Current cybersecurity risks and damages associated with Small and Medium Enterprises

Vos Nils
Fratu Mihai
Zamuruev Vladislav
Carcea Madalina
Vladutu Daria

November 1, 2024

1 Executive Summary

Objective: This policy paper explores the importance of cybersecurity and privacy practices for Small and Medium Enterprises (SMEs), focusing on the role these measures play in protecting consumer data, fostering consumer trust, and sustaining growth in the digital economy.

Context: Personal information has now become a big asset to businesses fostering innovation and economic growth in the digital economy. Cybersecurity and privacy are two related domains involving personal information and ensuring data security. Most SMEs face challenges in implementing robust cybersecurity because of financial constraints, lack of expertise, and resource limitations. Moreover, increased data collection practices employed by businesses presently raise the breach risk and undermine trustworthiness, especially for SMEs.

Key Findings:

- **Role of Trust in Data Management:** As consumers become more aware of data privacy issues, trust in a business's data protection practices becomes increasingly critical. Consumers prefer companies that prioritize cybersecurity and, effectively and directly communicate this. Effective data protection practices, including cybersecurity and privacy policies, significantly impact consumer confidence, which influences customer loyalty and business growth.
- **Challenges in Cybersecurity for SMEs:** SMEs often struggle with limited financial resources and expertise in cybersecurity. The cost of breaches—including losses, reputational damage, and legal penalties—is particularly severe for smaller enterprises. Furthermore, these enterprises face obstacles like low cybersecurity methods awareness, inadequate protection measures that are not representative of the current issues in this domain, and lack of allocated budget.
- **Cybersecurity Practices and Risk Management:** A layered cybersecurity approach, including intrusion detection and prevention systems (IDS/IPS), data encryption, and employee training, is essential for protecting SMEs from cyber threats. Integrating AI and

machine learning can further enhance detection and protection capabilities, reducing the risk of human error and social engineering attacks.

Policy Recommendations:

- **Strengthen Cybersecurity Infrastructure:** SMEs could adopt robust security technologies, including firewalls, IDS/IPS, and data encryption. Regular security audits and standards like ISO/IEC 27001 can provide a systematic approach to risk management and ensure legal compliance. This suggestion is derived from the importance of investing in the development of cybersecurity measures.
- **Promote Consumer Awareness:** SMEs could enhance consumer confidence by transparently communicating data handling practices, implementing two-factor authentication, and educating consumers about good cybersecurity practices.
- **Enhance Regulatory Compliance:** Governments and industry regulators could enforce some scalable cybersecurity standards tailored to SMEs. Sector-specific certifications (e.g., PCI DSS for retail) can also help SMEs achieve security excellence. Additionally, businesses could ensure employee seminars/ conferences where they would get educated about specific cyber attack methods and privacy concerns.

Conclusion: Investment in cybersecurity is not just a defensive measure but also an important strategic asset wherein consumer trust and economic growth are built. Good cybersecurity practice strengthens brand loyalty and fuels long-term success. As threats around the ever-changing digital landscape evolve, so should SMEs against them.

2 Introduction

2.1 The Importance of Personal Data in the Digital Economy

Personal data today is an important business asset; it drives innovation, improves customer experiences, and, thus, contributes much towards economic growth in the digital economy (Institute, 2020; Organisation for Economic Co-operation and Development, 2019). On the other hand, as more organizations collect, store, and analyze personal data, the associated risks have also grown, raising valid demands for effective data protection measures (Security & Institute, 2021). This has made trust a core component of efficient data management. Without solid foundations in data protection, consumer trust in businesses, especially small and medium-sized enterprises, can weaken immediately, which shakes up the stability of the digital economy (Accenture, 2022).

2.2 The Role of Trust in Data Management

Two interrelated yet distinct areas engage in keeping an individual's data safe: cybersecurity and data privacy. Cybersecurity entails the protection of data and systems from unauthorized access or cyber threats (National Institute of Standards and Technology, 2020). Complementary to this, privacy concerns the responsible handling and processing of personal information, and its adherence to concerned laws and regulations, respectively (European Union Agency for Cybersecurity, 2021). Altogether, these two domains form the core of risk management in digital operations, hence enabling business people to mitigate threats with the observation of one's rights to privacy (International Organization for Standardization, 2019). However, SMEs face the challenge of implementing these measures due to insufficient financial capacity, expertise, and access to more advanced technologies (International Trade Centre, 2021). This has made

most SMEs prone to such cyberattacks, which can have an important effect on their image by reducing consumer confidence in the way they manage such data (P. LLP, 2022).

