Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 263 (2025) 712–718

Procedia Computer Science

www.elsevier.com/locate/procedia

International Conference on Industry Sciences and Computer Science Innovation

Safeguarding the Future: Forecasting Cybersecurity and Privacy Challenges and Solutions in Emerging Technologies for SMEs

Daniel Moreira Campos*

University Institute of Lisbon (ISCTE-IUL), ISTAR, Av. das Forças Armadas, Lisbon 1649-026, Portugal

Carlos Coutinho†

University Institute of Lisbon (ISCTE-IUL), ISTAR, Av. das Forças Armadas, Lisbon 1649-026, Portugal

Abstract

Small and medium-sized enterprises (SMEs) are increasingly vulnerable to cybersecurity threats, risking their operations and growth. This paper examines SMEs' specific weaknesses and identifies effective protection strategies. Combining quantitative tests and qualitative surveys and interviews, the study highlights key challenges like limited resources, lack of expertise, and emerging technology threats. It investigates the impact of quantum computing, which could compromise current encryption methods, and Artificial Intelligence (AI), which can enhance threat detection. The findings guide SMEs in adopting new technologies, improving employee training, and bolstering cybersecurity. The paper aims to develop tailored cybersecurity plans to ensure SMEs' safety and success in the digital age.

Keywords: Cybersecurity; SMEs; Vulnerability; Training

1. Introduction

We live in a time when technology is advancing at an incredible pace, and with it comes a lot of worries about keeping our information safe online. The critical relevance of cybersecurity and privacy has never been more apparent in our rapidly advancing technological world. This research aims to explore future challenges in these areas, focusing on emerging technologies like Internet of Things (IoT), Artificial Intelligence (AI), Augmented Reality (AR), Virtual Reality (VR), Cloud Computing, and Quantum Computing. The goal is to highlight their significant impact on our lives and the necessity of anticipating cybersecurity and privacy concerns.

In an era defined by rapid technological advancements, the increasing dominance of emerging technologies has ushered in a new era of convenience and connectivity. However, this wave of innovation also brings profound concerns related to cybersecurity and privacy. Securing our technological landscape is crucial as we navigate this digital

* Corresponding author. Tel.: +351 963 746 024.
E-mail address: dmcsa@iscte-iul.pt
E-mail address: carlos.eduardo.coutinho@iscte-iul.pt

1877-0509
10.1016/j.procs.2025.07.085

revolution. Understanding the intricate relationship between digital transformation and its impact on total factor productivity is essential for ensuring efficiency and resilience against cyber threats [1]. The advent of IoT represents a paradigm shift in how we interact with the world, raising urgent concerns about data privacy and security. As smart devices become integral to our daily lives, addressing the evolving threat landscape is increasingly pertinent. Enterprises seem to prioritise other sides of the business and leave security and privacy of personal data as a secondary concern, only to realise that their whole business can collapse with a targeted attack [2].

Building on these insights, proactive risk management through integrated systems is crucial, with real-time monitoring being especially significant [3]. The role of artificial intelligence in enhancing cybersecurity is essential, particularly in addressing the widespread lack of knowledge and awareness about cybersecurity issues [4]. These considerations underscore the critical need for holistic strategies to secure our increasingly digital world. As society navigates the transformation brought by digital advancements, there is a pressing need for proactive measures to safeguard privacy and societal well-being [5]. Additionally, the implications of advanced connectivity generations on the cybersecurity threat landscape highlight future network challenges [6]. Addressing the multifaceted challenges posed by emerging technologies in daily life requires drawing on empirical evidence and diverse research insights. Forecasting and addressing cybersecurity issues is critical to prevent threats and privacy breaches from overshadowing technological progress. Continuous research, including case studies and experiments, is essential to develop effective cybersecurity solutions for SMEs [7].

1.1. Research question

This paper is about tackling those concerns, especially for small and medium-sized enterprises (SMEs), which often don't have the same resources as bigger companies to protect themselves. By looking into the latest technologies like AI and quantum computing, I hope to find practical ways to boost cybersecurity for these businesses.

