include deploying technical solutions like firewalls, encryption, and antivirus software, as well as implementing organizational policies such as incident response plans and regular security training for employees. It's important to recognise that cybersecurity isn't just about technology; it also involves the human element, where educating users and fostering a culture of security awareness plays a crucial role in preventing cyber incidents [1].

The field of cybersecurity is dynamic and constantly evolving as new threats emerge and technologies advance. This ever-changing landscape requires continuous effort and vigilance to stay ahead of potential attackers. For enterprises, this means regularly updating their security measures, conducting risk assessments, and ensuring that all employees are trained to recognise and respond to potential threats [3].

In a nutshell, cybersecurity is an important practice that involves protecting digital systems and data from a wide variety of threats. It is a multifaceted discipline that requires a combination of

technology, policy, and education to effectively mitigate risks and ensure the security of information in an increasingly digital world [2].

1.2 Small and Medium Enterprises

Small and Medium Enterprises (SMEs) are a crucial component of the global economy, playing a significant role in driving innovation, employment, and economic growth. SMEs are typically defined by their size, which is measured based on criteria such as the number of employees, annual turnover, and balance sheet totals. While the specific definitions may vary depending on the country or organization, SMEs are generally characterised as businesses that operate with a relatively small workforce and have limited financial resources compared to larger corporations [4].

In most contexts, Small Enterprises are businesses that typically employ fewer than 50 people, while Medium Enterprises may employ up to 250 individuals. These enterprises often have a more flexible and adaptable structure, enabling them to respond quickly to market changes and customer needs. Their size allows them to operate with greater agility, fostering innovation and niche market opportunities. Despite their smaller scale, SMEs contribute significantly to the economy by creating jobs, generating income, and supporting local communities [5].

Compared to larger businesses, SMEs face unique challenges, particularly in areas such as access to finance, market competition, and regulatory compliance. Due to their limited resources, SMEs often struggle with obtaining the capital necessary for expansion or investment in new technologies. Furthermore, they may lack the economies of scale enjoyed by larger firms, making it harder to compete on price and reach broader markets. However, their ability to innovate and develop close relationships with customers often gives them a competitive advantage in specific market segments [4].

The importance of SMEs extends beyond economic contributions; they also play a vital role in social and community development. SMEs are often deeply integrated into local economies, providing essential goods and services and fostering community engagement. Their presence in rural or underserved areas can be particularly impactful, as they help to stimulate local economic activity and provide employment opportunities where larger enterprises may not operate.

In conclusion, SMEs are a diverse and dynamic segment of the economy that, despite facing various challenges, contribute significantly to economic growth and community development. Their role in fostering innovation, providing employment, and supporting local economies underscores their importance in both developed and developing nations [5].

1.3 Background on Cybersecurity in SMEs

In today's digital age, cybersecurity has become a critical concern for Small and Medium Enterprises (SMEs). These businesses, while often less resourced than larger corporations, are increasingly reliant on digital technologies to manage their operations, communicate with customers, and compete in the marketplace. However, this growing dependence on technology also makes them more vulnerable to cyber threats that can disrupt their activities, compromise sensitive information, and lead to significant financial losses.

Cybersecurity in SMEs is particularly challenging due to the unique characteristics of these enterprises. Unlike large organizations, SMEs often operate with limited financial and human resources, hindering their ability to implement comprehensive security measures. Cybersecurity encompasses a wide array of processes, technologies, and practices designed to protect digital infrastructure from cyber threats. However, the complexity and cost associated with these measures can be overwhelming for SMEs, which may lack the necessary expertise and budget to manage their cybersecurity needs effectively [6].

Furthermore, the nature of cybersecurity threats is continually evolving, with cybercriminals increasingly targeting SMEs due to their perceived vulnerabilities. SMEs often have less sophisticated security defences, making them easier targets for attacks such as phishing, ransomware, and data breaches. These attacks can have devastating consequences, not only causing direct financial losses but also damaging the business's reputation and eroding customer trust. Given that SMEs often rely heavily on customer relationships and trust, a security breach can have far-reaching implications beyond the immediate financial impact.

Effective cybersecurity in SMEs requires a multidisciplinary approach, integrating knowledge from various fields such as risk management, technology, and human behaviour. This approach is essential because cybersecurity is not just a technical issue but also involves understanding the human and organizational factors that contribute to vulnerability. For instance, the lack of

cybersecurity awareness among employees, insufficient training, and inadequate security policies can all increase the risk of a successful cyber-attack [3].

Besides the challenges, SMEs can take several steps to improve their cybersecurity posture. These include adopting basic security measures such as using strong passwords, regularly updating software, and implementing firewalls and antivirus programs. Additionally, SMEs can benefit from cybersecurity frameworks and guidelines developed by experts, which provide a structured approach to identifying and managing. By prioritizing cybersecurity and leveraging available resources and expertise, SMEs can better protect themselves from cyber threats and ensure their long-term viability in a digital world [3].

Cybersecurity is a critical issue for SMEs, requiring a strategic and multifaceted approach to address the unique challenges they face. While SMEs may lack the resources of larger organizations, they can still implement effective security measures by focusing on education, awareness, and the adoption of best practices. As cyber threats continue to evolve, SMEs must remain vigilant and proactive in safeguarding their digital assets.

2. Objectives and methodology

2.1. Objectives

This thesis focuses on the relationship between cybersecurity breaches and small and medium-sized enterprises (SMEs), aiming to dissect the profound impact these breaches have on the operational and economic aspects of these businesses. SMEs are particularly vulnerable to cyberattacks due to their often-limited resources and underdeveloped cybersecurity infrastructures, making them an attractive target for cybercriminals. Unlike larger organizations, SMEs typically lack sophisticated defence mechanisms and dedicated IT departments that can promptly address emerging cyber threats. As a result, the fallout from a successful cyberattack can be devastating, potentially leading to significant operational disruptions, financial loss, and long-term reputational damage.

The primary objective of this research is to provide a comprehensive analysis of how cybersecurity breaches affect SMEs. To achieve this, the study will focus on several key areas. First, it will identify the most prevalent types of cyberattacks that target SMEs, as well as the specific vulnerabilities that make these enterprises particularly susceptible to such threats. This will include an examination of the tactics, techniques, and procedures commonly employed by attackers against SMEs.

Secondly, the research will investigate the operational disruptions caused by these cyberattacks. This includes analysing how breaches can affect business continuity, disrupt day-to-day operations, and lead to extended downtimes that can hinder the overall productivity of SMEs. Understanding the scope and severity of these disruptions is crucial for developing effective mitigation strategies.

2.2. Methodology

The thesis will aim to develop a strategic framework designed to protect the sensitive data of SMEs against cyber threats. This strategy will not only focus on safeguarding private data but also on reducing the potential economic repercussions of data breaches. By addressing these partial objectives, the research intends to offer actionable insights and recommendations that can help SMEs bolster their cybersecurity defences, thereby minimizing the risk and impact of cyberattacks.

3. Literature review

3.1 Defining Cybersecurity in the Context of SMEs

3.1.1 Multidisciplinary Definitions of Cybersecurity

Cybersecurity is a complex and evolving field that defies a singular definition, particularly when considered in the context of Small and Medium Enterprises (SMEs). As digital technologies have proliferated, the need for robust cybersecurity measures has become increasingly apparent. However, the definition of cybersecurity can vary significantly depending on the disciplinary lens through which it is viewed.

Cains et al. (2022) emphasize the importance of a multidisciplinary approach to defining cybersecurity, particularly in contexts where the stakes of cyber risk are high, such as in SMEs. They argue that cybersecurity cannot be adequately understood through a single disciplinary perspective, as it intersects with various fields, including information technology, psychology, risk management, and organizational behaviour. From an IT perspective, cybersecurity is often viewed as the protection of digital infrastructure against unauthorised access, attacks, or damage. This involves the implementation of technical safeguards such as firewalls, encryption, and intrusion detection systems.

However, Cains et al. (2022) extend this definition by incorporating perspectives from other disciplines. For example, from a psychological standpoint, cybersecurity also involves understanding human behaviours and how they contribute to both the vulnerabilities and defences of a system. This includes user behaviour, awareness, and compliance with security protocols. On the other hand, the organizational perspective emphasizes the role of policies, procedures, and governance structures in managing cybersecurity risks.

Craigen, Diakun-Thibault, and Purse (2014) also contribute to this multidisciplinary understanding of cybersecurity by defining it as a set of practices designed to protect information and systems from cyber threats. They highlight that cybersecurity is not just about technology but also encompasses people, processes, and the broader organizational environment. This holistic view is particularly relevant to SMEs, where technology integration with everyday business practices is often less formalised than in larger enterprises.

When applying these definitions to SMEs, it becomes evident that cybersecurity in these businesses must be approached in a comprehensive manner, considering both technical and human factors. SMEs often operate with limited resources, making them more susceptible to cyber threats. Thus, the definition of cybersecurity for SMEs must incorporate strategies that are scalable and adaptable to the specific needs and constraints of these enterprises. The interdisciplinary nature of cybersecurity highlights the need for SMEs to adopt a multifaceted approach that includes not only technological solutions but also robust policies, employee training, and risk management practices [3] [6].

3.1.2 Cybersecurity Risk in SMEs

SMEs face a unique set of cybersecurity risks that differ in nature and scale from those encountered by larger organizations. These risks stem from various factors, including limited financial and human resources, lower levels of cybersecurity awareness, and a lack of formalised security policies and procedures. According to a study by Verizon, SMEs have largely become the target of cyber-attacks, where 43% of all cyber-attacks target small businesses. There is a framework for understanding cybersecurity risk within a multidisciplinary context, which can be applied to the specific challenges SMEs face [3] [22].