With public awareness of data privacy questions, cybersecurity is instrumental in helping to engender confidence among consumers. Thus, more and more consumers consider interacting with a business based on its ability to protect data and its cybersecurity practices (Gartner, 2022). This trend puts pressure on SMEs to show transparent and secure data practices as a means of commanding customer loyalty and maintaining competitive advantage (International, 2021). Therefore, it is important that addressing cybersecurity challenges for SMEs is not only about protection but also about reinforcing consumer confidence in the digital market (E. Y. LLP, 2023).

3 Cybersecurity and Privacy: Definitions and Concepts

Cybersecurity and privacy, though closely related, address different but overlapping sides of digital protection. Cybersecurity refers broadly to the processes, practices and technologies used to protect systems, networks and data from unauthorised access. Privacy, on the other hand, focuses on the rights of people to control and protect their personal information, which is often focused on how data is collected, shared or used.

In the context of this policy paper, these definitions underline the need for Small and Medium Enterprises (SMEs) to find the middle ground between cybersecurity practices and privacy requirements to build and maintain consumer trust and data accuracy.

3.1 Cybersecurity in the Digital Market

Cybersecurity is essential to the workings of online transactions, data management and consumer engagement. The digital market is threatened by increasingly more sophisticated cyberattacks, putting consumer and business information at risk. This shows the importance of having strong cybersecurity protocols in place. For SMEs, cybersecurity involves protecting digital assets and consumer data through practices such as two-factor authentication (2FA), secure payment gateways, and proactive threat monitoring. Despite often having limited resources, SMEs face an increasing need to prioritise cybersecurity as both a responsibility and a trust-building strategy, as studies have shown that consumers tend to disengage with businesses following security breaches or mishandling data (Schomakers & Ziefle, 2022). As our research demonstrates, transparent communication of these security practices increases customers' willingness to share personal information with businesses, highlighting a direct link between effective cybersecurity and enhanced consumer trust (Vos, 2024).

3.2 Privacy and Risk Management

Privacy is legally mandated in most parts of the world through frameworks such as the General Data Protection Regulation (GDPR) in the European Union. Effective privacy practices focus on minimising data collection, securing data storage and allowing people to control how their data is being used. For SMEs, privacy practices represent a form of risk management, as consumer data misuse or accidental exposure can always happen, and can severely damage their reputation. Integrating privacy into risk management requires SMEs to adopt extensive data governance practices that ensure transparency in data practices, actively inform consumers about data use and comply with applicable legal standards.

3.3 The Overlap Between Cybersecurity and Privacy

The interplay between cybersecurity and privacy is particularly clear in the shared goal of protecting sensitive information. For SMEs, achieving a balance in these two facets requires developing cybersecurity practices that incorporate privacy considerations such as data encryption, minimising data collection and making sure consumers have access to clear information on how their data is being handled (Schomakers & Ziefle, 2022).

4 Current Challenges in Cybersecurity for Small and Medium Enterprises (SMEs)

4.1 SMEs and Cybersecurity: An Overview

It is stated that 84% of cyberattacks rely on social engineering (European Union Agency for Cybersecurity (ENISA), 2021). Small and medium enterprises (SMEs) form the backbone of many economies, but they are increasingly vulnerable to cyberattacks. As highlighted by Horn (2017), SMEs often lack the resources and expertise to effectively protect themselves. This is supported by a survey made by ENISA (2021), which identified the top 3 challenges for SMEs in this domain: low cybersecurity awareness of the personnel, inadequate protection of critical and sensitive information, and lack of budget. This low level of awareness and preparedness can make them attractive targets for cybercriminals. This might not seem like an intensive problem, as their size makes them secondary targets of attacks. However, they can still be hit, and SME servers can be used as an access point to other companies through their partnerships or usage of external services, such as cloud services (Falch, 2023). As a survey by ENISA (2021) indicated, many SMEs have outsourced the responsibility of managing IT systems without understanding the importance of cybersecurity. Therefore, they do not consider investing in cybersecurity a necessity and, as a result, have less formal organisations than their larger counterparts (Falch, 2023).

