How do SMEs perceive cybersecurity measures to protect customer data?

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

Oct 30, 2024

Abstract

In today's rapidly digitizing economy, small and medium-sized enterprises (SMEs) form the backbone of global business, representing over 90% of companies and driving innovation, job creation, and economic growth (Algan 2019). However, SMEs face significant cybersecurity challenges with increasing reliance on digital tools. Unlike large corporations with robust resources, SMEs often lack the financial means, expertise, and personnel needed to defend against sophisticated cyber threats, making them especially vulnerable to attacks that can result in financial loss, operational disruption, and reputational harm (Jahankhani, Kilpin, and Kendzierskyj 2022).

This paper investigates SMEs' perceptions of cybersecurity risks, using both qualitative interviews and a survey of 154 SME employees to explore how industry sector, company size, and resource constraints shape cybersecurity preparedness. The findings reveal notable confidence gaps, with sectors such as IT and finance showing stronger cybersecurity measures, while industries like agriculture and public relations report lower levels of preparedness due to limited resources and regulatory variations.

To address these disparities, this study recommends sector-specific cybersecurity guidelines, financial incentives, and public-private partnerships to support SMEs in developing resilient cybersecurity practices. These recommendations aim to bolster SMEs' ability to protect customer data and ensure business continuity, contributing to a more secure and resilient digital economy.

1 Introduction

In today's digital economy, small and medium-sized enterprises (SMEs) are the backbone, accounting for over 90 % of global businesses and significantly contributing to innovation, job creation, and economic growth (Algan 2019). With rapid technological advancement, SMEs have access to unique opportunities for scaling and competing in global markets. However, this increased reliance on digital infrastructure also exposes them to growing cybersecurity threats. Unlike large corporations with substantial resources dedicated to robust cybersecurity, SMEs often lack the financial means, technical expertise, and dedicated personnel necessary to defend against sophisticated cyber threats effectively (Jahankhani, Kilpin, and Kendzierskyj 2022). This gap in resources makes SMEs especially vulnerable to cyberattacks, leading to potential financial loss, operational disruptions, and reputational damage that can be difficult for smaller businesses to recover from.

1.1 Problem Statement

Despite SMEs' substantial economic role, cybersecurity policies and regulations tend to adopt a one-size-fits-all approach, often overlooking the unique challenges SMEs face. This generalization can leave SMEs at a disadvantage, particularly as industry-specific factors play a critical role in shaping both the types

of cybersecurity threats they encounter and the strategies they can employ. For instance, SMEs in the finance and healthcare sectors must comply with stringent regulations due to the highly sensitive nature of their data, while those in retail or manufacturing may face different kinds of cybersecurity risks. Consequently, SMEs across various sectors have varying levels of vulnerability and differing needs for cybersecurity measures, creating a pressing need for policies that recognize these distinctions.

1.2 Purpose and Objective

The purpose of this policy paper is to address the cybersecurity gap faced by SMEs by examining how sector-specific characteristics influence their cybersecurity needs and practices. By investigating these industry-specific challenges, this paper aims to provide policymakers with targeted recommendations that can enable SMEs to implement cybersecurity measures that are feasible within their resource constraints. This approach underscores the importance of adapting cybersecurity strategies to reflect the specific operational and regulatory environments of each sector, thereby improving the effectiveness of policies aimed at protecting SMEs from cyber threats.

1.3 Significance for Policymakers and Stakeholders

For SMEs, cybersecurity is more than a technical necessity; it is a foundational component of business resilience and trust. As SMEs strive to protect customer data and maintain operational continuity, policymakers, business owners, and cybersecurity experts must work together to develop sector-focused policies that address these distinct challenges. The insights from this paper aim to bridge the current gaps in cybersecurity policy by offering actionable solutions that SMEs in various industries can implement within their unique constraints. Through such targeted strategies, SMEs can be better equipped to defend against cyber threats, thereby strengthening the broader economic ecosystem in which they operate.

2 Approaches of the research

We decided to analyze both qualitative and quantitative data to answer our research questions.