One of the primary risks for SMEs is the threat of data breaches. Due to their smaller scale, SMEs may not have the same level of protection as larger organizations, making them attractive targets for cybercriminals. Data breaches may lead to losing important information, including customer data, intellectual property, and financial records. The consequences of such breaches can be devastating for SMEs, leading to financial losses, legal liabilities, and reputational damage. Understanding the risk of data breaches requires not only technical knowledge of how breaches occur but also an awareness of how human behaviour, such as phishing attacks or weak passwords, can contribute to these incidents [3].

Another significant risk for SMEs is ransomware attacks, where cybercriminals encrypt an organization's data and demand payment for its release. SMEs are particularly vulnerable to ransomware because they may lack the resources to implement advanced security measures, such as regular data backups and robust encryption. Moreover, the financial impact of a ransomware attack can be more severe for SMEs, as they may not have the reserves to pay the ransom or the insurance coverage to mitigate the costs. The multidisciplinary approach discussed by Cains et al.

(2022) suggests that addressing ransomware risks in SMEs involves both technical defences, such as anti-malware software and firewalls, and organizational strategies, including employee training and incident response planning [3].

Phishing attacks also represent a significant cybersecurity risk for SMEs. These attacks, which involve deceiving employees into providing sensitive information or clicking on malicious links, exploit human vulnerabilities rather than technological weaknesses. SMEs, which often have fewer employees and less formalised security training programs, are particularly at risk. Cains et al. (2022) highlight the importance of considering psychological factors in understanding and mitigating phishing risks, as attackers often use social engineering techniques to exploit employees' trust and familiarity [3].

The specific cybersecurity risks faced by SMEs are further complicated by the broader context in which these businesses operate. For example, SMEs are often part of larger supply chains, and a security breach in one SME can have cascading effects on other businesses within the network. This interconnectivity increases the potential impact of cyberattacks and highlights the need for SMEs to secure not only their own systems but also consider the security practices of their partners and suppliers.

Moreover, the rapid pace of technological change presents an ongoing challenge for SMEs in managing cybersecurity risks. As new technologies are adopted, they often introduce new vulnerabilities that SMEs must address. For instance, the increasing use of cloud services, while offering many benefits, also raises concerns about data security and access control. SMEs must stay informed about emerging threats and continually adapt their cybersecurity strategies to address these risks.

In conclusion, the cybersecurity risks SMEs face are multifaceted and require a multidisciplinary approach to manage effectively. The definitions of cybersecurity provided by Cains et al. (2022) and Craigen, Diakun-Thibault, and Purse (2014) underscore the complexity of these risks and the need for SMEs to adopt a comprehensive approach that includes both technical solutions and a deep understanding of human and organizational factors. By recognizing the unique challenges, they face and leveraging the insights provided by multidisciplinary research, SMEs can better protect themselves against the ever-evolving landscape of cyber threats [3] [6].

One significant trend impacting SMEs is the rise of remote work. The COVID-19 pandemic accelerated the shift toward remote and hybrid working arrangements, which, while offering flexibility and continuity for businesses, also introduced new cybersecurity challenges. SMEs, which may not have the robust IT infrastructure of larger corporations, found themselves particularly vulnerable to cyber threats in a remote work environment. The use of personal devices, unsecured home networks, and cloud-based collaboration tools increased the attack surface for cybercriminals. As highlighted, remote work has blurred the boundaries between personal and professional spaces, making it more difficult for SMEs to enforce strict cybersecurity measures [3]

In this context, endpoint security has become a critical area of focus. Endpoint security refers to protecting individual devices, such as laptops, smartphones, and tablets, that connect to a business's network. Ensuring that these endpoints are secure is essential for SMEs, as any compromise can lead to broader network vulnerabilities. Implementing measures such as multi-factor authentication (MFA), virtual private networks (VPNs), and regular software updates can help mitigate these risks. The effectiveness of these measures depends not only on the technology itself but also on the users' understanding and adherence to security practices [6]

Another emerging concern for SMEs is the Internet of Things (IoT). IoT devices, which include everything from smart thermostats to industrial sensors, are increasingly being integrated into business operations. While these devices can enhance efficiency and productivity, they also introduce new vulnerabilities. Many IoT devices are designed with convenience in mind, often at the expense of security. They may lack basic security features, such as strong authentication mechanisms, and can be easily exploited by cybercriminals to gain access to a network. This presents a significant challenge for SMEs, which may lack the resources to thoroughly vet and secure every IoT device they use. Ensuring that IoT devices are properly configured, regularly updated, and isolated from critical systems is crucial in minimizing the associated risks.

The supply chain has also emerged as a critical area of concern for SME cybersecurity. SMEs often serve as suppliers or partners within larger supply chains, and a breach in one SME can have cascading effects throughout the entire network. This interconnectedness makes SMEs both targets and vectors for cyberattacks. Cybercriminals may target SMEs as a means of accessing larger organizations that they supply. As a result, supply chain attacks have become more common and sophisticated, with attackers exploiting vulnerabilities in third-party software, hardware, or

services to infiltrate networks. The SolarWinds attack in 2020, which compromised numerous organizations worldwide through a software supply chain, underscored the potential impact of such threats [8].

To address supply chain risks, SMEs must not only secure their own systems but also carefully assess the cybersecurity practices of their partners and suppliers. This involves conducting regular audits, establishing clear security standards for third parties, and incorporating cybersecurity clauses into contracts. By taking a proactive approach to supply chain security, SMEs can reduce the likelihood of being compromised through their business relationships.

3.1.3 The Role of Cybersecurity Culture in SMEs

Beyond technological solutions, developing a strong cybersecurity culture within SMEs is essential for effective cyber risk management. A cybersecurity culture refers to the collective mindset, behaviours, and practices related to cybersecurity within an organization. In SMEs, where resources may be limited, fostering a culture that prioritises cybersecurity can be a powerful tool for mitigating risks.

Cains et al. (2022) emphasize the importance of human factors in cybersecurity, noting that even the most sophisticated technical defences can be undermined by human error or negligence. For SMEs, where employees often perform multiple roles and may not have specialised cybersecurity training, building awareness and instilling good cybersecurity habits are crucial. This can be achieved through regular training programs that educate employees about common threats, such as phishing, social engineering, and ransomware, and how to recognise and respond to them [3].

Moreover, leadership plays a pivotal role in shaping cybersecurity culture. SME leaders must lead by example, demonstrating a commitment to cybersecurity through their actions and decisions. This includes allocating resources for cybersecurity initiatives, encouraging open communication about potential threats or incidents, and holding everyone in the organization accountable for their role in maintaining security. When cybersecurity is viewed as a shared responsibility across all levels of the organization, it becomes ingrained in the daily operations and decision-making processes of the business [6].

A strong cybersecurity culture also involves establishing clear policies and procedures that guide employee behaviour. These should cover areas such as password management, data handling, use

of personal devices, and incident reporting. SMEs should ensure that these policies are not only documented but also regularly reviewed and updated to reflect evolving threats and best practices. Additionally, it is vital to create an environment where employees feel comfortable reporting potential security issues without fear of retribution. This encourages a proactive approach to cybersecurity, where potential threats can be addressed before they escalate into serious incidents.

3.1.4 The Economic Implications of Cybersecurity for SMEs

While the importance of cybersecurity is evident, SMEs often face significant economic challenges in implementing and maintaining adequate security measures. The cost of cybersecurity tools, services, and expertise can be prohibitive for smaller businesses, which may already be operating on tight budgets. This financial constraint is a major barrier to the adoption of comprehensive cybersecurity strategies in SMEs.

However, the economic impact of a cyberattack can far outweigh the cost of preventive measures. According to a report by the Ponemon Institute, the average price of a data breach for small businesses can run into hundreds of thousands of dollars, including direct costs such as remediation and indirect costs such as reputational damage and loss of customers. For many SMEs, a significant cyber incident can be catastrophic, potentially leading to business closure [8].

To mitigate these risks, SMEs should consider cost-effective cybersecurity solutions that balance affordability and protection. This may include leveraging cloud-based security services, which offer scalable and flexible security solutions without the need for significant upfront investment in hardware or software. Additionally, SMEs can benefit from cybersecurity insurance, which can help cover the costs associated with a cyberattack, such as legal fees, notification costs, and business interruption.

Another important consideration is the return on investment (ROI) of cybersecurity initiatives. While it may be difficult to quantify the ROI of preventing an incident that has not occurred, investing in cybersecurity can protect SMEs from the potentially devastating financial consequences of a successful attack. Furthermore, a strong cybersecurity posture can enhance customer trust and confidence, providing a competitive advantage in an increasingly digital marketplace.

In conclusion, the economic implications of cybersecurity for SMEs are profound. While the cost of implementing effective security measures can be challenging, the potential consequences of inaction are far more significant. SMEs must carefully assess their cybersecurity needs and invest in solutions that provide the best possible protection within their budget constraints. By doing so, they can safeguard their operations, protect their reputation, and ensure their long-term success in the digital age.

3.1.5 Future Directions and Recommendations

Looking ahead, SMEs must continue to adapt to the changing cybersecurity landscape. As new threats emerge and technologies evolve, it will be essential for SMEs to stay informed and proactive in their cybersecurity efforts. This includes regularly updating security measures, staying aware of industry trends, and fostering a culture of continuous improvement.

One key area for future focus is the integration of artificial intelligence (AI) and machine learning into cybersecurity practices. These technologies have the potential to enhance threat detection and response by analysing vast amounts of data in real-time, identifying patterns, and predicting potential threats before they materialise. While AI-based solutions may currently be out of reach for many SMEs due to cost and complexity, advances in technology and increased availability of affordable AI tools are likely to make these solutions more accessible in the coming years.