4.2 Financial and Expertise Barriers

Financial constraints and a shortage of cybersecurity expertise are two prominent obstacles that keep SMEs from adopting robust cybersecurity practices (IBM, 2021). The estimated global annual cost of cybercrime reached €5.5 trillion in 2021 (European Commission, 2022). This is devastating, as it encompasses financial impacts, legal fees, regulatory compliance, reputational damage, and potential fines (IBM, 2021). This financial burden can be particularly severe for smaller enterprises that lack the financial expertise of larger organizations, making it challenging to allocate funds toward critical cybersecurity initiatives. The expenses involved in purchasing and maintaining security software, hiring cybersecurity professionals, and conducting regular security assessments can often be out of reach for such enterprises due to a lack of funds. As a result, SMEs may adopt only basic security measures, which may not offer adequate protection against the dynamic and increasingly sophisticated cyber threats they face. This aligns with findings from recent literature indicating that SMEs investing in cybersecurity see fewer breaches and enhanced consumer trust, which ultimately contribute to business growth and success (IBM, 2021) (DINNOCAP, 2021). However, these benefits remain primordial for SMEs, as they are unable to overcome financial constraints, underscoring a need for cost-effective and accessible cybersecurity solutions. SMEs frequently lack the in-house expertise necessary to address cybersecurity challenges effectively. Many smaller enterprises rely on general IT staff who may lack advanced cybersecurity knowledge, leaving them vulnerable to threats that dedicated

security personnel could potentially mitigate. This expertise gap can further expose SMEs to preventable risks. As such, the necessity of practical, affordable cybersecurity solutions for SMEs is evident. Targeted support—such as simplified cybersecurity frameworks like NIST (2019)'s IP-DRR (Identify, Protect, Detect, Respond, Recover)—and awareness initiatives could help SMEs build resilience, even with limited financial and human resources.

4.3 Intrusion, Detection, and Prevention Methods

The adoption of cybersecurity safeguards in SMEs is primarily about changing how organisations implement IT systems (Falch, 2023). Therefore, SMEs should strive to employ up-to-date security measures, as currently less than 50 per cent do so (Figure 1).

Despite the identified, SMEs can still implement effective cybersecurity measures to protect their assets. Intrusion detection and prevention systems (IDS/IPS) play a crucial role in this regard (Wylde, 2022). IDS systems continuously monitor network traffic for suspicious activity that may indicate a cyberattack. They can alert IT personnel to potential threats and help to mitigate damage. IPS systems go a step further by actively blocking malicious traffic before it can reach critical systems and data.

However, IDS/IPS systems are most effective when used in conjunction with other security measures. Firewalls can help to protect networks from unauthorised access, data encryption can safeguard sensitive information, and employee training can reduce the risk of human error and social engineering attacks. By implementing a layered approach to cybersecurity, SMEs can significantly improve their ability to detect, prevent, and respond to cyberattacks. As noted by Wylde et al. (2022), the effectiveness of these measures depends on their proper implementation and maintenance.

Additionally, technologies such as big data, AI, and Machine Learning can be used as a proactive measure to detect what traditional methods cannot. Unsupervised learning algorithms (decision trees, neural networks, etc.) could be used to highlight how data is treated and managed to produce an outcome (Wylde, 2022). On the other hand, these methods could be used as an addition to IDS/IPS systems to learn about malicious patterns, thus shielding the data better (Wylde, 2022).

When discussing increasing awareness among SME employees and owners, the most accessible solution is to instil awareness programmes internally. It must target the employee experiences with digital systems, making cybersecurity a habitual part of routine activities. Such programs should focus on familiarising employees with the most common cyber threats, such as phishing, malware, and social engineering tactics (European Union Agency for Cybersecurity (ENISA), 2021). Training should incorporate practical examples relevant to the SME's industry and address realistic scenarios they might face. Interactive tools like quizzes, simulations, and role-playing exercises have proven effective in reinforcing cybersecurity principles and improving retention of best practices (e. a. Ponsard, 2019). A further step proposed by (European Union Agency for Cybersecurity (ENISA), 2021) would be to set up incident response protocols that are straightforward and communicated. Hence, employees understand their role in mitigating risks and responding to potential threats.

