SMALL AND MEDIUM BUSINESSES AND THEIR PERCEPTION ON CYBERSECURITY

Musaed Sadeq Musaed Al-Fareh, Musaed, Pierezza, Edoardo, Davila Cadena, Felipe, and Roelevink, Bread

27-09-2024

1 Introduction

The increasing digitization of businesses necessitates that organizations, especially small and medium-sized enterprises (SMEs), address significant cybersecurity challenges. Unlike larger organizations, which typically have dedicated resources for robust cybersecurity measures, SMEs often face more hurdles due to limited financial and technical capabilities (Rawindaran et al. (2023); Haastrecht et al. (2021)). Consequently, SMEs are frequently targeted by cybercriminals, leading to severe consequences such as financial losses, reputational damage, and legal ramifications.

While extensive research (e.g., ENISA (2021); Inayatulloh (2020)) has explored the technical aspects of cybersecurity implementation and the impact of cyberattacks on SMEs, a notable gap exists regarding SMEs' perceptions of these measures. Understanding these perceptions is crucial, as they directly influence cybersecurity decisions, investment strategies, and overall preparedness. For instance, Rawindaran et al. (2022) underscore the role of awareness in shaping SMEs' cybersecurity approaches, while Inayatulloh (2020) highlights the importance of knowledge acquisition in fostering security adoption.

This study aims to fill this gap by analyzing how SMEs perceive cybersecurity measures to protect customer data. By exploring this topic from various perspectives, this research seeks to provide valuable insights that can enhance the security strategies of SMEs and inform future policy recommendations.

1.1 Research Question

The rise in cybersecurity threats poses a significant risk to SMEs, which often lack the necessary resources and expertise to implement robust cybersecurity measures. As Chaudhary et al. (2023) point out, many SMEs remain unaware of critical vulnerabilities, limiting their ability to effectively respond to cyber threats. Similarly, Amrin (2014) emphasize that SMEs frequently prioritize short-term operational needs over long-term investments in cybersecurity, exacerbating their risks. Addressing the gap in the literature, which primarily focuses on larger enterprises, this study explores the unique challenges and perceptions of SMEs regarding cybersecurity Erdogan et al. (2023). By examining SMEs' awareness of cyber risks and their readiness to adopt security measures, this research will offer insights into improving their resilience against cyberattacks.

Main research question: **How do SMEs perceive cybersecurity measures to protect customer data?**

To be able to answer this research question, we will consider the following sub-questions:

1. Is there a significant relationship between the industry sector and SMEs' perceptions of the importance and influence of cybersecurity measures?

2. Is there a difference in the perception of the importance of cybersecurity measures among SME employees based on the company size?
3. How do SMEs address the key challenges they encounter in protecting data and maintaining privacy?
4. Does work experience influence the knowledge an SME employee has in cybersecurity measures?

2 Literature Study

2.1 Perception of Cybersecurity across Industries

The topic of SMEs and their cybersecurity practices has gained increasing attention in recent years, particularly as cyber threats continue to evolve and target businesses of all sizes, including those that are more vulnerable. Several studies have been conducted to understand how different industry sectors perceive the importance of cybersecurity and the factors influencing the implementation of protective measures.

A study by Rawindaran et al. (2022) examined SMEs in Wales, revealing variations in cybersecurity awareness and implementation across different sectors. The research indicated that industries with less digitization, such as retail and wholesale, demonstrate lower levels of cybersecurity awareness compared to sectors like finance and healthcare. The findings suggest that SMEs often prioritize business operations over adopting advanced cybersecurity measures, partly due to limited knowledge and a lack of industry-specific guidance. Notably, only 30 percent of the surveyed SMEs understood the terminology associated with cybersecurity, underscoring the need for enhanced education and resources in this area.

In addition, a peer-reviewed study presented at the 16th International Conference on Availability, Reliability, and Security in 2021 examined the cybersecurity competence of SMEs across various industries. The research revealed that sectors such as financial services and healthcare demonstrate more advanced cybersecurity practices due to stricter regulatory requirements. Conversely, industries like retail and hospitality exhibit lower levels of implementation due to perceived lower risk and resource constraints. The study also discussed the influence of industry-specific vulnerabilities, noting that cybersecurity awareness and threat preparedness tend to improve in industries where regulations are tighter and risks are more apparent.