SMEs should also consider collaborating with industry partners and government agencies to share knowledge, resources, and best practices. Collaborative efforts can help SMEs enhance their cybersecurity capabilities without bearing the entire burden alone. Participation in industry groups, cybersecurity forums, and government initiatives can provide valuable support and insights.

Finally, SMEs must remain vigilant about regulatory changes related to cybersecurity. As governments around the world introduce stricter data protection and cybersecurity regulations, SMEs will need to ensure compliance to avoid legal penalties and protect their reputation. This may involve investing in compliance management tools and seeking legal advice to navigate the complexities of cybersecurity regulations.

In conclusion, the future of cybersecurity in SMEs will require a dynamic and adaptable approach. By staying informed, investing in emerging technologies, and fostering collaboration, SMEs can

continue to protect themselves against evolving cyber threats and ensure their long-term success in an increasingly digital world.

3.2. Common Cyberattacks and Vulnerabilities Targeting SMEs

3.2.1 Types of Cyberattacks

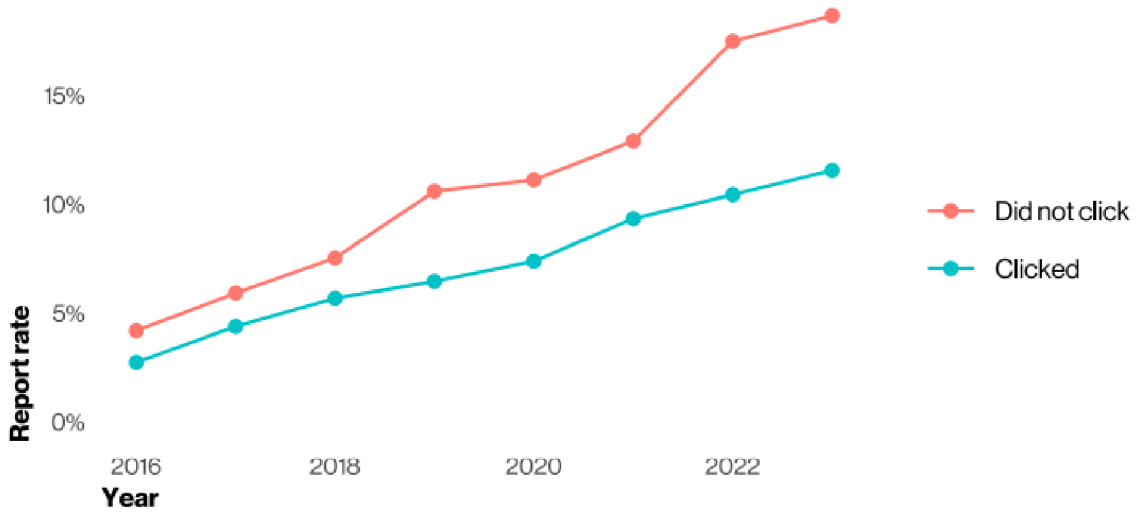
In today's digital landscape, the variety of cyberattacks continues to grow, posing significant threats to organizations of all sizes, particularly small and medium-sized enterprises (SMEs). Understanding the different types of cyberattacks is crucial for businesses to develop effective cybersecurity strategies. This section discusses the most common cyberattack vectors, including phishing, ransomware, malware, denial-of-service (DoS) attacks, and insider threats, among others.

3.2.1.1. Phishing Attacks

Phishing attacks represent one of the most prevalent forms of cyber threats targeting SMEs. In a phishing attack, cybercriminals masquerade as legitimate entities to deceive individuals into revealing sensitive information, such as login credentials or financial details. These attacks often occur via email but can also take place through text messages, social media, and other communication channels. Phishing emails typically contain malicious links or attachments designed to exploit vulnerabilities in users' systems [6].

The increasing sophistication of phishing techniques, such as spear phishing—where attackers tailor their messages to specific individuals or organizations—makes these attacks particularly dangerous. A successful phishing attack can lead to illegal access to company networks, resulting in data breaches, financial losses, and reputational damage. SMEs are often targeted because they may not have robust security measures in place, making them easier targets for cybercriminals [9].

Figure 1: Phishing email report rate by click status



Source:[19]

3.2.1.2 Ransomware

Ransomware has emerged as one of the most significant threats facing SMEs in recent years. This type of malicious software encrypts a victim's data, rendering it inaccessible until a ransom is paid to the attacker. Ransomware attacks can have devastating consequences for SMEs, often resulting in the loss of critical data and extended operational downtimes [8]

Cybercriminals frequently use social engineering techniques to deliver ransomware, often through phishing emails or compromised websites. Once the ransomware is installed, it can spread rapidly across the organization's network, affecting multiple systems. The decision to pay the ransom is fraught with ethical dilemmas and potential legal repercussions, and paying does not guarantee that the attackers will restore access to the data. Moreover, the growing trend of "double extortion," where attackers not only encrypt data but also threaten to leak sensitive information if the ransom is not paid, adds another layer of complexity to this issue [7].

3.2.1.3 Malware

Malware, short for malicious software, encompasses various types of harmful software designed to infiltrate, damage, or disable computers and networks. This category includes viruses, worms, Trojans, and spyware. Each type of malware has distinct characteristics, but they all share the common goal of causing harm to systems or stealing sensitive data [10].

For SMEs, malware infections can lead to significant operational challenges, including system failures and data loss. The complexity of malware threats has increased, with some sophisticated forms employing techniques such as obfuscation to evade detection by antivirus software. Regular updates to software and comprehensive security training for employees are critical for preventing malware infections.

3.2.1.4 Denial-of-Service (DoS) Attacks

Denial-of-Service (DoS) attacks are designed to overwhelm a network, service, or application, rendering it unavailable to users. Attackers achieve this by flooding the target with an excessive amount of traffic, effectively exhausting the resources needed to maintain normal operations. A Distributed Denial-of-Service (DDoS) attack amplifies this effect by using multiple compromised systems to launch the attack, making it even more challenging to mitigate [7].

For SMEs, a successful DoS attack can lead to significant financial losses and reputational damage. Extended downtimes can prevent customers from accessing services, resulting in lost sales and decreased customer trust. Mitigating DDoS attacks often requires sophisticated technology and expertise that may be beyond the reach of many SMEs, making them vulnerable to this type of threat.

3.2.1.5 Insider Threats

Insider threats pose a unique challenge for SMEs, as they involve individuals within the organization who may intentionally or unintentionally compromise security. These threats can arise from disgruntled employees, negligent staff, or even third-party vendors with access to the company's network. Insider threats can manifest in various ways, including data theft, unauthorised access to sensitive information, and unintentional introduction of malware [10].

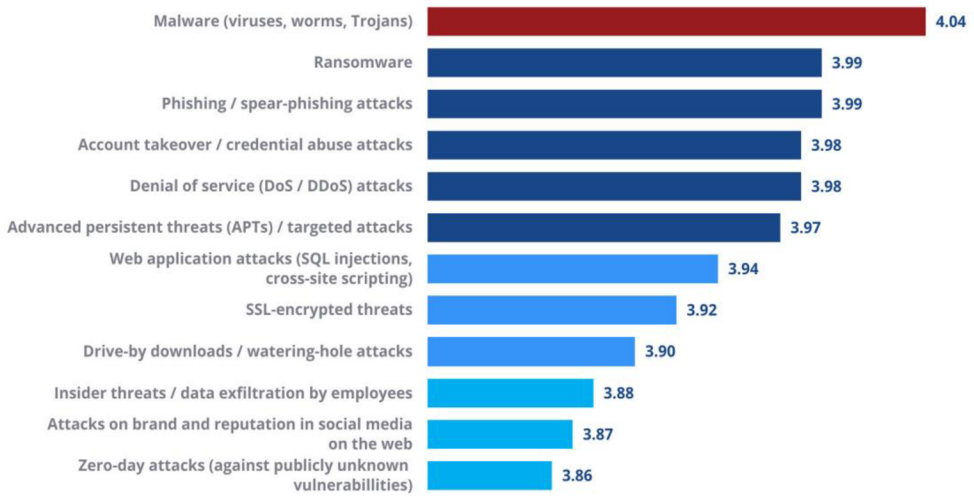
Unlike external attacks, insider threats can be more challenging to detect and prevent, as trusted individuals often have legitimate access to the systems they exploit. Organizations must implement

comprehensive access controls and regular monitoring to identify unusual behaviour that may indicate an insider threat. Cultivating a culture of security awareness among employees is essential to minimizing these risks.