Additionally, according to a recent report from (World Economic Forum, 2020), implementing effective cybersecurity measures could potentially increase SMEs' annual revenue by an average of 5%. This highlights the financial benefit of cybersecurity as not only a defensive investment but also a revenue-enhancing strategy. Additionally, IBM's 2021 report indicates that organizations with full security automation in place reduced the average total cost of a data breach

by nearly 80% worldwide. This significant reduction underscores how critical it is for SMEs to integrate cybersecurity measures like automated threat detection and incident response, as they can substantially decrease the financial burden during critical events (IBM, 2021).

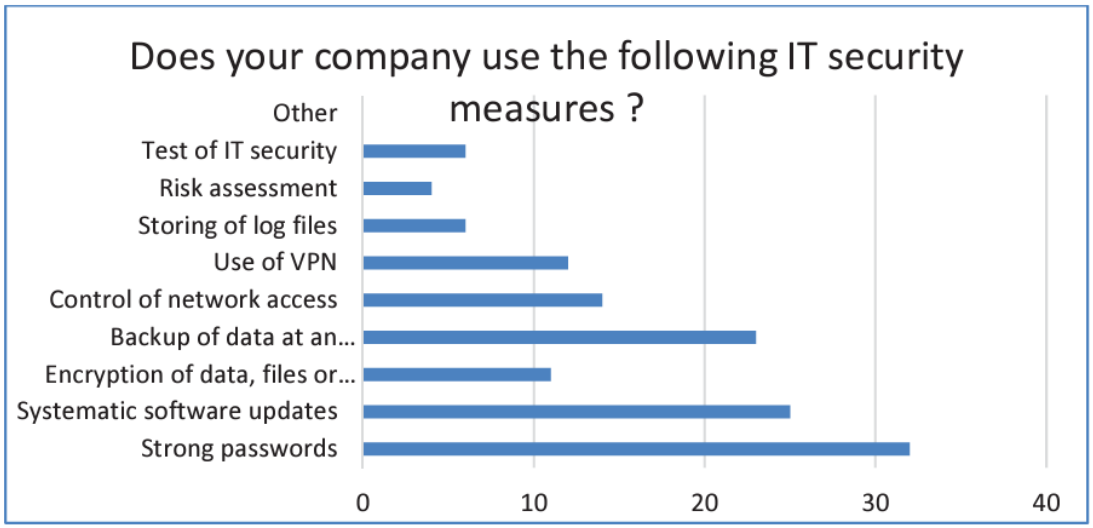

Figure 1: *No. of SMEs using different security measures. Source: DINNOCAP survey (2021)*

5 The Impact of Cybersecurity on Consumer Confidence

5.1 Consumer Awareness of Data Usage

As customer awareness of data usage increases, businesses are being required to protect the flow and storage of information across their organisations. However, mistakes regularly occur. Along with all the technological advancements, consumers have become more conscious and often judge companies based on how honest and secure their protection processes are, as shown in Figure 2. According to our research, over 80 per cent of consumers consider cybersecurity a key factor when it comes to establishing their trust in an organization.

Furthermore, multiple respondents reported stopping doing business with a firm after experiencing breaches of their data, making it even more vital that SMEs adopt clear and prominent cybersecurity controls to both maintain consumer trust and also protect brand reputation as shown in Figure 3 (Carcea, 2024).