To guide this study, I've come up with a crucial question that I want to answer:

- **RQ1:** *How vulnerable are SMEs in Portugal, and what are the most effective practices for individuals and employees to enhance their online security and respond effectively to cyber threats?*

1.2. Methodology

The primary goal of this research is to explore how SMEs can prepare for cybersecurity threats using emerging technologies like AI and quantum computing. To achieve this, a comprehensive methodological approach that combines qualitative and quantitative methods has been developed.

The research process began with selecting articles that align with the main theme, focusing on the relationship between cybersecurity, privacy challenges, and emerging technologies for SMEs. Databases such as Scopus, IEEE, and SpringerLink were used, with specific keywords guiding the search. In addition to peer-reviewed articles, grey literature, including industry reports and government publications, was incorporated to provide practical insights and address gaps in academic research.

Next, the credibility of the articles was evaluated by considering the reputation of the publishing journals and assessing the relevance and impact of the content. This ensured a solid foundation for the study. A temporal filter was then applied to prioritize recent articles, ensuring the research reflects the latest developments in the rapidly evolving cybersecurity landscape.

Finally, the value of the articles was assessed based on their contributions to the field, ensuring they offer meaningful insights and stimulate scholarly discourse on cybersecurity and privacy in SMEs.

In addition to literature review, semi-structured interviews were conducted with experts and SME stakeholders to gain in-depth insights into cybersecurity challenges and strategies related to emerging technologies. The interviewees, with over 20 years of experience and relevant positions, provided a holistic perspective on the global situation of SMEs. A script with over 40 questions was designed to guide these interviews, covering topics such as the current state of SME cybersecurity, the influence of AI, future implications of quantum computing, and best practices for employee training.

To broaden the perspective on cybersecurity awareness in Portuguese SMEs, a survey was conducted to gather data on their current cybersecurity practices, awareness, and perceptions regarding new technologies. This qualitative data provides a comprehensive understanding of the real-world challenges and solutions applicable to SMEs.

2. Literature review

Small and medium-sized enterprises (SMEs) make up 99% of all businesses within the EU and employ around 100 million people. They account for more than half of Europe's GDP and add value to all sectors of the EU economy [8]. Although large organisations are bigger targets for cyberattacks and have more resources for cybersecurity measures, SMEs are not safe from these threats. Underestimating these risks can lead to significant consequences, including business bankruptcy [9].

SMEs are often targeted by data breaches, data destruction, and data access denial, which negatively impact various business activities. Many SMEs fail to implement adequate security measures [10]. Cybersecurity awareness is crucial for SMEs to understand and mitigate these threats [11]. Despite acknowledging the threat, SMEs often believe they are less vulnerable due to their size [12]. Estimating the cost of cybercrimes is challenging due to unreported incidents [13]. Official reports indicate SMEs are prime targets for cyberattacks due to less sophisticated defence mechanisms compared to larger firms [12].

Risk management is crucial for SMEs due to limited resources and support mechanisms [14]. SMEs face six main types of risks: interest rate risk, raw material prices risk, e-business and technological risks, supply chain risks, growth risks, and management and employee risks [15]. Many SMEs lack adequate risk management strategies due to limited resources and knowledge gaps [16]. They often rely on informal processes, hindering effective risk identification, assessment, and mitigation [17]. Limited access to resources and expertise is a significant challenge [18], including up-to-date information and guidance on risk management practices [19]. Budget constraints also make it difficult to allocate sufficient resources to risk management [20].

Insufficient risk management can lead to financial losses, reputational damage, and business closure [21]. The impact of risk events is amplified for SMEs due to their smaller size and limited resources [22]. Therefore, SMEs must prioritise risk management and adopt a proactive approach to address risks [23]. This includes investing in training and resources to enhance capabilities [24] and leveraging external expertise and resources [25]. Effective risk management can protect SMEs and increase their resilience to potential risks.