3.2.2 Conclusion

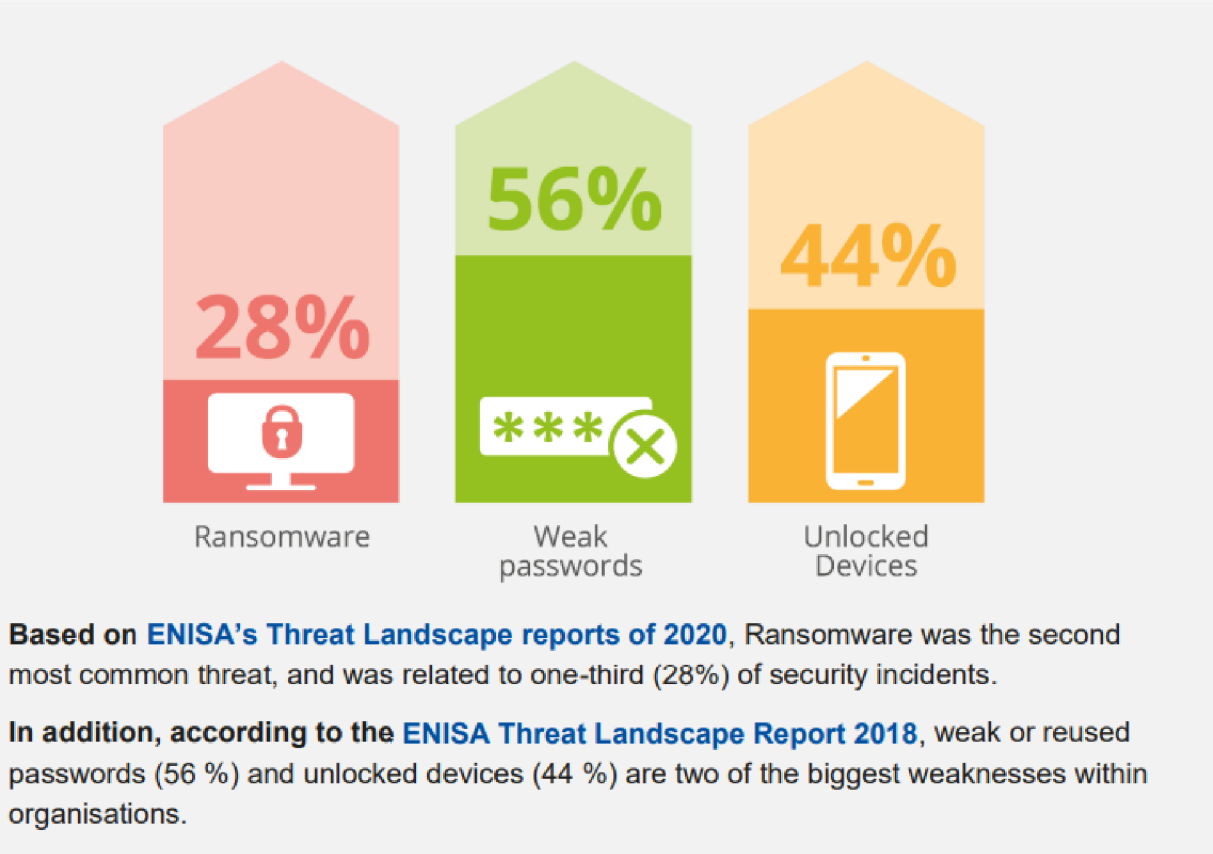
In summary, the landscape of cyber threats continues to evolve, and SMEs must remain vigilant to protect themselves against a diverse array of cyberattacks. From phishing and ransomware to malware, denial-of-service attacks, and insider threats, each type of cyber threat presents unique challenges that require tailored strategies for prevention and response. Understanding the nature of these attacks is critical for SMEs to enhance their cybersecurity posture, safeguard their data, and ensure business continuity in an increasingly digital world. Developing effective training programs and employing the latest security technologies can significantly mitigate the risks associated with these threats, empowering SMEs to navigate the complexities of the cybersecurity landscape with confidence.

Figure 2: Relative concern for cyber threats by type



Source: [17]

Figure 3: Cybersecurity threat landscape



Source:[14]

3.3 Vulnerabilities of SMEs

Small and medium-sized enterprises (SMEs) play a vital role in the global economy, driving innovation and job creation. However, these organizations are particularly susceptible to cyber threats due to various inherent vulnerabilities. This section explores the key weaknesses that SMEs face, including limited resources, lack of cybersecurity expertise, lower security budgets, insufficient security policies, and the challenges posed by remote work. Additionally, it integrates insights from Hasan regarding how these vulnerabilities influence the overall cybersecurity readiness of SMEs [11].

3.3.1 Limited Resources

One of the most significant vulnerabilities SMEs faces is their limited financial and human resources. Unlike large corporations that can allocate substantial budgets to cybersecurity, SMEs

often operate with constrained financial resources. This limitation affects their ability to invest in advanced security technologies, hire specialised personnel, and implement comprehensive training programs for employees. According to a survey by the Ponemon Institute (2020), 60% of SMEs reported that insufficient budget was a significant barrier to effective cybersecurity implementation [8].

Due to their resource constraints, SMEs may resort to using basic security measures, such as free antivirus software or minimal firewall protections, which often do not provide adequate defence against sophisticated cyber threats. When faced with competing priorities—such as business expansion, customer acquisition, or day-to-day operations—cybersecurity can take a backseat, resulting in neglected security practices. This lack of investment can lead to an increased vulnerability to cyberattacks, as attackers tend to target organizations that exhibit weaknesses in their defences [12].

3.3.2 Lack of Cybersecurity Expertise

Another critical vulnerability for SMEs is the lack of in-house cybersecurity expertise. Many SMEs do not have dedicated IT staff with specialised knowledge in cybersecurity, leaving them ill-equipped to identify, assess, and respond to potential threats. The rapidly evolving nature of cyber threats further exacerbates this issue, as keeping up with the latest security trends and best practices requires continuous education and training. A report from Cybersecurity Ventures indicates that the cybersecurity skills gap is projected to leave 3.5 million positions unfilled by 2025, further complicating the situation for SMEs [14].

SMEs may struggle to implement effective security policies and practices without the necessary expertise. For instance, they may not conduct regular security audits or vulnerability assessments, which are essential for identifying their systems' weaknesses. Moreover, the absence of cybersecurity professionals can hinder the development of incident response plans, making it difficult for SMEs to react swiftly and effectively in the event of a breach. This lack of preparedness can lead to prolonged downtimes and significant financial losses when cyber incidents occur.

3.3.3 Lower Security Budgets

Budget constraints play a crucial role in shaping the cybersecurity posture of SMEs. Many SMEs allocate a minimal portion of their overall budget to cybersecurity, often viewing it as an expense rather than a critical investment in their business continuity. This mindset can result in the adoption of subpar security measures that fail to protect sensitive information and critical infrastructure adequately. A survey conducted by the National Cyber Security Centre (2020) found that only 20% of SMEs have a dedicated cybersecurity budget.

Research has highlighted that the limited budgets of SMEs often lead to a reactive rather than proactive approach to cybersecurity. SMEs may only invest in security solutions after experiencing a cyber incident, which can be too late to mitigate the damage effectively. This reactive mindset further compounds their vulnerabilities, as it prevents them from building a robust cybersecurity framework that addresses potential risks before they materialise [15].

Moreover, the cost of implementing effective security measures can deter SMEs from taking action. The high costs associated with cybersecurity technologies, including firewalls, intrusion detection systems, and employee training programs, can be overwhelming for organizations operating on tight margins. As a result, many SMEs may delay essential cybersecurity investments, leaving them exposed to an array of cyber threats.

3.3.4 Insufficient Security Policies

Many SMEs lack formal cybersecurity policies, which can lead to inconsistent security practices and increased vulnerabilities. A well-defined cybersecurity policy establishes guidelines for data protection, incident response, and employee responsibilities, ensuring that all staff understand their role in maintaining security. However, a survey by the European Union Agency for Cybersecurity found that over 40% of SMEs do not have a cybersecurity policy in place [14].

The absence of such policies can result in employees being unaware of best practices for cybersecurity, making them more susceptible to social engineering attacks. Additionally, without clear procedures for reporting incidents, SMEs may struggle to respond effectively when breaches occur, leading to delayed mitigation efforts and exacerbating the attack's impact.

3.3.5 Challenges Posed by Remote Work

The rise of remote work has introduced new vulnerabilities for SMEs, particularly in the wake of the COVID-19 pandemic. While remote work offers flexibility and potential cost savings, it also increases the risk of cyber threats. Employees working from home may use personal devices and unsecured networks, making it easier for cybercriminals to gain access to corporate data. A report by IBM indicated that 70% of organizations experienced increased cyberattacks because of the shift to remote work [16].

The lack of oversight and control over home networks can lead to significant security gaps. Furthermore, employees may not adhere to the same security protocols when working remotely, increasing the risk of inadvertent data breaches. To mitigate these challenges, SMEs must develop remote work policies that emphasize security best practices, provide necessary training, and ensure that employees have access to secure tools and resources.

3.3.6 Influence on Cybersecurity Readiness

The inherent vulnerabilities of SMEs collectively contribute to a low level of cybersecurity readiness. As indicated by Hasan et al. (2021), this lack of preparedness can have profound implications for the overall security posture of these organizations. Cybersecurity readiness refers to an organization's ability to anticipate, withstand, and recover from cyber threats, and it is influenced by factors such as security policies, employee training, and incident response capabilities [15].

For SMEs, the combination of limited resources, lack of expertise, and lower security budgets creates a perfect storm that undermines their cybersecurity readiness. Many SMEs lack formal cybersecurity policies, leaving employees uncertain about their roles and responsibilities in maintaining security. Additionally, without ongoing training and awareness programs, employees may fall victim to social engineering attacks, inadvertently compromising the organization’s security.

Furthermore, the absence of incident response plans can hinder SMEs' ability to recover from breaches effectively. When a cyber incident occurs, organizations that have not prepared adequately may struggle to contain the damage, leading to extended downtimes and increased costs associated with recovery efforts. According to a study by the Ponemon Institute (2020), the average

cost of a data breach for SMEs can reach up to $3 million, highlighting the financial impact of inadequate cybersecurity preparedness [8].

3.3.7 Conclusion

In conclusion, the vulnerabilities inherent to SMEs—including limited resources, lack of cybersecurity expertise, lower security budgets, insufficient security policies, and challenges posed by remote work—significantly impact their overall cybersecurity readiness. The findings from Hasan et al. (2021) underscore the need for SMEs to prioritize cybersecurity as a fundamental aspect of their operations rather than viewing it solely as an expense. By adopting a proactive approach to cybersecurity, investing in employee training, and developing comprehensive security policies, SMEs can strengthen their defences against cyber threats and enhance their resilience in an increasingly complex digital landscape. Addressing these vulnerabilities is essential for empowering SMEs to thrive while safeguarding their sensitive information and ensuring business continuity in the face of evolving cyber risks [15].