2.1 Qualitative Data

To gather qualitative data we interviewed 6 different SMEs employees and we decided to then create a thematic analysis for each interview. Our goal in conducting this interview was to deeply explore how small and medium-sized enterprises (SMEs) manage cybersecurity and data privacy challenges. The design of the interview was a semi-structured one, we chose this format to enable interviewers to cover essential research questions while enabling participants to share insights openly, resulting in more comprehensive data collection. The interviews were between 15 to 25 minutes long, conducted either in person, over the phone, or via video calls to accommodate participant availability. Audio recordings of each interview (with prior consent) ensured accuracy, and interviews were later transcribed verbatim for analysis

To collect participants purposive sampling was used, which enabled the participants to be persons with experience in cybersecurity decision-making or management within their SMEs. The participant pool was diverse, representing a range of industries, thus enhancing the depth of the insights obtained. Recruitment was carried out through LinkedIn, personal networks, industry events, and targeted internet searches, allowing for a broad yet focused sample of participants.

As it was stated before thematic analysis as outlined by Braun and Clarke (2006) was used at the end of the data-gathering process to analyze them. This process involved six steps:

- Familiarization with the data through repeated readings of transcripts.
- Generating initial codes by identifying key phrases and concepts.
- Searching for themes by organizing codes into broader categories.
- Reviewing themes to refine and ensure their relevance.
- Defining and naming themes to capture the essence of each.
- Writing the report to present findings with direct quotes that illustrate key insights.

This approach enabled the identification of patterns and common themes related to the cybersecurity and privacy strategies employed by SMEs, offering a comprehensive understanding of these challenges.

2.2 Quantitative Data

Alternatively, if the attempt is to explore the relationship between variables, quantitative research is a solid approach to answer the research question. Therefore, a survey was created to record quantitative data. Made of over 60 questions, the survey focuses on a sample used in the study, which consists of 154 respondents, all employees of SMEs located in Brabant working with DigiWerkPlaats, who provided a vast amount of data that created deep insights when analyzed. The survey comprised a mix of Likert scale questions (ranging from 1 =" Strongly Disagree" to 5 =" Strongly Agree") and multiple-choice questions to capture employees' attitudes toward cybersecurity. Every quantitative sub-research question had both types of hypotheses, null and alternative, which

would provide answers to the research question further on. The data was collected online through Qualtrics over a few days prior to these studies, ensuring that the information was as recent and accurate as possible. Additionally, the help of DigiWerkPlaats as a mediator for distribution likely motivated participants to respond, as personnel in the companies may be interested in the results that the research will provide.

2.3 Ethical Considerations

Both in our Qualitative and quantitative data collection strict ethical guidelines were followed, Participants of the interview were informed about the study's objectives and assured of confidentiality and anonymity. All data were stored securely, with access limited to authorized researchers, ensuring participant privacy and compliance with ethical standards. The participants of the survey for the quantitative data were able to read a paper where it was described how we were going to use their data.

3 Results

This section presents the consolidated findings from the research, exploring the perceptions and practices of SMEs regarding cybersecurity across different dimensions. The data is presented quantitatively and qualitatively to illustrate how company size and sector impact cybersecurity awareness, resource allocation, and practical measures.

3.1 Impact of Company Size on Employee Perceptions of Cybersecurity

In line with the research objective, we analyzed the relationship between company size and employees' perceptions of cybersecurity using descriptive statistics and t-tests. As shown in Table 1, the analysis examined key variables, including the perceived importance of cybersecurity, knowledge of cybersecurity practices, confidence in the company's cybersecurity measures, and familiarity with policy adherence consequences.

Table 1: Descriptive Statistics of Responses by Company Size (n = 40 for Small Companies, n = 89 for Large/Very Large Companies)

Question	Small Mean	Small SD	Large Mean	Large SD
Importance of Cybersecurity for Role	3.23	1.19	3.71	1.13
Knowledge of Cybersecurity Practices	3.28	0.82	3.63	0.96
Confidence in Cybersecurity Measures	2.28	1.01	2.85	1.03
Familiarity of Not Adhering to Policies	3.30	1.29	3.61	1.25

A significant difference was found in confidence levels in cybersecurity measures between small and large companies, with employees at larger organizations showing greater confidence ($p = 0.004$, Bonferroni-corrected) Table 2. This discrepancy likely reflects the broader resources and investments in cybersecurity typically available to larger companies. In contrast, no statistically significant

differences were found for perceived importance, knowledge, or familiarity, suggesting that employees across company sizes share similar awareness and understanding of cybersecurity, even if their confidence in actual measures varies.