More than half of hacked SMEs go bankrupt within six months of an attack [26]. Effective IT security relies on collaboration with employees, emphasising cybersecurity awareness tailored for both employees and the organisation. This awareness involves understanding the significance of IT security, appropriate security levels, and individual security responsibilities [27].

Additionally, recent trends highlight the growing importance of AI in the cybersecurity landscape for SMEs. AI has become a double-edged sword, being used both to defend against and conduct cyberattacks. AI tools help detect data breaches more quickly, counter deepfakes, and address phishing attempts, thereby enhancing the cybersecurity posture of SMEs. However, cybercriminals are also leveraging AI to bypass traditional defences like multi-factor authentication (MFA), making it crucial for SMEs to stay ahead in this evolving threat environment [28]. Furthermore, cybersecurity should be considered a strategic business priority, and SMEs must collaborate with governments and industries to bridge the cybersecurity skills gap and strengthen their defences. This collaboration can enhance awareness, improve risk management practices, and ultimately protect SMEs from cyber threats [29].

3. Results

This chapter presents the results and findings from the survey and interviews conducted as part of the study on safeguarding the future of SMEs in cybersecurity. The focus is on understanding current cybersecurity practices, challenges, and the potential of emerging technologies like AI and quantum computing to enhance SME security against cyberattacks. The methods used include a comprehensive survey of SMEs and semi-structured interviews with cybersecurity experts and SME stakeholders. The survey gathered quantitative data on the current state of cybersecurity among SMEs, while the interviews provided qualitative insights into the potential and challenges of

implementing advanced technologies in cybersecurity. This combination of quantitative and qualitative approaches ensures a well-rounded understanding of the cybersecurity landscape for SMEs.

3.1. Literature Review

The literature review highlights significant gaps in current cybersecurity strategies for SMEs, particularly in their ability to address emerging threats and technologies. SMEs, which constitute 99% of businesses in the EU, are increasingly vulnerable to cyberattacks due to inadequate security measures, limited resources, and a general underestimation of risks. The review points out that while larger organizations may be more obvious targets, SMEs often lack the sophisticated defenses needed to protect themselves, leading to severe financial and reputational damage, with more than half of hacked SMEs going bankrupt within six months.

A critical gap identified is the lack of integration between emerging technologies like AI and quantum computing in SME cybersecurity strategies. AI, while offering significant potential to enhance cybersecurity, is also being used by cybercriminals to exploit weaknesses in traditional defenses. SMEs are particularly susceptible to these advanced attacks due to their limited resources and expertise. Additionally, there is a lack of clear guidance on how SMEs can effectively utilize AI and other technologies to improve their cybersecurity posture. The literature also highlights the need for better collaboration between SMEs, governments, and industries to address the cybersecurity skills gap, which remains a significant barrier to effective risk management and defense against cyber threats.

3.2. Surveys Results

3.2.1. Participant Demographics

The survey included 101 participants from SMEs across various industries in Portugal, including education, IT, sales, administration, politics, finance, and marketing. The participants held various roles within their organizations, such as owners, salespeople, technicians, HR personnel, and employees. The demographic distribution within the participants regarding their age group and gender, can be seen in *Figure 1*. Due to the limited size and diversity of the people that got to respond to the survey, more than half of the participants found themselves within the 18- to 25-year-old group. This could be a point to improve next time, as it might affect the results by influencing the numbers due to uneven distribution.

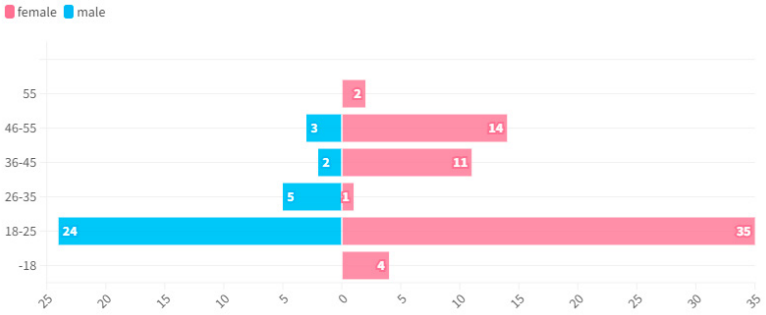

Figure 1. Age and gender distribution.