3.4. Operational Disruptions Caused by Cyber-Attacks on SMEs

Cyberattacks have become increasingly prevalent, posing significant risks to small and medium-sized enterprises (SMEs). The consequences of these attacks extend far beyond financial losses, deeply affecting the operational capabilities of these organizations. This section analyses how cyberattacks disrupt the operations of SMEs, exploring operational challenges such as downtime, loss of productivity, and damage to reputation. Furthermore, this analysis includes case studies of SMEs that have experienced significant operational disruptions due to cyberattacks, illustrating the real-world implications of cyber threats.

3.4.1 Impact on Operations

The impact of cyberattacks on SMEs can be devastating, leading to substantial disruptions in daily operations. When an SME experiences a cyber incident, the immediate effects often manifest as system downtime, which refers to the period during which critical business operations are halted. System downtime can arise from various incidents, such as ransomware attacks, where access to data and systems is blocked until a ransom is paid. According to the Cybersecurity and Infrastructure Security Agency, the average downtime for businesses affected by ransomware

attacks can range from a few days to several weeks, depending on the severity of the incident and the organization's response capabilities [7].

The disruption of operations can result in significant loss of productivity. Employees may be unable to perform their usual tasks, leading to delays in service delivery and project completion. For SMEs, which often operate with limited staff, even a minor disruption can have a cascading effect on overall productivity. A study by the Ponemon Institute (2020) found that the average cost of downtime due to a cyber incident for SMEs can exceed $100,000, a significant amount for organizations with limited financial resources. This financial strain can hinder growth opportunities and lead to a loss of competitive advantage in the marketplace [8].

3.4.2 Financial Consequences

The financial implications of cyberattacks extend beyond immediate operational disruptions. In addition to the costs associated with downtime, SMEs may face significant expenses related to recovery efforts. These expenses can include hiring external cybersecurity experts to investigate and remediate the incident, restoring systems and data, and implementing additional security measures to prevent future attacks. A report by CyberEdge Group indicates that 59% of SMEs that experienced a cyberattack reported incurring costs related to recovery that exceeded their initial cybersecurity budgets [17].

Moreover, SMEs may also experience long-term financial consequences as a result of diminished customer trust and loyalty. Following a cyber incident, customers may hesitate to engage with the affected business, fearing for the security of their personal information. This decline in customer trust can lead to reduced sales and revenue, further exacerbating the financial impact of the breach. According to a survey conducted, 87% of consumers stated that they would take their business elsewhere if they found out their data had been compromised [18].

3.4.3 Damage to Reputation

In addition to operational and financial disruptions, cyberattacks can inflict significant damage to an SME's reputation. The public perception of a business can be drastically altered following a breach, as stakeholders, customers, and partners become concerned about the organization's ability to safeguard sensitive information. Rebuilding trust after a cyber incident is a challenging process that often requires extensive public relations efforts and communication strategies.

The reputational damage incurred by an SME can have long-lasting effects. Customers may choose to sever ties with the organization, and potential clients may be deterred from engaging due to security concerns. A case study conducted highlights that 43% of SMEs experienced a decrease in customer loyalty following a cyber incident, illustrating the lasting consequences that can arise from compromised security [19].

3.4.4 Case Studies

The following case studies showcase real-world examples of SMEs that have faced significant challenges post-breach to illustrate further the operational disruptions caused by cyberattacks.

Case Study 1: Wire fraud attack on a boutique hotel

A boutique hotel was a victim of a bank transfer scam after its CEO unknowingly gave cybercriminals the login credentials. The incident started when the CEO received what appeared to be an official email from the IRS (Internal Revenue Service), prompting them to click a link and enter their credentials. The consequences were grave as the attackers made unauthorised transfers of over $1 million to an overseas account. As a result of the breach, the hotel hired a cybersecurity firm to assess the damage and prevent future incidents. However, no funds were recovered, and the hotel's cash reserves were drained entirely. Unfortunately, the email was a phishing scam, allowing hackers full access to the hotel's financial accounts. This attack exposed critical vulnerabilities in the hotel's cybersecurity practices [21].

Takeaways include:

- Employee Awareness is Crucial: The CEO fell for the phishing scam, highlighting the need for ongoing cybersecurity training for all staff to recognise fraudulent emails and suspicious links.
- Stronger Financial Safeguards: The hotel lacked secondary verification for wire transfers. Implementing a process requiring dual approval for large transactions could have prevented this loss.
- A Cyber Incident Response Plan is Essential: Without a clear action plan, the hotel was unprepared to quickly detect and respond to the breach [21].

Case Study 2: Phishing attack on a government contracting firm

A government contracting firm faced a major cybersecurity problem when its CEO was alerted that company data was being sold on the dark web. The leaked data supposedly included sensitive information about military clients, but after investigation, the data turned out to be outdated and unrelated to government agencies. The breach happened because a senior employee had unknowingly downloaded a malicious email attachment, believing it came from a trusted source. This phishing attack installed malware, compromising company data. The IT team immediately shut down the affected server and conducted a full cybersecurity scan, and a cybersecurity forensics firm was hired to investigate the extent of the breach. Government agencies that could have been impacted were notified, and the U.S. Secret Service assisted in the investigation [21].

The impact of the Attack was that the breach had serious financial and operational consequences, costing the company over $1 million in damages. Some losses included several days of downtime and disruption of business operations. In addition to that, there were expenses for new security software licenses and server replacements [21].

Lessons Learned:

- No business is too small to be a target: Cybercriminals attack companies of all sizes.
- Employee training is critical: Staff must be able to recognise phishing emails and suspicious links.
- Strong security measures are essential: Installing and updating antivirus software, firewalls, and encryption tools helps prevent malware infections.
- Regular cybersecurity testing: Ongoing vulnerability assessments help identify weak points before they're exploited [21].

Case Study 3: Staff Negligence

A hardware store faced a significant business disruption after an employee ignored internal cybersecurity policies and clicked a malicious email attachment. The next day, the store's cash registers, and stock ordering system began to fail, causing significant operational downtime. The attack resulted in $178,000 in damages, including:

- $18,000 in extra staff costs to restore the network.
- $50,000 in lost revenue due to business interruptions.

- $110,000 in cybersecurity response expenses, including forensic investigations and an incident response manager [23].

Lessons Learned:

- Regular cybersecurity training is necessary to prevent the staff from falling for phishing attacks.
- Access to sensitive information should be restricted, and only authorised personnel should have access to important business systems.
- Investing in educating the staff and strict internal policies can help prevent costly incidents like this [23].

Case Study 4: Cyber Fraud at Advanced Electrical Varnishes Ltd (AEV)

Data breaches of large enterprises often make headlines in the news, and this deceives the owners and employees of SMEs to think that they are not as vulnerable as the big companies. In 2014, Advanced Electrical Varnishes Ltd (AEV), a UK-based manufacturing firm, learned this the hard way when a malware attack led to the theft of $30,000 and €100,000 from their company bank account. AEV is known for manufacturing and supplying superior varnishes and insulating products made for electronic and electrical businesses worldwide. They are based in Birkenhead but have several other branches in Spain, Italy, and Malaysia. This breach happened in the UK branch. AEV's systems became infected with malware, which altered the appearance of their online banking platform. When the financial controller logged in, they were prompted to enter the full PIN for the company account, something the bank would never usually ask for. Trusting the system, the employee entered the information, unknowingly handing over full access to cybercriminals. Within three minutes, large sums were transferred to accounts in Ukraine and Cyprus. Recovering the stolen funds was a long and challenging process, taking four months and requiring the intervention of Members of Parliament. Initially, the bank refused to reimburse AEV, arguing that the employee had violated banking terms by entering the full PIN. It was only through the determination from AEV's director, Jonathan Kemp, and cybersecurity experts that the funds were eventually recovered [24].

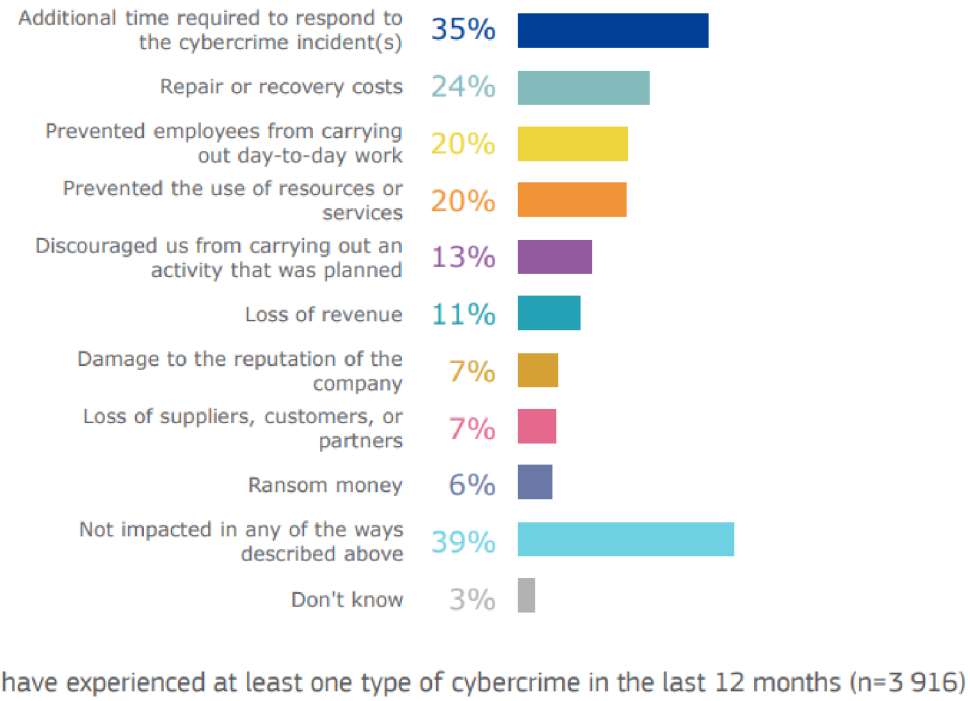
Lessons Learned:

- Human error is a significant cybersecurity risk, and any employee can fall victim to scams, making training essential.
- Technical controls add an extra layer of security, requiring multiple people's approval for high-value transactions, could have prevented this attack [24].