Table 2: T-test Results with P-values and Significance

Question	T-statistic	P-value	Significance
Importance of Cybersecurity for Role	-2.21	0.29	Fail to reject null hypothesis
Knowledge of Cybersecurity Practices	-2.03	0.044	Fail to reject null hypothesis
Confidence in Cybersecurity Measures	-2.97	0.004	reject null hypothesis
Familiarity Not Adhering to Policies	1.28	0.203	Fail to reject null hypothesis

3.2 Cross-tabulation and Visualization of Confidence Levels by Sector

A cross-tabulation analysis (Table 3) and a stacked bar chart (Figure 1) were used to examine confidence in cybersecurity measures across different industry sectors. The cross-tabulation shows varied levels of confidence, with sectors like *Information Technology (IT)* and *Finance* exhibiting higher confidence levels. In contrast, sectors such as *Agriculture* and *Public Relations and Marketing* demonstrated comparatively lower confidence levels. These sectoral variations suggest that industries with greater data sensitivity and regulatory pressures may invest more heavily in cybersecurity, fostering higher confidence among employees.

Confidence	A great deal	A little	A lot	A moderate amount	None at all
Agriculture and Food Production	1	1	0	1	0
Chemical Industry	0	0	1	1	0
Construction and Engineering	2	2	2	2	0
Consulting and Professional Services	2	1	0	3	0
Education	0	4	2	4	0
Environmental Services	0	0	1	0	0
Finance and Banking	12	2	4	3	0
Government and Public Sector	0	0	4	1	0
Healthcare and Pharmaceuticals	2	2	0	1	0
Hospitality	0	1	2	2	0
Hotel	0	1	0	0	0
Information Technology (IT)	9	0	10	6	0
Insurance	1	0	0	1	0
Legal Services	1	0	2	3	0
Manufacturing	2	1	2	2	0
Media and Entertainment	2	0	2	5	0
Mining and Natural Resources	0	0	0	1	0
Non-Profit and NGOs	0	1	1	2	0
Private Equity and Investment	1	0	1	0	0
Public Relations and Marketing	2	0	3	1	0
Real Estate	0	0	1	1	0
Retail and E-commerce	2	1	3	3	0
Shipping and Maritime	0	1	1	0	0
Sports and Recreation	0	1	0	0	1
Telecommunications	3	0	2	0	0
Transportation and Logistics	0	1	2	0	0

Table 3: Cross-Tabulation of Sector and Confidence

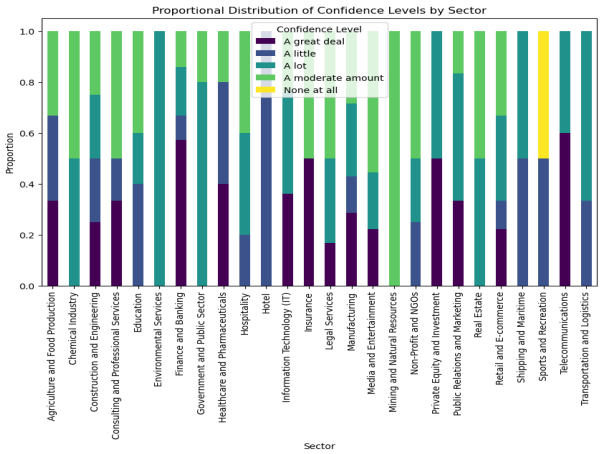

Figure 1: Proportional Distribution of Confidence Levels by Sector

A Chi-Square test ($p = 0.00014$) confirmed a significant relationship between sector and confidence levels, suggesting that industry-specific practices influence employee confidence in cybersecurity. This finding underscores the need for tailored cybersecurity strategies by sector to align with specific industry requirements.

3.3 Interview Analysis: Challenges Faced by SMEs in Cybersecurity

Through thematic analysis of interviews, four key themes emerged that provide further insights into the cybersecurity challenges faced by SMEs:

Reliance on External Providers: Many SMEs, especially those with limited in-house expertise, rely on Managed Security Service Providers (MSSPs) to handle cybersecurity. Several participants mentioned outsourcing tasks like threat monitoring and incident response due to limited internal resources. However, some expressed concerns regarding data control when relying on external entities, though this was not widely elaborated upon.