3.2.2. Current Cybersecurity Practices

Common cybersecurity measures adopted by the surveyed SMEs include antivirus software, two-factor authentication, and the use of strong passwords. However, only 25% of respondents avoid reusing passwords, and only 21% store their passwords in secure password managers. Notably, 3% of the participants reported not using any cybersecurity protection methods. Industry-specific differences were observed: the education sector showed the least adoption of cybersecurity measures, while those in IT, who enjoy the subject or fear losing information, were more likely to implement protections beyond basic strong passwords.

3.2.3. Challenges Faced by SMEs

SMEs face significant challenges in implementing cybersecurity measures, primarily due to limited financial resources and a lack of trained personnel. Approximately 50% of the surveyed individuals reported receiving no cybersecurity training, and only 22.5% received regular training and awareness programs. Of those who did receive training, only 31% found it effective or very effective, indicating that merely 10% of the participants benefited from effective cybersecurity training. These challenges underscore the need for more accessible and practical training solutions.

3.2.4. Awareness and Preparedness

The survey revealed, as can be seen in Figure 2, low levels of awareness and preparedness for cyber threats among SMEs. Only 9% of participants reported having high or very knowledge about cybersecurity, while 49.5% admitted to having low to no awareness or knowledge at all. IT and finance sectors showed higher levels of knowledge in cybersecurity awareness, whereas education and governance sectors scored the lowest. Despite these gaps, all participants agreed or strongly agreed that cybersecurity education should be integrated into school curriculums and workplace training programs, as we can see by 92.1% agreeing or strongly agreeing on cybersecurity training in companies, and 90.1% to teach it in schools.

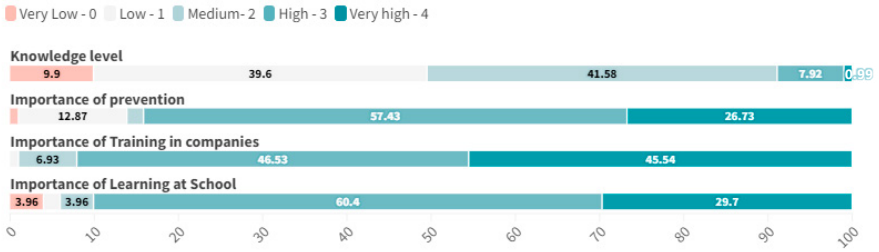

Figure. 2. Likert test results on knowledge level and importance of awareness.

3.2.5. Other Relevant Findings

A notable finding from the survey is the unanimous agreement on the importance of cybersecurity education both in schools and workplaces. This consensus highlights a collective recognition of the need for foundational cybersecurity knowledge to combat the increasing threat of cyberattacks.

3.3. Interview Insights

Interviews with cybersecurity experts revealed a multifaceted perspective on the potential and challenges of implementing advanced technologies like AI in SME cybersecurity. The consensus among experts underscores the importance of a balanced approach that integrates technological solutions with robust risk assessment and continuous employee training.

3.3.1. Cloud Cybersecurity and Resource Management

The research contacted a cloud provider specialist, who highlighted the advantages of cloud cybersecurity for SMEs, emphasizing scalable security solutions and cost-effective data protection. However, he cautioned that cloud solutions should only be adopted if they align with the company's specific needs and structure, warning against the costly nature of unnecessary implementations. This aligns with what an expert from one of the most renowned consultancy companies worldwide that we contacted said underscored the critical difficulties of SMEs to protect themselves, with their limited financial and human resources, and sated that they should focus on essential areas such as authentication, access management, and privacy. This expert's advice to develop the areas that SMEs can control the best, echoes the sentiments of other experts from the industry, who further advocated for greater governmental investment in companies advancing cybersecurity technologies, suggesting that increased support could accelerate the development of more secure solutions.