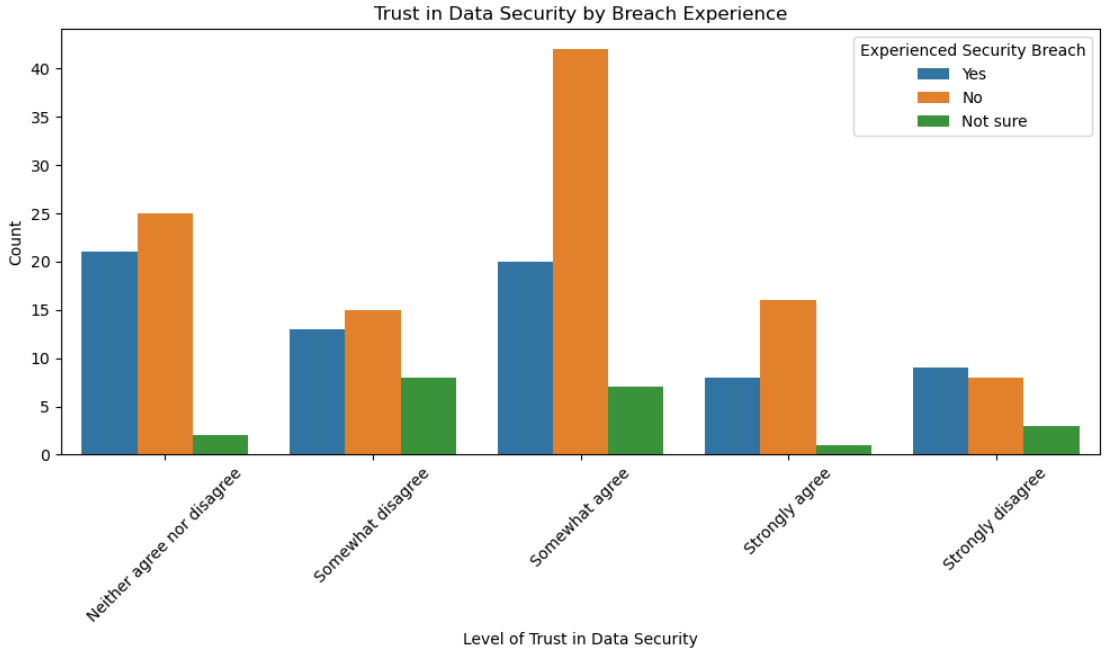

Figure 2: *Q: I trust most companies will protect and secure my data against breaches or attacks.*

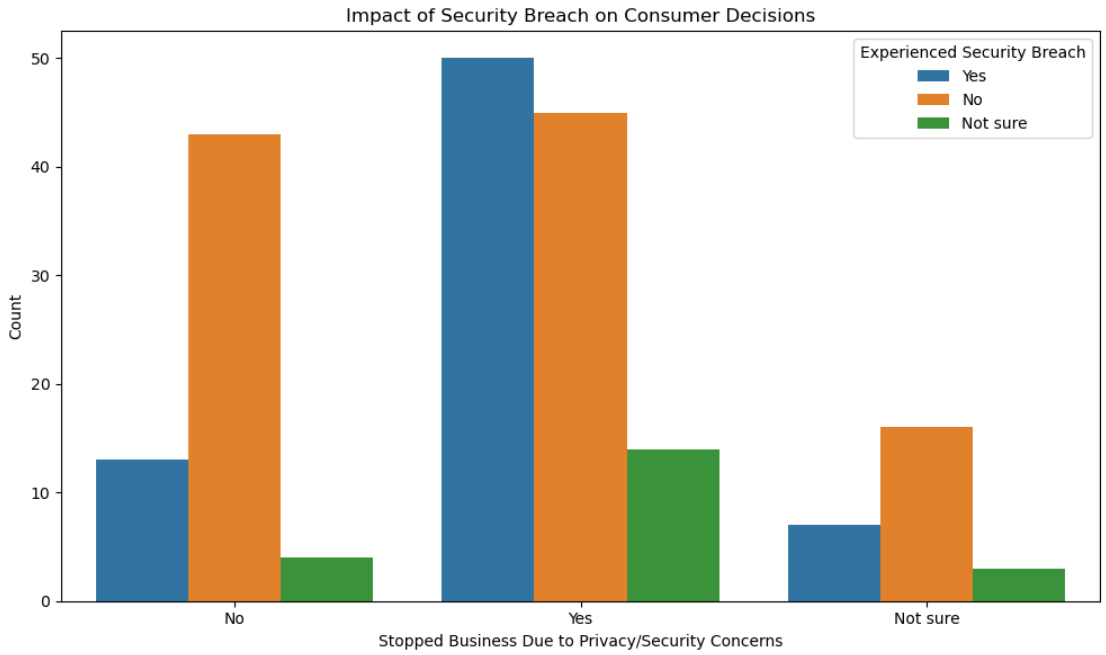

Figure 3: *Q: Have you ever stopped doing business with a company due to privacy/security concerns?*

5.2 Trust and Security in SMEs

Trust is essential for the digital marketplace, where competitive advantage can hinge on consumer perception of data security. Robust cybersecurity practices—like two-factor authentication, data encryption, and transparent privacy policies—help SMEs build trust by demonstrating commitment to protecting customer data. More and more studies show a positive correlation between cybersecurity investments and raised consumer loyalty, with SMEs prioritising security, and seeing higher rates of customers and long-term growth (Amir et al., 2018). The focus on cybersecurity transforms it from a defensive measure into a strategic asset, fostering trust and ultimately driving economic gains for SMEs (Alharbi et al., 2022). After analysing our data based on the mixed-matched approach, responders of all ages expressed their critical need for data protection as shown in Figure 4.