Financial Constraints: Financial limitations frequently emerged as a barrier to cybersecurity investment. Participants noted budget constraints that prevent hiring specialized staff or purchasing advanced security software, with one participant stating, "Our budget doesn't allow for hiring additional cybersecurity staff." This finding highlights the tension between budget priorities and cybersecurity, pointing to a need for affordable, scalable cybersecurity solutions for SMEs.

Awareness and Resource Limitations among Small SMEs: Smaller enterprises, particularly those with fewer than 20 employees, struggle with cybersecurity awareness and resource allocation, often relying on a single ICT or general IT employee to manage cybersecurity. One participant commented, "We have one ICT person, and they manage everything, but it's difficult for one person to cover all aspects of cybersecurity." This theme reflects the challenges smaller SMEs face in achieving comprehensive cybersecurity coverage, suggesting that such businesses may be especially vulnerable to cyber threats.

Compliance and Future Strategies: Emerging themes included the intention to adopt more advanced cybersecurity measures, such as multi-factor authentication and encryption, to align with regulatory standards like GDPR. Some participants mentioned that compliance is a driver for future cybersecurity strategies, although specific regulatory challenges were not explored in depth.

3.4 Summary of Findings

These findings reveal that SME approaches to cybersecurity are heavily influenced by company size, industry sector, financial resources, and regulatory pressures. While larger companies and industries handling sensitive data demonstrate higher employee confidence in cybersecurity measures, smaller SMEs and sectors with less data sensitivity face additional challenges in maintaining comprehensive security practices. These insights highlight the need for targeted support to enhance cybersecurity resilience across SMEs, particularly in smaller and resource-constrained enterprises.

4 Conclusion

Based on the findings, SMEs demonstrate a complex perception of cybersecurity measures for protecting customer data, with substantial variation influenced by company size, industry sector, and resource availability.

First, there is a general acknowledgment across SMEs of the importance of cybersecurity for safeguarding customer data, though perceptions of specific measures vary significantly. Larger SMEs and industries such as finance and IT, which handle highly sensitive customer data, report higher levels of confidence in their cybersecurity practices. Employees in these sectors tend to believe that existing measures adequately protect customer information, likely due to more substantial investments in cybersecurity infrastructure and regulatory compliance efforts. This awareness translates into greater confidence in cybersecurity protections, suggesting a positive correlation between perceived data sensitivity, regulatory pressure, and proactive security measures.

In contrast, smaller SMEs, particularly in sectors like agriculture or public relations, perceive cybersecurity as important but report lower confidence levels in their current practices. These SMEs often face financial and operational constraints, limiting their ability to implement comprehensive security solutions. Limited resources typically necessitate outsourcing cybersecurity to third-party providers, which, while practical, may introduce concerns about data control and security oversight. These findings suggest that while there is a foundational awareness of cybersecurity's role in customer data protection, smaller SMEs may lack the resources and confidence to fully execute on these measures, increasing their vulnerability to data breaches.

Furthermore, the thematic analysis focuses on compliance-driven future strategies, particularly as SMEs anticipate regulatory changes. The drive to adopt measures such as multi-factor authentication and encryption indicates a willingness among SMEs to enhance customer data protection, though this is often hindered by budget limitations and the need for external support.

In conclusion, SMEs generally perceive cybersecurity as essential to protecting customer data but face divergent challenges in implementing effective

measures. Larger SMEs and data-sensitive sectors feel more equipped to handle cybersecurity demands, whereas smaller SMEs, constrained by resources, exhibit both reliance on external providers and lower confidence in their ability to protect customer information. For SMEs to strengthen cybersecurity measures and protect customer data effectively, targeted, affordable solutions and industry-specific guidance are crucial to overcoming these limitations, especially for smaller and resource-constrained businesses.

5 Recommendations

Sector-Specific Cybersecurity Guidelines: Given the varied levels of vulnerability across industries, policymakers should develop cybersecurity guidelines tailored to the unique risks and needs of each sector. Industries like finance, healthcare, and IT, which handle sensitive data, should receive specific guidance on compliance and advanced security practices, while sectors such as agriculture and public relations could benefit from foundational security strategies suited to their lower-risk profiles.

Incentivized Cybersecurity Investments for SMEs: Financial incentives, such as tax credits or grants, can help SMEs afford essential cybersecurity tools and practices. Governments could establish programs that subsidize cybersecurity training, software, and infrastructure for SMEs, helping them improve their resilience without straining limited budgets.