3.3.2. Risk Assessment and Regulatory Challenges

These experts noted that extensive risk assessment is a priority to access first, before making any cybersecurity investments. Understanding the specific risks and vulnerabilities is crucial for devising effective solutions. This advice fixated on prioritizing the risk was similar of the thoughts and comments shared by other experts, who highlighted the bureaucratic challenges SMEs face in complying with data protection laws and regulations. It was clear to every interviewee that extensive reporting requirements can make responding to cyberattacks slow and tedious, suggesting that a thorough understanding of risks can streamline compliance and response efforts.

3.3.3. The Role of AI and Employee Training

The experts also delved into the dual-edged nature of AI in cybersecurity. One of the experts contacted warned that "AI can be the very weapon that can be used against itself", highlighting the need for cautious implementation. Despite the potential risks, AI is recognized for its ability to enhance threat detection, automate response mechanisms, and predict potential attacks, provided it is integrated thoughtfully with existing systems.

Employee training emerged as a crucial element in strengthening cybersecurity defenses. It was emphasized that "the people are the weakest link when it comes to cyber vulnerability," advocating for comprehensive training programs to improve knowledge and skills. The last suggestion was for SMEs to create a multifaceted training approach, including online and offline teaching, phishing tests, newsletters, and gamified learning to maximize effectiveness. By focusing on practical and accessible security measures, we will be reinforcing the idea that human factors are as vital as technological advancements in cybersecurity.

Based on the survey and interview findings, several best practices for enhancing SME cybersecurity emerged:

- **Immediate Actions:** SMEs should prioritize enhancing employee training, conducting regular security audits, and adopting AI-driven security tools.
- **Long-term Strategies:** Strategic planning should include investments in advanced technologies like AI and quantum computing, alongside continuous improvement of cybersecurity policies tailored to SMEs' specific needs.
- **Collaboration and Support:** SMEs are encouraged to collaborate with industry experts, participate in cybersecurity networks, and seek support from government and industry programs.

4. Conclusion

Safeguarding SMEs against cyberattacks requires a balanced approach that includes thorough risk assessments, practical resource management, and tailored use of advanced technologies like AI and cloud computing. Our survey revealed that many SMEs lack advanced protections and proper training, with only a minority implementing secure practices such as unique passwords and password managers. Expert insights further emphasize the importance of continuous employee training to enhance cybersecurity knowledge and skills.

Despite the challenges, there is hope for SMEs to protect themselves effectively. By focusing on their most valuable asset, the information managed by their team, therefore they need to prioritize training their employees on cybersecurity. This approach not only addresses the technical aspects but also empowers the workforce to be the first line of defence against cyber threats.

Our future work will focus on testing various employee training methods within an actual SME to evaluate their effectiveness. We will implement a mix of online courses, phishing simulations, newsletters, and gamified learning modules, measuring improvements in cybersecurity awareness, knowledge, and behavior. The goal is to identify the most effective training strategies, providing valuable insights to strengthen cybersecurity defenses for SMEs.

5. Acknowledgements

This work was supported by Fundação para a Ciência e a Tecnologia, I.P. (FCT) [ISTAR Projects: UIDB/04466/2020 and UIDP/04466/2020].