Both studies highlight the critical role of industry in shaping cybersecurity perceptions and practices among SMEs. They underscore the need for tailored cybersecurity strategies that consider sector-specific risks, regulatory environments, and the maturity of IT infrastructure. These studies indicate a significant gap in cybersecurity practices within less-regulated industries, warranting further exploration and policy intervention.

Haastrecht et al. (2021) emphasized that SMEs are not a homogeneous group, and their approaches to cybersecurity vary based on their expertise and awareness levels. They proposed a classification framework with five types of SMEs: cybersecurity-abandoned SMEs, unskilled SMEs, expert-connected SMEs, capable SMEs, and cybersecurity-provider SMEs. These categories are crucial for understanding that uniform solutions are ineffective for SMEs. For instance, cybersecurity-abandoned SMEs lack awareness and often do not have cybersecurity policies, whereas capable SMEs possess a well-developed cybersecurity framework and continuously monitor threats. Such classifications are vital for tailoring solutions, tools, and communication strategies to enhance cybersecurity competence.

2.2 SMEs perception of cybersecurity given the size of the company

Larger SMEs tend to perceive cybersecurity as a critical component of their business operations. They often have more resources to dedicate to cybersecurity tools, personnel, and awareness programs. studies such as this one made by Rawindaran et al. (2023) show that larger SMEs are more likely to prioritize cybersecurity due to their larger digital footprints and greater exposure to risk. Additionally, they often face more stringent regulatory pressures, especially when handling customer data, which forces them to focus on compliance measures like GDPR.

For example, the EU paper (ENISA, 2021) on cybersecurity highlights that larger SMEs are more proactive in their cybersecurity efforts, often investing in advanced threat detection and prevention measures. Their increased budget allows them to invest in more sophisticated solutions such as firewalls, intrusion detection systems, and employee training programs.

Instead Small SMEs (less than 50 employees) , and micro-enterprises with fewer than 10 employees, often do not perceive cybersecurity as a top priority. This group typically lacks the financial and technical resources to implement comprehensive cybersecurity strategies how it is stated by Rawindaran et al. (2023). Many smaller SMEs focus on immediate business survival and operations, rather than long-term risk mitigation.

Research conducted on Welsh by Rawindaran et al. (2023) SMEs showed that smaller businesses had limited awareness of the importance of cybersecurity. Only 30 percent of the sampled SMEs in this study understood key cybersecurity concepts, and many had gaps in their awareness of intelligent cybersecurity solutions, such as machine learning algorithms for threat detection. This suggests that smaller SMEs might not view cybersecurity as a pressing concern unless they have already experienced a cyber incident.

Threat Awareness and Risk Perception

Larger SMEs tend to perceive themselves as more vulnerable to cyberattacks due to their greater exposure to digital operations how it was highlighted in this two papers made by Amrin (2014) and Rawindaran et al. (2023). With a broader network of customers, partners, and employees, they recognize the importance of securing their data and systems. As such, they often incorporate cybersecurity into their business strategies. A study by ENISA (2021) found that larger SMEs were more likely to undergo cybersecurity audits and implement risk management frameworks .

Additionally, larger companies are more likely to conduct regular cybersecurity training for their employees, increasing threat awareness across the organization. This contributes to a more security-focused culture, where employees are seen as a crucial line of defense against cyber threats how is again stated in the research paper ENISA (2021).

Threat Awareness in Smaller SMEs In contrast, tend to have lower levels of threat awareness but still their level of risk is still very high. Instead they believe that their smaller size often gives them the false perception that they are not prime targets for cyberattacks. However, as cybercriminals increasingly target vulnerable organizations, this perception has proven dangerous. Research such as the one made by Lejaka (2021) shows that small SMEs often only invest in cybersecurity after a breach has occurred, due to their limited budgets and lack of cybersecurity expertise.

A South African study by Lejaka (2021), reveal that smaller SMEs struggle with cybersecurity due to a lack of resources and insufficient knowledge on how to implement effective security practices.

Factors Influencing Cybersecurity Perceptions

The size of an SME influences not only its perception of cybersecurity but also how it responds to threats it is stated by Rawindaran et al. (2023). Larger SMEs benefit from having dedicated IT departments or access to cybersecurity professionals. In contrast, smaller SMEs often rely on outsourced IT services or basic off-the-shelf software, which may not be sufficient to counteract advanced cyber threats.

Conclusion

The size of an SME plays a significant role in shaping its perception of cybersecurity importance and threat awareness. Larger SMEs tend to take cybersecurity more seriously, allocating more resources to it, while smaller SMEs often deprioritise it, largely due to resource constraints and a lack of expertise. As cyber threats continue to grow in sophistication, it is critical that SMEs of all sizes increase their awareness of cybersecurity risks and invest in more robust protections to safeguard their business operations.