Public-Private Cybersecurity Partnerships: Facilitating partnerships between SMEs and larger corporations with established cybersecurity frameworks can offer SMEs access to shared resources and expertise. Such collaborations could provide SMEs with affordable access to cybersecurity technologies, mentoring, and up-to-date threat intelligence.

Mandatory Cybersecurity Training and Awareness Programs: Introducing mandatory cybersecurity training for SME employees can address knowledge gaps across company sizes. These programs should focus on practical skills like threat recognition, data protection basics, and safe internet practices to help employees across all sectors contribute to a secure environment.

Compliance Assistance and Simplified Standards: To ease regulatory burdens on SMEs, policymakers should simplify compliance processes and provide support for meeting essential standards, such as GDPR. Assistance programs could offer easy-to-follow guidelines, templates, and audits, especially beneficial for SMEs without dedicated cybersecurity personnel.

References

Algan, Neşe (2019). "The importance of SMEs on world economies". In: *Proceedings of International Conference on Eurasian Economies, Turkish Republic of Northern Cyprus*. Vol. 12.

Jahankhani, Hamid, David V Kilpin, and Stefan Kendzierskyj (2022). *Blockchain and other emerging technologies for digital business strategies*. Springer.

A Appendix A: Stakeholder Analysis for Digiwerkplaats Project

In the context of the digital transformation project led by Digiwerkplaats, it is essential to identify and analyze key stakeholders to ensure effective decision-making and collaboration. Stakeholders in this project include Digiwerkplaats, SMEs, customers, and the Municipality of Breda, each playing a unique role in shaping the project's success. Understanding the power, interest, and priority of each stakeholder allows for strategic engagement and allocation of resources to maximize the project's impact.

The following stakeholder matrix highlights the influence and interest levels of these stakeholders, providing a basis for understanding their role in the project and the priority they should be given.

Stakeholder Descriptions

Digiwerkplaats: Digiwerkplaats is a vital platform designed to facilitate the digital transformation of small and medium-sized enterprises (SMEs). It offers access to digital tools, expertise, and personalized guidance to help businesses enhance their online presence, digital marketing strategies, and operational efficiency. Supported by government initiatives and educational institutions, Digiwerkplaats plays a key role in building digital capacity among SMEs.

- **Power:** Medium
- **Interest:** High
- **Priority:** High
- **Justification:** Digiwerkplaats has significant influence in the project as it directly controls the resources and services provided to SMEs. Their high interest stems from the platform's mission to drive digital growth among businesses, making their engagement crucial for success.

SMEs: SMEs represent a diverse range of businesses that vary in size, industry, and market presence. They typically operate with limited resources but are focused on growth and digital innovation to stay competitive. SMEs depend on Digiwerkplaats for cost-effective digital solutions to improve their operations.

- **Power:** Low
- **Interest:** High
- **Priority:** High
- **Justification:** While SMEs have little control over the project's direction, they are the primary beneficiaries of Digiwerkplaats's services. Their success in adopting new technologies is a key objective of the project, making them highly invested in the outcomes.

Municipality of Breda: The municipality plays a regulatory and supportive role in the project. They help facilitate SME development by providing resources, guidance, and support.

B Appendix B: Survey Questions

The following survey questions were used in the study:

- **Q1:** How would you rate your overall knowledge of cybersecurity practices?
- **Q2:** How important is cybersecurity for your role?
- **Q3:** Does your industry have specific cybersecurity regulations your business must follow?
- **Q4:** How often do you follow cybersecurity guidelines (e.g., password updates, cautious browsing) in your daily work?
- **Q5:** Do you believe that your awareness of cybersecurity threats has improved over the years?
- **Q6:** Which of these cybersecurity measures does your company use? (Select all that apply)
- **Q7:** How likely are you to report a security issue (e.g., a suspicious email) to your IT department or security team?
- **Q8:** How often are you informed about cybersecurity measures and potential threats at your workplace or school?
- **Q9:** How often does your company review or update cybersecurity policies?
- **Q10:** How concerned are you about cyber threats like phishing or data breaches?
- **Q11:** How confident are you in your company's ability to protect customer data with its current cybersecurity measures?
- **Q12:** How confident do you feel that your company's current cybersecurity measures are enough to prevent cyberattacks?
- **Q13:** How adequately are you able to recognize and respond to cybersecurity threats?
- **Q14:** How often do you update or maintain the cybersecurity tools you use?
- **Q15:** Please rank the following factors based on their importance for effective cybersecurity within your company (1 = Most important, 5 = Least important):
  - User-friendly interfaces for cybersecurity tools
  - Regular updates to cybersecurity tools
  - Quick access to support for cybersecurity tools
  - Employee training on how to use cybersecurity tools
  - Integration of cybersecurity tools with other systems