3.4.5 Conclusion

The operational disruptions caused by cyberattacks on SMEs are profound, encompassing significant financial, operational, and reputational consequences. These disruptions can result in extended downtimes, loss of productivity, and long-term damage to customer trust and business reputation. The case studies presented illustrate the real-world implications of cyber threats, highlighting the need for SMEs to prioritise cybersecurity as an essential component of their operational strategy. By adopting proactive security measures, investing in employee training, and developing comprehensive incident response plans, SMEs can enhance their resilience against cyber threats and mitigate the operational challenges that arise in the wake of cyber incidents.

Figure 4: Different impacts on SMEs



Source:[20]

4. Practical part

4.1. Introduction

This thesis's practical part will be to develop a strategy aimed at safeguarding the private data of small and medium enterprises against cyber threats. This will be achieved by using a hypothetical case study: La luna supermarket. La Luna Supermarket will act as a representative model of the cybersecurity challenges faced by SMEs. Supermarkets are a good example of SMEs facing cybersecurity threats due to their high customer traffic, reliance on point-of-sale (POS) systems, and significantly increased use of digital payment methods. This hypothetical scenario is based on real case studies of cybersecurity breaches in similar businesses, as detailed in Chapter 3, to create a realistic context for our analysis.

La Luna supermarket faces common vulnerabilities such as limited resources allocated to cybersecurity, lack of awareness among staff regarding cybersecurity practices, and insufficient security policies. These vulnerabilities are worsened by the fast implementation and use of digital technology, but without proper security.

In this chapter, we will first discuss a hypothetical profile of La luna supermarket including its background, technical infrastructure, data handling, and assumed current security measures. Following this, based on the identified weaknesses and drawing upon best practices and the theoretical part of this thesis, we will propose a comprehensive cybersecurity strategy. The strategy proposed will include infrastructure enhancements, data protection measures, and policy initiatives, all will be carefully tailored to the specific needs and resource limitations typically encountered by SMEs. Finally, a cost-benefit analysis will explore the potential return on investment from these cybersecurity improvements for businesses like La Luna. The ultimate aim of this hypothetical case study will be to provide a practical and adaptable cybersecurity framework that other SMEs can implement to enhance their protection against cyber threats.

4.2. Hypothetical profile

In this section, we will list in detail the hypothetical characteristics of La luna supermarket.

A. Background:

La Luna Supermarket is a medium-sized grocery store located in Kigali, Rwanda. It has been serving the local community for approximately ten years and has an established loyal customer base. The supermarket has 50 individuals, including cashiers, stock clerks, administrative staff, and management. La Luna has a significant role in the local economy and is striving to modernise its operations to remain competitive. However, like many SMEs, because cybersecurity has not been a primary focus, this has led to potential vulnerabilities.

B. Technical Infrastructure:

La Luna's technical infrastructure is functional for its daily operations; however, it reflects the typical limitations and weaknesses often seen in SMEs:

Point-of-Sale (POS) Systems: Ten POS terminals are placed at the checkout counters. These terminals run a standard POS software package (for example, a system called "RetailPro"). This software has several versions behind the current release. The POS terminals are connected via a local network, which is also used for other business functions.

Inventory Management: Inventory control is managed through a combination of spreadsheets and a basic, locally hosted database. Data backups, when performed, are not frequent and are stored on a USB drive kept in the office.

Office Network: A small office network connects the administrative computers used for tasks like accounting, payroll, and email communication. This network uses a basic router provided by the internet service provider and lacks advanced security features like intrusion detection or a robust firewall. The Wi-Fi network is used by both staff and guests and is secured with a simple password.

Antivirus: Some computers have basic, free antivirus software, but these installations are often outdated, and not all systems are protected.

Firewall: A basic firewall is provided by the internet service provider, but it is not configured and lacks advanced features like intrusion detection or application control

C. Data Handling:

La Luna handles various types of data, each with its level of sensitivity. Sensitive data is not separated from less sensitive data. All data is located on the same server within the office, often

within the same databases or file systems. This lack of data segregation makes it a significant vulnerability.

Customer Data: Personal information such as names, phone numbers, and email addresses is collected from loyalty program members and is subject to Rwandan data protection regulations.

Financial Data: The POS and inventory management systems generate and store sales data, transaction records, and financial statements. This data is crucial for business operations and must be protected from manipulation or theft.

Inventory Data: Data related to stock levels, pricing, and supplier information is managed in the inventory system. This data is vital for efficient operations.

Backups: Data backups are infrequent, manual, and stored on a USB drive kept in the office. This makes them vulnerable to theft, damage, or ransomware attacks.

D. Policies:

La Luna's current security measures are assumed to be basic and inadequate, representing the common situation in many SMEs:

Policies: No formal, written security procedures are in place. Cybersecurity awareness training is non-existent, and hence, many employees face phishing attacks but don't recognise them.

Password Management: Most employees either use weak, easily guessable passwords or share passwords among themselves.

Personal device usage: Employees can use their personal devices (phones, laptops…, etc.) for work purposes.

4.2.1 Simulated cyberattack: Ransomware attack

To illustrate the impact of poor cybersecurity, a ransomware attack on La Luna supermarket was simulated.

Scenario:

A cashier at La Luna supermarket received an email that seemed to be a supplier invoice. The email was well written, appearing to come from a trusted supplier, and included an attached file

named 'Invoice-January2025.pdf'. Unaware of the threat, the cashier opened the file, which installed ransomware on the computer. All the company data, including customer details, transaction history, and inventory records, were encrypted within minutes. Employees could no longer access the POS system, leading to a total shutdown of sales operations. Later, a message appeared on all computers stating that 'your files have been encrypted. To recover them, send $30,000 to the following Bitcoin wallet within 72 hours. If you fail to do so, it will result in permanent data loss.' Panic spread among the staff, and management had to decide whether to pay the ransom or attempt recovery. Without recent backups, La Luna was at risk of losing years of business data.

The ransomware was identified as some variation of Ryuk, specializing in small to mid-sized businesses. It locked files with AES-256 encryption and took advantage of outdated systems on La Luna computers that missed important security updates.

Consequences:

-Financial loss: Estimated downtime costs La Luna $2,000 - $5,000 daily in lost sales, with total losses reaching $70,000 in ransom, lost sales, and recovery expenses.

-Operational disruption: POS systems and inventory management don't function.

-Reputational damage: Customers lose trust, which reduces long-term income.

Mitigation Strategy: Implementing data backups, strong access controls, and an incident response plan could have minimised the damage.

4.3. Strategy

The main contribution of this thesis is to develop a practical cybersecurity framework that SMEs can adopt to strengthen their security by proposing a set of measures they can take in addition to their current security measures.

A. Infrastructure enhancements

USB Port Locking: To prevent unapproved devices, La Luna Supermarket's computers will have their USB ports locked so that only the approved flash drives will work. This will reduce the risk of external flash drives being connected to computers to extract data, and hence keep data safer.

Regular Software Updates: La Luna supermarket will have to implement regular upgrades of software as soon as it is released, such as POS software and antivirus software, as well as all other software for computers, phones, or other machines used. It is proposed that there should be a specific schedule, i.e., to be done at least once a month, and that the updates be made strictly to reduce attacks and system failures.

Firewall Appliance: Instead of just an Internet Service Provider Firewall, which is useful but not sufficient, it is proposed that La Luna supermarket should enhance its security by investing in a Next-Generation Firewall such as Fortinet FG series or Palo Palto Network PA series. It provides more advanced features like packet inspection, application control, intrusion prevention, and often integrated threat intelligence. This will help in controlling network traffic and better detection of attacks.

Secure WIFI for Staff: If La Luna wishes to offer WIFI to clients, it should be different from the one used by the staff and with a different router. The staff's WIFI should be secured with strong, unique passwords and be isolated from the internal business network (where POS systems, servers, etc., are found). Furthermore, it is recommended that MAC address filtering should be implemented. The administrator will create a list of allowed or blocked devices to control which can connect to the network. Also, it is suggested that the staff network should have limited bandwidth to prevent it from being used for non-business purposes.

IP whitelisting and Geofencing: It is endorsed that La Luna should apply IP whitelisting and geofencing to prevent illegal access to sensitive business data. IP whitelisting will grant only company-approved devices access to the database, reducing the risk of remote attacks. Geofencing adds another layer by blocking access from high-risk countries known for cybercrime. This is important for La Luna because SMEs are often targeted by international cybercriminals who want to exploit weak security systems.

Antivirus software: Bitdefender GravityZone Business Security Premium is recommended because it provides advanced ransomware protection and network attack prevention. Compared to Kaspersky Endpoint Security, Bitdefender offers better performance in detecting zero-day vulnerability, making it suitable for SMEs like La Luna. Additionally, Bitdefender provides central management, which grants La Luna to control all devices from a single dashboard.

Zero Trust Architecture: This is a security framework that supposes that no user or device should be trusted by default. So, it requires first requesting to be authenticated through multi-factor authentication and be approved before granting access to any resource. This prevents both external and internal threats due to strict access control.

AI Threat Detection: This analyses network activity and identifies and responds to threats in real-time. It uses machine learning and behavioural analysis to detect suspicious behaviour, like unauthorised access and unusual data transfers. To enhance security, SMEs could implement AI threat detection because it acts as a guard by blocking phishing emails, isolating infected computers, and stopping the attacks before they become serious problems. An example is Darktrace.