2.3 Challenges Faced by SMEs in Cybersecurity

2.3.1-**Financial Constraints and Limited Resources**

A significant challenge faced by SMEs is their inability to allocate sufficient funds for effective cybersecurity investments. Haastrecht et al. (2021) indicated that due to limited financial resources, SMEs often cannot afford advanced security systems, thereby increasing their exposure to cyber risks. These financial constraints hinder SMEs from accessing innovative cybersecurity tools and acquiring expert services, which are essential for enhancing their cybersecurity posture.

2.3.2-**Knowledge Gaps and Technical Expertise Deficiency**

Many SMEs lack the awareness and skills necessary to effectively manage their cybersecurity challenges. Rawindaran et al. (2023) found that while most SME owners understand the general aspects of cybersecurity, their comprehension of topics related to machine learning and artificial intelligence is limited. This lack of knowledge may hinder their ability to adopt these technologies, which typically require significant financial investment and technical expertise.

2.3.3-**Lack of Adequate Testing Environments**

Inayatulloh (2020) notes that SMEs often cannot afford or dedicate resources to create testing environments for cybersecurity. This limitation hinders their ability to conduct necessary tests and prepare for potential cyber incidents. Unlike larger organizations that can invest in comprehensive incident response training, SMEs frequently lack the means to develop these capabilities. As an alternative, SMEs may consider collaborating with third-party providers or licensing packages to access necessary testing and training resources, ensuring they remain prepared for potential cybersecurity threats.

Barriers to Implementing Cybersecurity Measures

2.3.4-**Complexity of Cybersecurity Solutions**

While SMEs may possess a general awareness of existing cybersecurity solutions, their ability to implement these measures is often hindered by the complexity of the technologies involved. According to Haastrecht et al. (2021), many SMEs, particularly those with lower levels of digital maturity, encounter significant difficulties with the technical aspects of these solutions. Rawindaran et al. (2022) further support this by indicating that SMEs may recognize available cybersecurity options, but their understanding of how to apply these technologies effectively is limited. Additionally, Haastrecht et al. (2021) emphasize that the solutions are frequently not tailored to the specific needs and capacities of SMEs, resulting in a disconnect between awareness and effective implementation. This complexity can lead to frustration and reluctance to invest in cybersecurity measures, as highlighted byRawindaran et al. (2022), ultimately further exposing SMEs to potential risks.

2.3.5-**Priorities Mismatch**

SMEs often experience a discrepancy in their priorities when it comes to cybersecurity. Many SMEs do not prioritize advanced technologies such as Artificial Intelligence (AI) and Machine Learning (ML), leading to insufficient awareness and education regarding the significance of these tools in enhancing cybersecurity measures Rawindaran et al. (2023). This lack of focus on emerging technologies can hinder their ability to effectively protect against evolving cyber threats.

Current Approaches and Potential Solutions

2.3.6-**Socio-Technical Frameworks**

According to Haastrecht et al. (2021), it is recommended that SMEs utilize socio-technical frameworks that take into account both human and technical aspects to effectively address their cybersecurity requirements. These frameworks suggest that SMEs be classified based on their level of digitalization, which refers to the extent to which they adopt digital technologies in their operations. Subsequently, the cybersecurity measures should be tailored to align with this classification. For example, SMEs with low digitalization levels may require more basic cybersecurity training and solutions, while those with higher digitalization levels may benefit from more advanced protective measures that incorporate AI and ML to enhance threat detection and response.

2.3.7-**Government Support and Policy Interventions**

In conclusion, enhancing cybersecurity within Small and Medium Enterprises (SMEs) requires significant support from the government. According to Rawindaran et al. (2023), various literature sources indicate that financial measures such as grants, subsidies, and educational interventions can effectively alleviate the resource constraints commonly faced by SMEs. For instance, studies have shown that financial assistance programs can enable SMEs to invest in necessary cybersecurity technologies and training, ultimately improving their security posture.

Moreover, engagement with government stakeholders is essential for guiding SMEs toward areas that require attention. This includes the implementation of training programs focused on cybersecurity awareness. General awareness campaigns have also been identified as effective strategies for enhancing cybersecurity among SMEs, as they help to inform business owners and employees about potential threats and best practices for prevention.