- **Q16:** How often are you required to run antivirus or security scans on your devices?
- **Q17:** What is the most important factor you consider when choosing a cybersecurity tool?
- **Q18:** Do you think AI should be used for identifying and/or mitigating cybersecurity threats?
- **Q19:** How confident are you in AI technology's ability to identify and/or mitigate cybersecurity threats?
- **Q20:** Are you concerned that bias may affect AI cybersecurity tools' ability to identify and mitigate threats?
- **Q21:** Are you concerned that bias may cause AI cybersecurity tools to incorrectly identify threats?
- **Q22:** Which outcome is worse for an AI cybersecurity tool?
- **Q23:** How often do you review your organization's cybersecurity policies?
- **Q24:** Do you know where to find the cybersecurity policies in your organization?
- **Q25:** How familiar are you with the consequences of not adhering to the organization's cybersecurity policies?
- **Q26:** Do you feel that the current cybersecurity policies in your organization are effective?
- **Q27:** You discover that a colleague is regularly bypassing the organization's cybersecurity policies by sharing sensitive data via unapproved methods. Please rank the following steps in the order you believe they should be taken (1 being the first and 5 being the last):
  - Confront the colleague directly about the violation
  - Report the violation to your manager or HR
  - Review the organization's policy on reporting violations
  - Gather evidence of the policy breach before taking any action
  - Consult with the IT department for advice on how to handle the situation
- **Q28:** Does your company have an IT specialist or IT department?
- **Q29:** Do you believe that having an IT specialist always available increases your awareness of cybersecurity risks?
- **Q30:** Do you rely on the IT specialist to solve most of your cybersecurity problems?
- **Q31:** Have you noticed any improvement in your cybersecurity knowledge due to the IT specialist's support?

- **Q32:** Does your company provide cybersecurity training to employees?
- **Q33:** Are you willing to follow cybersecurity training if your company provides it?
- **Q34:** How frequently are you provided with cybersecurity training or resources (e.g., online courses, workshops, manuals)?
- **Q35:** How relevant do you find the content of cybersecurity training to your daily tasks?
- **Q36:** How much do you feel your understanding of cybersecurity improves after each training session?
- **Q37:** After training, how often do you implement the cybersecurity practices you learned?
- **Q38:** In your opinion, would more frequent cybersecurity training improve your ability to protect yourself or your organization from cyber threats?
- **Q39:** How familiar are you with phishing attacks (e.g., deceptive emails designed to steal personal information)?
- **Q40:** How frequently do you update your passwords?
- **Q41:** Do you ever use public WiFi networks? For example: free company WiFi, free WiFi in a coffee shop, or restaurant.
- **Q42:** How often do you lock your computer screen when stepping away from your workstation?
- **Q43:** How often do you have sensitive information on your local device (work phone or laptop)?
- **Q44:** Do you use the same passwords for multiple systems?
- **Q45:** Do you ever get pop-ups like "ransomware detected" or "Attention: Illegal activity was revealed!"?
- **Q46:** Do you ever download software or files not related to work on work devices?
- **Q47:** When you receive a message or email from an unknown person or company with a link, what are you most likely to do?
- **Q48:** Does your company have a documented Cyber Incident Response Plan (CIRP) that you are aware of?
- **Q49:** Is there a dedicated department or employee to handle cyber threats?
- **Q50:** Does your company perform regular simulations or drills to test the incident response plan?
- **Q51:** Is there a protocol in place to notify key stakeholders (e.g., management, customers, regulators) during a cybersecurity incident?

- **Q52:** Do you have protocols for securely sharing sensitive information during a cybersecurity incident?
- **Q53:** How old are you?
- **Q54:** What is your nationality?
- **Q55:** How do you describe yourself? (Select choice)
- **Q56:** What sector do you work in?
- **Q57:** How many employees does your company have?
- **Q58:** What department do you work in?
- **Q59:** How many years of experience do you have working for a Small Medium Enterprise?
- **Q60:** How long has your current company been operating?