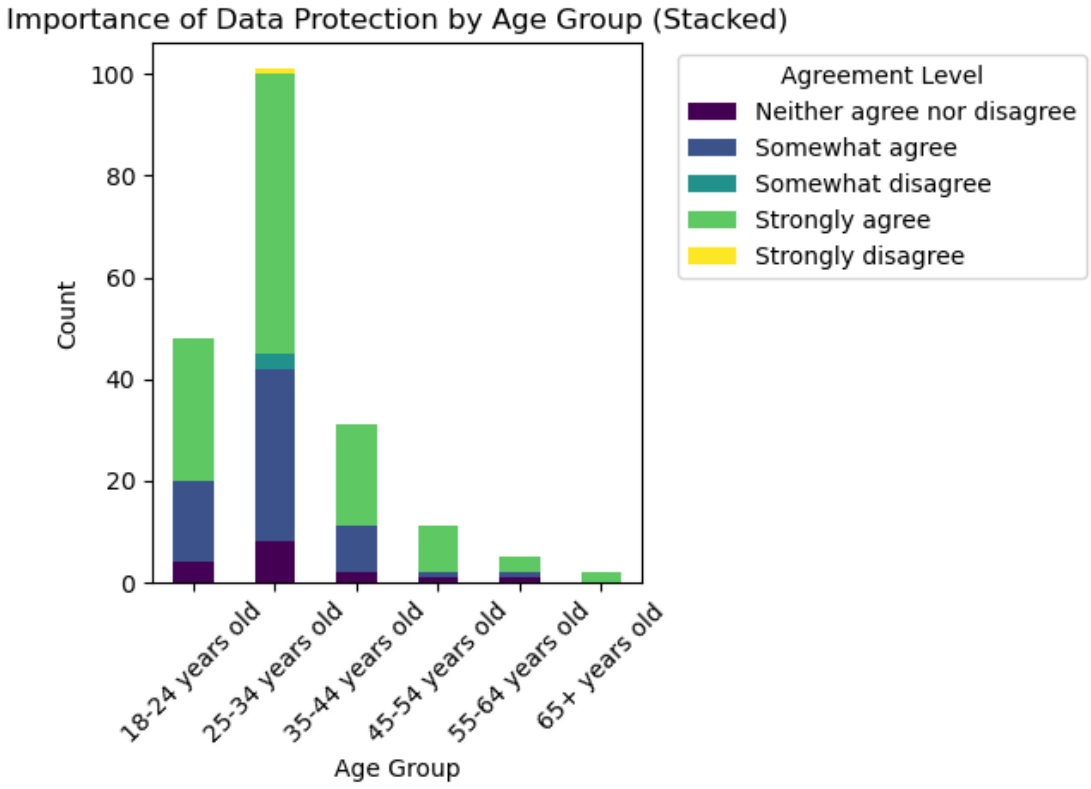

Figure 4: *Q: It is important to me that measures are taken to protect my data.*

6 Policy Recommendations for Strengthening Cybersecurity in SMEs

The following policy recommendations aim to provide a comprehensive approach to strengthening cybersecurity in SMEs, focusing on improving infrastructure, promoting consumer awareness, and ensuring regulatory compliance.

6.1 Improving Cybersecurity Infrastructure for SMEs

To make the cybersecurity infrastructure of SMEs more advanced, it is very important to adopt both technological and organizational measures. Enterprises should invest in cybersecurity technologies like firewalls, cloud-based data storage and encryption tools. In addition to that, regular security checks and vulnerability assessments can help identify and eliminate potential risks before causing damage (Antunes et al., 2021; Renvall, 2018).

Moreover, adopting information standards, such as ISO/IEC 27001, can provide a more comprehensive framework for implementing data privacy systems into SMEs (Renvall, 2018). The aforementioned standard helps SMEs manage their data security, whilst also being in line with legal requirements.