6. References

1. Digital Transformation and Total Factor Productivity: Empirical Evidence from China. *Journal Name*, *Volume*(Issue),

Pages.
2. Solangi, Z., Solangi, Y., Murad, S., Sheikh Abdul Aziz, M., Hamzah, M., & Shah, A. (2018). The future of data privacy and security concerns in the Internet of Things. *Proceedings of the International Conference on Innovation and Research in the Digital Era (ICIRD)*, 1-4. https://doi.org/10.1109/ICIRD.2018.8376320
3. Building the Dashboard to Monitor and Analyze Data when Forecasting Risks in Integrated Management Systems. *Journal Name*, *Volume*(Issue), Pages.
4. AI in Cybersecurity: Bridging the Knowledge Gap. *Journal Name*, *Volume*(Issue), Pages.
5. Digital Society Future Transformation Perspectives in the Informational Age. *Journal Name*, *Volume*(Issue), Pages.
6. Impact of xG on Cybersecurity. *Journal Name*, *Volume*(Issue), Pages.
7. A generic reference indicating the need for continuous research and development of effective cybersecurity solutions for SMEs. (Specific paper not mentioned in the provided context).
8. European Commission SMEs report. *Journal Name*, *Volume*(Issue), Pages.
9. Hollman, K. W., & Mohammad-Zadeh, S. (1984). Risk management in small business. *Journal of Small Business Management*, *1*, 47–55.
10. Renaud, K., & Weir, G. R. S. (2016). Cybersecurity and the Unbearability of Uncertainty. In *Proceedings of the 2016 Cybersecurity Cyberforensics Conference*, IEEE, 137–143.
11. Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. *Journal Name*, *Volume*(Issue), Pages.
12. Barlette, Y., Gundolf, K., & Jaouen, A. (2017). CEOs' information security behavior in SMEs: Does ownership matter? *Systemes d'Information et Management*, *22*(3), 7–45.
13. Berry, C. T., & Berry, R. L. (2018). An initial assessment of small business risk management approaches for cybersecurity threats. *International Journal of Business Continuity and Risk Management*, *8*(1), 1–10.
14. Brustbauer, J. (2016). Enterprise risk management in SMEs: Towards a structural model. *International Small Business Journal*, *34*(1), 70–85.
15. Falkner, E. M., & Hiebl, M. R. W. (2015). Risk management in SMEs: A systematic review of available evidence. *Journal of Risk Finance*.
16. Nicolaou, N. (2008). The impact of internal and external factors on SMEs' strategic choices: Evidence from the UK. *Journal of Business Research*, *61*(4), 227-231.
17. Arunrat, N., & Heerdegen, G. (2019). Risk management in SMEs: A literature review and research agenda. *Journal of Small Business Management*, *57*(2), 334-362.
18. Panourgias, N. S., et al. (2011). How do small and medium enterprises manage and sustain change? A literature review. *Journal of Change Management*, *11*(1), 15-35.
19. Short, J. C., et al. (1993). Perceptual and archival measures of Miles and Snow's strategic types: A comprehensive assessment of reliability and validity. *Journal of Management*, *19*(1), 85-117.
20. Mazzarol, T., & Reboud, S. (2010). Strategic planning in small and medium enterprises: A note on research and applications. *International Small Business Journal*, *28*(1), 43-49.
21. Naab, E., & Knight, A. (2006). Risk management in small and medium-sized enterprises. *Journal of Small Business and Enterprise Development*, *13*(2), 175-187.
22. Amos, A., et al. (2013). Understanding how SMEs identify, assess, manage, and respond to risk. *Journal of Small Business and Enterprise Development*, *20*(1), 46-66.
23. Brouard, F., et al. (2010). Environmental strategy and organizational design in small firms: Insights from the French organic food industry. *Business Strategy and the Environment*, *19*(7), 436-450.
24. Mackenzie, H., & McAllister, P. (2014). Work–life balance and informal learning in small businesses: Perspectives of owner-managers. *Journal of Workplace Learning*, *26*(2), 85-102.
25. Lawrence, S., & Turner, M. J. (2011). An exploration of management consultancy as a mode of intervention in small and medium-sized enterprises. *International Small Business Journal*, *29*(6), 629-650.
26. NCSA. (2018). Stay Safe Online - Cybersecurity Awareness Toolkit for SMB. *National Cyber Security Alliance*. Retrieved from https://staysafeonline.org
27. ISF. (2002). Effective security awareness. *Information Security Forum*.
28. British Assessment Bureau. (2024). SME Cyber Security: The Impact of AI and Trends to Watch in 2024. Retrieved from https://www.british-assessment.co.uk/insights/sme-cyber-security-the-impact-of-ai-and-trends-to-watch-in-2024/
29. World Economic Forum. (2024). SMEs can turn cybersecurity risk into opportunity – here's how. Retrieved from https://www.weforum.org/agenda/2024/07/smes-can-turn-cybersecurity-risk-into-opportunity-heres-how/