B. Data protection measures

Data Division: This includes separating sensitive data such as financial and payment card data from less sensitive data like names of products. This means creating separate database systems or file systems for different types of data. For example, financial data is stored in one database, inventory data is stored in another database, and so on. This practice will help to reduce the vulnerability of sensitive data as it will be given stricter security and specific access control.

Real-Time Backup: This means automatically backing up data as soon as it is created or edited, ensuring that the small updates are always updated. This is an advantage to weekly or monthly backups because it removes the risk of data being lost between backup intervals. It is also a good choice for La Luna supermarket because La Luna is an active environment where data is frequently updated and created, so it will minimise data loss because each change in data is backed up instantly.

Access Control: Strong access controls should be implemented to restrict access to sensitive data. Different user accounts with appropriate permissions should be created for various roles. Employees will only have access to the information and systems they need. For example, a cashier can only access the checkout system, not financial reports. This will reduce the risk of insider threats and limit data exposure if an account is hacked.

Read-Only Memory (ROM): ROM can be used to store the BIOS/UEFI firmware that initiates the boot process. Hence, it will ensure that only trusted operating systems load and block any malware

injections at startup. Moreover, as ROM is not easily modified, it can be stored in devices like routers and firewalls to store security protocols.

C. Policy initiatives

Enforcing strong passwords: Most employees at La Luna use weak passwords, which represents a big threat because it's easy to hack them. It is advised that they set passwords to passwords with at least 12 characters, at least one capital letter, at least one number, and at least a special symbol. Passwords shouldn't be easily guessable, such as names of a person or other personal information like birthdays, common words, and must be different from their previous passwords.

Multi-factor Authentication: This involves making hacking harder by requiring users to verify their identity through multiple authentication methods. To access the account, a user will be asked something in addition to a strong password. For example, a user will be required to enter a code he received via SMS or an authenticator app, a fingerprint, or biometric recognition, especially for high-sensitivity data.

Awareness training**:** The training should aim to educate employees to identify and respond to threats as soon as possible and efficiently. To measure the effectiveness of the training, employees should be given a test, such as random phishing stimulation tests to see how they respond. Those with the lowest marks should do continuous tests until they succeed. The training should be regular, for example, monthly or as needed. It would be best if trainings are also role-specific in addition to general knowledge. Each role should have a specific role-based module, for instance, managers on data access, cashiers focus on POS security, and general knowledge. The training should always be updated to cover new threats and trends. The human factor plays a big role in cybersecurity threats and vulnerabilities like phishing attacks, so training is critical to reduce human error.

Restriction of the use of personal devices: This will reduce the risk of data breaches because personal devices are hard to monitor. It will also prevent employees from copying and sharing the company's data on their personal devices and prevent ex-employees from keeping confidential information when they leave the company.

Incidence response plan: La Luna supermarket should have a basic incident response plan in case an attack happens. This plan should include detecting and identifying threats, stopping the threat

from spreading, removal of threats, restoring normal operations, lessons learned, and future prevention.

The proposed strategy gives the following advantages:

- Enhanced Cybersecurity Protection: It reduces vulnerabilities against cyberattacks such as phishing, ransomware, and data breaches.
- Minimise financial Losses: It reduces losses through disabling cyber threats, which in turn results in uninterrupted sales.
- Cost-Effective Security Measures: It seeks to implement security upgrades under SMEs' budget constraints, thus offering a high return on investment.
- Improved Customer Trust: It enhances company's reputation by protecting its customers' data.
- Reliable system: fewer disruptions and steady performance.

The table below consolidates the findings from our analysis and summarises the cybersecurity threats SMEs face and their vulnerabilities, their impact, and recommended prevention strategies. This table is an accessible guide for SMEs to consolidate and strengthen their cybersecurity:

Table 1: A framework for SME cybersecurity defence

Identified cyber-attack / SME vulnerability	**Disruption level (Small, Medium, Large)**	**Preventive strategy**
Phishing attack	Medium: loss of access to systems, risk of stolen login credentials.	Employee awareness training, AI threat detection, multi-factor authentication, Usage of strong and unique passwords.
Ransomware attack	Large: Significant financial loss, complete operational shutdown, data loss.	Real-time backup, AI threat detection, robust firewall, and regular software updates.
Malware	Medium: Compromised data quality, system slowdown, data theft.	Strong antivirus software (Bitdefender), USB port-locking, regular software

		updates, using Read-only Memory (ROM) to protect UEFI/BIOS firmware.
Denial-of-Service (DOS) attacks	Medium: Temporary operational disruption, loss of sales, reduced productivity, customer frustration.	Robust firewall (Next-Generation), IP whitelisting, geofencing, secured Wi-Fi.
Insider threats	Medium to Large: Financial loss, data loss, sabotaged systems, Reputation damage.	Strict access control, restriction of personal devices, zero trust architecture.
Weak passwords and poor access control	Medium: Unauthorised access, data breaches, risk of financial theft.	Multi-factor authentication, Strong password policy (length, complexity, expiration).
Outdated software systems	Large: Taking advantage of unaddressed vulnerabilities, malware infections, and system failures.	Adopt a strict software update schedule and regular review of system integrity.
Unsecured network (Wi-Fi, network intrusion due to weak firewall)	Medium: Unauthorised access, data breaches, denial-of-service attacks.	Secured Wi-Fi with strong passwords and encryption, implement modern firewall (Next-Generation), geofencing, IP whitelisting, zero trust architecture
Unseparated data	Large: sensitive data exposure and data breaches, loss of customer trust.	Data division, stricter access control to sensitive data.
Limited financial resources	Medium: Failure to establish security defences, delayed	Explore affordable but efficient solutions and prioritise security needs.

	action in addressing security threats.	
Lack of cybersecurity expertise and policies	Medium: The growing threat of phishing, social engineering, and attacks caused by human mistakes	Regular employee training with assessments, and development of clear security policies.

Source: Author

4.4 Implementation Phase

The strategy is designed to be implemented in three phases to accommodate limited resources and enable gradual improvement:

Phase 1: Immediate (0-30 days)

Regular software updates

Employee awareness training

Real-time data backup implementation

Data classification to identify sensitive and non-sensitive data

Basic firewall configuration

Strong password policy enforcement and multi-factor authentication

Phase 2: Short-term (1-3 months)

Set up of antivirus software on devices

Network segmentation implementation

Separate sensitive data and non-sensitive data

Access control policies

Next-generation firewall implementation

Incident response planning

USB port locking

IP whitelisting

Geofencing

Phase 3: Long-term (3-6 months)

Zero Trust Architecture

AI threat detection

Establish a real-time backup system

This phased approach allows SMEs like La Luna to prioritise the most critical security measures while planning for protection over time.

4.5 Cost-Benefit Analysis

4.5.1 Introduction

Implementing these cybersecurity measures requires financial investment, but the potential cost of a cyberattack far outweighs these expenses. This section will present a cost-benefit analysis to explain the proposed cybersecurity improvements at La Luna Supermarket. The costs are based on real-world pricing from cybersecurity vendors, while the potential losses are estimated from reports on SME cyber breaches.

4.5.2 Cost-Benefit Analysis of Cybersecurity Implementation Table

Table 2: Cost-Benefit Analysis of Cybersecurity Implementation for La Luna Supermarket

Cybersecurity measure	Estimated cost (annual)	Potential benefit	Sources
Antivirus software (AVG antivirus business edition)	939.8$ for 20 devices	Protects against malware and viruses, reducing potential	[25]

		downtime and preventing data loss.	
Firewall and network security (Next-Generation Firewall (Fortinet FG-100F)	Approximately $2,075.99 for hardware	Improves network performance, strengthens security, and prevents unauthorised access	[26]
Ransomware protection (Bitdefender GravityZone Business Security)	$811.99 for 15 devices	It has automated threat detection, stops harmful traffic, and prevents harmful code from being added to your system.	[27]
Cloud Backups (Acronis cyber protect)	$595	Ensures there is recovery of data in case of breaches, hence minimizing operational disruptions.	[28]
Incidence response plan and simulation (Sophos threat response)	€5,256	It offers complete security monitoring, threat detection, and incident response, including root cause analysis, a response expert, and breach protection assurance.	[29]
Employee cybersecurity training (KnowBe4)	$500 for 50 users	It contains simulated phishing tests, security awareness courses, and training	[30]

		programs that engage employees.	
Total estimated annual cost	$10178.78		-
The potential cost of a cyberattack on SMEs	$25,000 to $3 million	-	[31]
Return On Investment	Minimum potential loss scenario ($25,000 attack cost) = 145.61% Money saved: $25,000 - $10,178.78 = $14,821.22 Maximum potential loss scenario ($3,000,000 attack cost) = 29,373.08% Money saved: $3,000,000 - $10,178.78 = $2,989,821.22	Minimum potential loss scenario: For every $1 spent on cybersecurity, SME will save $1.46 in potential losses. Maximum potential loss scenario: For every $1 spent, you save $293.73 in potential losses.	-

Source: Author

4.5.3. Conclusion of Cost-Benefit Analysis

Investing in cybersecurity measures for small and medium-sized enterprises (SMEs) provides a good return on investment (ROI). In a scenario where a cyberattack costs around $25,000, an SME could save $14,821.22 by spending $10,178.78 on cybersecurity, resulting in a return of 145.61%. In a more severe situation where a cyber-attack costs up to $3 million, the SME could save $2,989,821.22 with an ROI of 29,373.08%.

This cost-benefit analysis showed that the benefits of investing in cybersecurity outweigh the costs, especially considering the potential for massive losses if a cyberattack occurs. Cybersecurity is not just another expense for the business but an essential investment in safeguarding operations, securing data, and preventing financial damage.

For SMEs, investing in cybersecurity measures like antivirus software, firewall and network security, ransomware protection, cloud backups, incident response, and employee training is vital to reduce risks and ensure long-term business success.