6.2 Promoting Consumer Awareness and Education

Two critical components of a cybersecurity strategy, and, in general, of SMEs, are consumer awareness and education. Transparency and clear communication of data handling practices should be a huge priority of SMEs. The measures taken to protect personal data, such as two-factor authentication, can significantly enhance consumer confidence, therefore, SMEs should provide detailed information about them (Bada & Nurse, 2019; C. Ponsard & Grandclaudon, 2020). This could be achieved by a simpler way of conveying the information to buyers online, such as a modified version of the privacy disclaimer shown when browsing websites.

SMEs should also show educational initiatives, like holding a workshop about common cybersecurity practices or creating a few online resources. They can help both employees and consumers understand cybersecurity and its importance, whilst also learning about how they can protect their personal information (Bada & Nurse, 2019).

6.3 Strengthening Regulations and Compliance

Another essential for ensuring that SMEs follow better cybersecurity practices is regulatory compliance. Regulations that require SMEs to implement cybersecurity standards should be developed and enforced by governing bodies. They should be tailored to, or at least include a section dedicated to, SMEs (Antunes et al., 2021; C. Ponsard & Grandclaudon, 2020). On the other hand, this would be difficult to achieve if the implementation process would not strive to be as easy to implement as possible. Ever since the EU started implementing tighter restrictions on online business practices, it has given a one-year adaptation period for affected businesses to update their operations and comply with new standards (E. Y. LLP, 2023). However, in cases involving more complex compliance requirements—such as those related to data protection under the GDPR—the compliance window has been extended to two years, allowing organizations additional time to make necessary adjustments and integrate more comprehensive cybersecurity measures.

In addition to the already mentioned measures, specific guidelines and certifications, based on the industry, can provide SMEs with a well-organized roadmap for implementing cybersecurity (Mihai, 2024). A good example of such guidelines is the Payment Card Industry Data Security Standard (PCI DSS), which provides specific requirements for securing card data, which can be particularly useful for SMEs in the retail sector (Renvall, 2018).

7 Conclusion

The paper outlines how consumer trust and the economy can be enhanced through the implementation of critical cybersecurity practices by small and medium-sized enterprises. The research demonstrated how SMEs that allocate funds for substantial cyber-defensive mechanisms are able not only to protect their resources but also to strengthen client trust, which in return leads to higher profits. The data and information collected present a compelling business case that bears an economic focus on cybersecurity by SMEs as a compliance obligation and a source of competitive benefit. Considering the dynamic nature of threats on the internet, it would be prudent for SMEs to begin deploying sophisticated cybersecurity measures as a critical commercial strategy intended to protect their digital footprints and enhance brand loyalty.

8 Appendix

Nevertheless, to effectively manage and align the interests of all parties involved in this project, a stakeholder analysis has been conducted. This analysis identifies each stakeholder group, evaluates their level of interest and influence, and classifies them based on their role within the project. By understanding the varying degrees of management and engagement required, this analysis provides a structured approach to stakeholder management, ensuring that key players are actively involved, informed or monitored. Table 1 summarizes the stakeholder groups, their interests, influence, and recommended actions to foster effective collaboration and project alignment.

Table 1: Stakeholder Analysis (Source: Compiled Individual Research)

Stakeholder Group	**Interest**	**Influence (Power)**	**Category**	**Action**
SME Owners/Managers	High	High	Key Players	Actively engage and be involved in decision-making.
SME Employees	High	Medium	Keep Informed	Regular updates and involvement in project tasks.
Digiwerkplaats MKB Advisors	High	High	Key Players	Collaborate closely and consult regularly.
BUAS Students	High	Medium	Keep Informed/Monitor	Guide and provide regular feedback.
BUAS Academic Supervisors	Medium	High	Key Players	Coordinate and ensure alignment with academic goals.
Customers	Medium	Low	Keep Satisfied	Communicate benefits and gather feedback.
Regulatory Bodies	Low	High	Key Players/Monitor Closely	Ensure compliance and provide the necessary documentation.
Business Partners/Suppliers	Medium	Medium	Keep Satisfied/Monitor Closely	Maintain communication and address potential impacts.
Investors/Financial Institutions	Medium	Medium/High	Key Players/Keep Satisfied	Provide updates on project progress and outcomes.
Municipality	Medium	Medium/High	Keep Satisfied/Monitor Closely	Maintain communication to ensure alignment with local regulations and community interests.