Gaps in the Literature

There are critical areas that remain unexplored regarding the identification of distinct small and medium-sized enterprise (SME) requirements across different categories, as well as the overall effectiveness and sustainability of available interventions. More evidence is needed to study how the increasing use of artificial intelligence (AI) and machine learning (ML) services can be tailored to various industries, particularly for SMEs, and to evaluate the effects of such interventions in conjunction with corresponding governmental policies.

2.4 SME employees knowledge of cybersecurity given years of experience

The literature about cybersecurity knowledge shines a light on the influence of both experience and organizational culture on people's awareness and practices. Studies have shown that employees with more years of experience tend to show a higher knowledge of cybersecurity measures, but this knowledge does not always make for better security behavior. Research from Bhaskar (2022) points out that organizational culture, including factors such as communication, risk aversion, and power dynamics, can hinder cybersecurity effectiveness despite experience levels. For example, even experienced employees could be less proficient in security measures due to a lack of training or organizational support for measures like multi-factor authentication (Bhaskar, 2022). Furthermore, research from Akter et al. (2022) shows that knowledge in cybersecurity can improve through education and continual adaptation to evolving threats, suggesting that while experience is valuable, ongoing training is crucial to maintaining high-quality cybersecurity practices.

3 Methodology

To understand and solidify the topic for our research questions, we will use appropriate techniques for data collection, combining both quantitative and qualitative approaches. This allows us to effectively choose the most suitable methods for addressing the research questions.

For data collection, we will use qualitative methods such as structured interviews and case studies. These will help us gain deeper insights into our topic and enable us to target the right group for effective responses. In addition, quantitative methods will involve developing specific survey questions tailored to align with our research objectives. The survey will assist in determining whether our research questions contribute to meaningful improvements for SMEs.

In our Data Management Plan (DMP), we will outline how data is collected, stored, and protected to maintain integrity and ensure compliance with ethical and regulatory standards. Data storage will be managed on a secure platform, especially for sensitive information like interview and survey responses. Regarding data retention, we plan to keep the data only for the duration of the project, with a maximum retention period of five years if needed for validation. Ethical

considerations will be central to our methodology, with participants providing informed consent through a consent form, especially when handling sensitive data. We will carefully choose sampling methods for both qualitative and quantitative approaches to ensure they are appropriate and suitable for our research. The sampling techniques will adhere to the guidelines we have studied to minimize bias. For data analysis, we plan to use coding software such as NVivo or ATLAS.ti

for qualitative data. For quantitative data, we will employ techniques like descriptive statistics, regression analysis, or hypothesis testing, depending on the nature of the data. Ensuring reliability and validity in our data collection instruments is essential, and we will use established measurement scales, particularly for assessing cybersecurity awareness. We also

recognize potential limitations, such as small sample sizes or respondent bias, which we will address to ensure they do not significantly affect the research outcomes.

4 PREDICTED OUTCOMES

The predicted outcomes of this research, centered on the main question of how SMEs perceive cybersecurity measures to protect customer data and the challenges they face, suggest several key insights. It is anticipated in this proposal that SMEs generally perceive cybersecurity as important, even though their level of understanding and implementation varies widely based on factors such as industry, size, and strategies of the business. Many SMEs are likely to recognize the need for cybersecurity to protect customer data, but they may face significant challenges in implementing effective measures due to limited resources, lack of expertise, and insufficient knowledge about advanced technologies like AI.

This research is expected to reveal that SMEs encounter common challenges in cybersecurity practices, such as financial limits, difficulties in maintaining up-to-date security protocols, and a lack of awareness about evolving threats. The research aims to highlight how these challenges impact SMEs' ability to protect customer data effectively. Furthermore, it is predicted that while some SMEs may be aware of advanced cybersecurity solutions like AI, they may be hesitant to adopt these technologies due to concerns about cost, complexity, and a lack of understanding of their benefits.

Bigger SMEs might be more open to adopting innovative cybersecurity measures, viewing them as integral to their business strategy. In contrast, smaller SMEs may rely on traditional security practices and face challenges in adapting to expensive technologies. The study also anticipates a need for increased education and support for SMEs in developing effective cybersecurity strategies, particularly in sectors with less regulatory oversight or fewer resources.

The following hypotheses are proposed for the main research question:

1. **H0 (Null Hypothesis):** SMEs do not perceive significant challenges in implementing cybersecurity measures to protect customer data.
2. **H1 (Alternative Hypothesis):** SMEs perceive significant challenges in implementing cybersecurity measures to protect customer data.