5. Conclusion and future research directions

5.1 Summary of Key Findings

The growing prevalence of cyber threats has emphasized the urgent need for small and medium-sized enterprises (SMEs) to implement robust cybersecurity measures. During this literature review, some key findings were brought to light regarding the cybersecurity landscape for SMEs. First, SMEs are particularly vulnerable to cyberattacks due to their limited resources, lack of cybersecurity expertise, and lower security budgets. These vulnerabilities significantly affect their overall cybersecurity readiness, making it essential for SMEs to adopt proactive strategies to safeguard their operations [15]

Additionally, there has been diversification in types of cyberattacks that target SME, phishing, ransomware, and malware being among the most common threats. These attacks do not only disrupt the operations of SMEs but also have long-lasting repercussions that may involve reputational damage and financial loss. The operational disruptions caused by cyber incidents also indicate the great importance of not only preventing attacks but also of having effective plans in place to mitigate the impact when breaches do occur [3]

The review also underscored employee training and awareness, as highly important as employees hold a significant place between prevention and response when it comes to cyber incidents. Such training is necessary for building up a culture of cybersecurity awareness and vigilance of threats within the organization.

5.2 Gaps in the Literature and Future Research

While research has made progress in identifying cybersecurity issues for SMEs, existing studies reveal numerous literature gaps that need more thorough investigation. Researchers have yet to conduct extensive empirical studies to identify which cybersecurity strategies work best for SMEs. Establishing theoretical frameworks and guidelines requires additional empirical research to validate their practical applicability and effectiveness in real SME environments. [15]

Future research should focus on identifying unique cybersecurity requirements across various SME industry sectors. Each sector faces distinct cybersecurity threats and vulnerabilities, which can help to create more effective cybersecurity solutions tailored to specific sector needs.

Additionally, long-term studies that track the effectiveness of implemented cybersecurity measures on SME resilience could provide valuable insights for identifying best practices and improvement areas.

Moreover, there is a need to explore how emerging technologies, such as artificial intelligence and machine learning, can help to enhance cybersecurity for SMEs. As cyber threats continue to evolve, those advanced technologies could offer innovative solutions to mitigate risks. The future study area needs to explore barriers SMEs face in adopting technology, while seeking solutions to stimulate their cybersecurity technology adoption

Lastly, examining the regulatory environment and its impact on SMEs' cybersecurity practices could demonstrate how legal compliance obligations influence security investments and strategies. Understanding how SMEs navigate these regulations and the resources they allocate to meet compliance can help inform policy recommendations aimed at strengthening the overall cybersecurity posture of the SME sector.

5.3 Conclusion

In conclusion, the findings of this literature review highlight the critical need for SMEs to find ways that offer total and proactive cybersecurity preparedness for small and medium enterprises to enable them to secure their functionalities and data. The continuing evolution of cyber threats continues to validate the need for small and medium enterprises to place cybersecurity as one of the core parts of their business strategy. In addressing the literature gaps identified and pursuing empirical research, various stakeholders could build on the understanding of the challenges of cybersecurity in small and medium enterprises in developing solutions to safeguard this critical sector of the economy.

6. References

[1] Pfleeger, C. P., Pfleeger, S. L., and Margulies, J., 2015. *Security in Computing*. 5th ed. Prentice Hall.

[2] Stallings, W., Brown, L., Bauer, M., and Bhattacharjee, A., 2012. *Computer Security: Principles and Practice*. 2nd ed. Pearson.

[3] Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2022). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. Risk Analysis, 42(8), 1643-1669.

[4] European Commission, 2020. *User guide to the SME definition*. [online] Available at: https://ec.europa.eu/growth/smes/sme-definition_en [Accessed 28 July 2024]

[5] Ayyagari, M., Beck, T., and Demirgüç-Kunt, A., 2007. *Small and medium enterprises across the globe*. Small Business Economics, 29(4), pp.415-434.

[6] Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. Technology innovation management review, 4(10).

[7] CISA, 2020. *Remedial Actions for SolarWinds Orion Platform Security Incident*. Available at:https://www.cisa.gov/news-events/directives/ed-21-01-mitigate-solarwinds-orion-code-compromise. [Accessed 02 August 2024].

[8] Ponemon Institute, 2020. *2020 Cost of a Data Breach Report*. IBM Security. Available at: https://www.ibm.com/security/data-breach. [Accessed 05 August 2024].

[9] Symantec, 2020. *Internet Security Threat Report*. Available at: https://docs.broadcom.com/doc/istr-03-jan-en. [Accessed 10 August 2023].

[10] Kaspersky, 2020. *Cybersecurity Threats: The Current Landscape*. Available at: https://www.kaspersky.com/resource-center/threats. [Accessed 01 August 2024].

[11] Hasan, R., Anwar, F., & Husnain, M., 2021. *Assessing the Cybersecurity Readiness of Small and Medium Enterprises: Challenges and Strategies*. Journal of Information Security, 12(2), pp. 120-134.

[12] Baker, W. H., Wallace, L., & Dutton, W. H., 2020. *Cybersecurity in the Age of Digital Transformation: A Study of SMEs*. Journal of Business Continuity & Emergency Planning, 14(3), pp. 234-247.

[13] Cybersecurity Ventures, 2021. *Cybersecurity Workforce Study: 2021 Report*. Available at: https://cybersecurityventures.com/cybersecurity-workforce-report. [Accessed 06 August 2024].

[14] ENISA, 2021. *Cybersecurity for SMEs: A Study on the Current State and Future Trends*. European Union Agency for Cybersecurity. Available at: https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes. [Accessed 07 August 2024].

[15] Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. Journal of Information Security and Applications, 58, 102726.

[16] IBM, 2020. *Cost of a Data Breach Report*. Available at: https://www.ibm.com/security/data-breach. [Accessed 08 August 2024]

[17] CyberEdge Group, 2021. *2021 Cyberthreat Defence Report*. Available at: https://cyberedgegroup.com/research/2021-cyberthreat-defence-report/. [Accessed 10 August 2024].

[18] PwC, 2020. *2020 Consumer Intelligence Series: Trust in the Age of COVID-19*. Available at: https://www.pwc.com/gx/en/issues/crisis-solutions/covid-19-consumer-i ntelligence-series.html. [Accessed 10 August 2024].

[19] Verizon, 2021. *Data Breach Investigations Report*. Available at: https://enterprise.verizon.com/resources/reports/dbir/. [Accessed 10 August 2024].

[20] European union, *Eurobarometer*. SMEs and cybercrime report pp.52. Available at https://europa.eu/eurobarometer/surveys/detail/2280. [Accessed 08 December 2024]

[21] NIST, 2020. *Small Business Cybersecurity Case Study Series.* Available at https://www.nist.gov/itl/smallbusinesscyber/cybersecurity-basics/case-study-series. [Accessed 10 February 2025].

[22] NFP 2023, *The threats cyber criminals pose to SMEs.* Available at https://www.nfp.co.uk/media/insights/the-threats-cyber-criminals-pose-to-smes/. [Accessed 20 February 2025]

[23] Chubb Insurance in Australia, 2022. *Cyber case studies for SMEs.* Available at https://www.chubb.com/au-en/articles/business/cyber-case-studies-for-smes.html. [Accessed 20 February 2025]

[24] Citation Cyber, 2019. *SMEs and Cyber Security: A case study - Citation Cyber.* Available at https://citationcyber.com/smes-and-cyber-security/. [Accessed 23 February 2025]

[25] AVG. *Business Antivirus Software.* Available at https://www.avg.com/en-us/antivirus-business-edition#pc. [Accessed 24 February 2025]

[26] CDW.com. *Fortinet FortiGate 100F - security appliance - FG-100F - Firewalls & VPN.* Available at https://www.cdw.com/product/fortinet-fortigate-100f-security-appliance/5615104. [Accessed 24 February 2025]

[27] Bitdefender. *Bitdefender GravityZone Business Security Premium.* Available at https://www.bitdefender.com/en-us/business/products/gravityzone-premium-security. [Accessed 24 February 2025]

[28] Acronis. *Acronis Cyber Protect – Purchasing options.* Available at https://www.acronis.com/en-sg/products/cyber-protect/purchasing/. [Accessed 24 February 2025]

[29] SOPHOS. *MDR vs SOC Pricing Tool: MDR Proposal Generator.* Available at https://www.sophos.com/en-us/products/managed-detection-and-response/mdr-proposal-generator. [Accessed 25 February 2025]

[30] Knowbe4. *KnowBe4 Security Awareness Training Pricing.* Available at https://www.knowbe4.com/pricing-security-awareness-training. [Accessed 25 February 2025]

[31] Tech heads. *The Cost of a Cyberattack to Small and Medium Businesses (SMBs).* Available at https://blog.techheads.com/the-cost-of-a-cyberattack-to-small-and-medium-businesses-smbs. [Accessed 25 February 2025]

7. List of pictures, tables, and abbreviations

7.1 List of pictures

Figure 1: Phishing email report rate by click status 24
Figure 2: Relative concern for cyber threats by type 26
Figure 3: Cybersecurity threat landscape 27
Figure 4: Different impacts on SMEs 36

7.2 List of tables

Table 1: A framework for SME cybersecurity defence 44
Table 2: Cost-Benefit Analysis of Cybersecurity Implementation for La Luna Supermarket 47

7.3 List of abbreviations

SMEs	Small and Medium Enterprises
AEV	Advanced Electrical Varnishes Ltd
AI	Artificial Intelligence
DDoS	Distributed Denial-of-Service
DOS	Denial-of-Service
IoT	Internet of Things
MFA	Multi-Factor Authentication
POS	Point-of-Sale
ROI	Return On Investment
ROM	Read-Only Memory
USB	Universal Serial Bus
VPNs	Virtual Private networks