References

Accenture. (2022). *The state of cybersecurity resilience 2022: Perspectives for small and mid-sized enterprises* (tech. rep.). Accenture.

Alharbi, A., et al. (2022). Transparency in data handling and consumer trust. *Journal of Business Ethics*, *30*(1), 89–105.

Amir, E., et al. (2018). The financial impact of cybersecurity investments. *Journal of Financial Economics*, *29*(2), 123–145.

Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. (2021). *Information security and cybersecurity management: A case study with smes in portugal* (tech. rep.). Journal of Cybersecurity and Privacy.

Bada, M., & Nurse, J. R. (2019). *Developing cybersecurity education and awareness programes for small- and medium-sized enterprises (smes)* (tech. rep.). Information & Computer Security.

Carcea, M. (2024). *The impact of robust cybersecurity practices on consumer confidence and economic outcomes in sme investments* [Unpublished manuscript, Overleaf]. https://www.overleaf.com/project/670bfe1316bee6ecd7305d86

DINNOCAP. (2021). *Digital innovation and capability* (tech. rep.). https://www.diginnobsr.eu/dinnocap

European Commission. (2022). *State of the union: New eu cybersecurity rules ensure more secure hardware and software products* (tech. rep.). European Commission.

European Union Agency for Cybersecurity. (2021). *Cybersecurity and data protection in the eu: Policy and practice* (tech. rep.). ENISA.

European Union Agency for Cybersecurity (ENISA). (2021). *Enisa threat landscape 2021* (tech. rep.). European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

Falch, e. a., M. (2023). *Cybersecurity strategies for smes in the nordic baltic region* (tech. rep.).

Gartner, I. (2022). *Understanding consumer trust in digital markets* (tech. rep.). Gartner.

IBM. (2021). *Cost of a data breach report 2021* (tech. rep.). Ponemon Institute. https://www.ibm.com/reports/data-breach

Institute, M. G. (2020). *Digital transformation and the global economy: An outlook for data-driven growth*. McKinsey & Company.

International, K. (2021). *Data protection and the trust imperative for smes* (tech. rep.). KPMG.

International Organization for Standardization. (2019). *Iso/iec 27001:2019 – information security management* (tech. rep.). ISO/IEC.

International Trade Centre. (2021). *Smes and cybersecurity: Challenges and solutions for a digital economy* (tech. rep.). ITC Publications.

LLP, E. Y. (2023). *Cybersecurity in smes: A roadmap to building resilience* (tech. rep.). EY.

LLP, P. (2022). *Protecting data in the digital economy: Cybersecurity for small and medium enterprises* (tech. rep.). PwC.

Mihai, F. V. (2024). Awareness of small and medium enterprises employees regarding business data privacy practices.

National Institute of Standards and Technology. (2020). *Framework for improving critical infrastructure cybersecurity* (tech. rep.). NIST.

Organisation for Economic Co-operation and Development. (2019). *Digital economy outlook: Data as an asset for economic growth*. OECD.

Ponsard, C., & Grandclaudon, J. (2020). *Guidelines and tool support for building a cybersecurity awareness program for smes* (tech. rep.). Proceedings of the International Conference on Information Systems Security and Privacy (ICISSP).

Ponsard, e. a., C. (2019). *Survey and lessons learned on raising sme awareness about cybersecurity* (tech. rep.).

Renvall, A. (2018). *Improving cybersecurity through iso/iec 27001 information security standard in the context of smes* (tech. rep.). Master's Thesis, Helsinki Metropolia University of Applied Sciences.

Schomakers, E.-M., & Ziefle, M. (2022). Privacy vs. security: Trade-offs in the acceptance of smart technologies for aging-in-place. *International Journal of Human-Computer Interaction*, *39*, 1–16. https://doi.org/10.1080/10447318.2022.2078463

Security, I., & Institute, P. (2021). *Cost of a data breach report 2021* (tech. rep.). Ponemon Institute.

Vos, N. (2024). Impact of sme cybersecurity practices on consumer trust and data protection awareness [*This manuscript was compiled on October 21, 2024*].

World Economic Forum. (2020). *The global risks report* (tech. rep.). World Economic Forum. https://www.weforum.org/publications/the-global-risks-report-2020/

Wylde, e. a., V. (2022). Cybersecurity, data privacy.