For each quantitative subquestion, we have designed specific hypothesis:

4.1 Perception of Cybersecurity across Industries

1. **H0 (Null Hypothesis):** There is not a significant relationship between industry sector and SME's perceptions of the importance of cybersecurity measures.
2. **H1 (Alternative Hypothesis):** There is a significant relationship between industry sector and SME's perceptions of the importance of cybersecurity measures due to the fact that certain industries dedicate more resources to the confidentiality of their data.

4.2 Perception of Cybersecurity based on company size

1. **H0 (Null Hypothesis):** There is no difference in the perception of the importance of cybersecurity measures among SME employees based on the company size.
2. **H1 (Alternative Hypothesis):** There is a difference in the perception of the importance of cybersecurity measures among SME employees based on the company size due to greater exposure, handling larger volumes of data and stricter requirements.

4.3 Knowledge of Cybersecurity based on work experience

1. **H0 (Null Hypothesis):** Work experience does not influence the knowledge on cybersecurity measures of an SME employee.
2. **H1 (Alternative Hypothesis):** Work experience does influence the knowledge on cybersecurity measures of an SME employee due to longer exposure to risks, policies, and training within the company.

The third sub-question ”How do SMEs address the key challenges they encounter in protecting data and maintaining privacy?” is a qualitative research question, and therefore does not need a formal hypothesis because it seeks to explore and understand the experiences, practices, and strategies used by SMEs, rather than test a specific, measurable relationship between variables.

In qualitative research, the goal is to generate insights, uncover patterns, and provide a deeper understanding of how SMEs handle these challenges, which requires open-ended inquiry rather than predefined predictions.

In conclusion, the predicted outcomes suggest that SMEs generally perceive cybersecurity measures as essential for protecting customer data. However, variations are likely depending on factors such as industry sector, company size and employee experience. Companies belonging to expensive industries may invest and prioritize better cybersecurity options, while other industries avoid big spending in this area. On the other hand, larger SMEs may prioritize cybersecurity more due to higher data volumes and regulatory pressures, while smaller SMEs might view it as less urgent. Additionally, employees with more work experience are expected to demonstrate greater knowledge of cybersecurity measures, but newer employees could bring updated insights from recent training. These differences will shape how cybersecurity is implemented and valued across SMEs.

References

Shahriar Akter, Mohammad Rajib Uddin, Shahriar Sajib, Wai Jin Thomas Lee, Katina Michael, and Mohammad Alamgir Hossain. Reconceptualizing cybersecurity awareness capability in the data-driven digital economy. *Annals of operations research*, pages 1–26, 2022.

Nabila Amrin. The impact of cyber security on smes. Master's thesis, University of Twente, 2014.

R Bhaskar. Better cybersecurity awareness through research. *ISACA Journal*, 3:1–10, 2022.

Sunil Chaudhary, Vasileios Gkioulos, and Sokratis Katsikas. A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. *Computer Science Review*, 50:100592, 2023.

ENISA. Cybersecurity for smes, 2021.

Gencer Erdogan, Ragnhild Halvorsrud, Costas Boletsis, Simeon Tverdal, and J Brian Pickering. Cybersecurity awareness and capacities of smes. 2023.

M. Haastrecht, I. Sarhan, A. Shojaifar, L. Baumgartner, W. Mallouli, and M. Spruit. A threat-based cybersecurity risk assessment approach addressing sme needs. In *Proceedings of ARES 2021: The 16th International Conference on Availability, Reliability, and Security*, volume 158. Association for Computing Machinery, 2021. doi: 10.1145/3465481.3469199.

Inayatulloh. Technology acceptance model (tam) for the implementation of knowledge acquired model for sme. In *2020 International Conference on Information Management and Technology (ICIMTech)*, pages 767–770. IEEE, 2020.

Tebogo Lejaka. A framework for cyber security awareness in small, medium and micro enterprises (smmes) in south africa. *University of South Africa*, 2021.

Nisha Rawindaran, Ambikesh Jayal, and Edmond Prakash. Exploration of the impact of cybersecurity awareness on small and medium enterprises (smes) in wales using intelligent software to combat cybercrime. *Computers*, 11(12):174, 2022.

Nisha Rawindaran, Ambikesh Jayal, Edmond Prakash, and Chaminda Hewage. Perspective of small and medium enterprise (sme's) and their relationship with government in overcoming cybersecurity challenges and barriers in wales. *International Journal of Information Management Data Insights*, 3(2):100191, 2023.