Online Journal of Applied Knowledge Management

A Publication of the International Institute for Applied Knowledge Management

Volume 10, Issue 2, 2022

Assessing SMEs' cybersecurity organizational readiness: Findings from an Italian survey

Martina Neri, University of Pisa, Italy, martina.neri@phd.unipi.it

Federico Niccolini, University of Pisa, Italy, federico.niccolini@unipi.it

Rosario Pugliese, University of Florence, Italy, rosario.pugliese@unifi.it

Abstract

The Small and Medium-sized Enterprises' (SMEs) level of organizational cybersecurity readiness has been poorly investigated to date. Currently, all SMEs need to maintain an adequate level of cybersecurity to run their businesses, not only those wishing to fully exploit digitalization's benefits. Unfortunately, due to their lack of resources, skills, and their low level of cyber awareness, SMEs often seem unprepared. It is essential that they address the digital threats that they face by using technology and complementary (and not alternative) factors, such as guidelines, formal policies, and training. All these elements trigger development processes regarding skills, awareness, the organizational cybersecurity culture, and the organizational resilience. This paper describes Italy's first multidisciplinary attempt to assess its SMEs' overall cybersecurity readiness level. We used a survey as its initial quantitative assessment approach, although SMEs can also use it as a cyber self-assessment tool, which prepares them better to navigate the digital ecosystem. Thereafter, we held semi-structured interviews to explore the critical points that had emerged from the study's first phase. The overall results show that SMEs have not yet achieved high levels of organizational readiness. SMEs are currently starting to set the stage for their organizational cyber readiness and will, therefore, have to take many more proactive steps to address their cyber challenges.

Keywords: Cybersecurity; Small and Medium Enterprises (SMEs); Cybersecurity organizational readiness, Italian organizational cybersecurity.

Introduction

In the growing interconnected environment in which organizations operate, cybersecurity's significance develops proportionally with Information and Communication Technology (ICT)'s importance. Contemporary societies and their organizational systems are increasingly exposed to unexpected disruptive events (Pettit et al., 2013). For at least two decades, organizations have not been able to manage their administrative processes and Information Systems (IS) without paying sufficient attention to the information security issues associated with such ISs (Gupta & Hammond, 2005). This became even more evident when the COVID-19 pandemic drove the digital acceleration. Cybersecurity refers to protecting computer networks to safeguard their IS resources' (e.g., hardware, software, firmware, information or data, and telecommunications') Confidentiality, Integrity, and Availability (aka the "CIA triad") (Onwubiko & Lenaghan, 2007). Whether it is a confirmed data breach compromising the data confidentiality, or an integrity incident, such as altering a person's behavior via phishing, all actions against assets compromise the CIA triad. According to Annarelli and Nonino (2016), "The environment surrounding organizations increasingly challenges them by posing different threats in various forms from both inside and outside an enterprise's boundaries" (p. 2). Cyber-attacks are just one such threat. Since cyber-attacks are becoming increasingly sophisticated, targeted, and coordinated (Farwell & Rohozinski, 2011), cybersecurity is a growing and evolving phenomenon. Moreover, global cybercrime costs are expected to increase by 15% per year over the next five years, reaching $10.5 trillion annually by 2025 (Morgan, 2020).

Given the fundamental role Small and Medium Enterprises (SMEs) play in most countries' economies, including Italy, focusing on them is truly important. The use of IS assumes they play a relevant role in SMEs. Indeed, ISs are an essential tool for improving SMEs' competitive advantage (Tarutė and Gatautis, 2014), for making knowledge available beyond geographical boundaries, for enhancing information acquisition's effectiveness (Walczuch et al., 2000), and for increasing the flow of information (Khatibi et al., 2003). Most SMEs are part of larger organizations' supply chain, and a successful cyber-attack on one of them could significantly disrupt a whole industry (Rezaei et al., 2015). News and scholarly research outlets have thoroughly documented that data breaches and cyber-attacks impact large and small organizations (Gafni & Pavel, 2019). While larger organizations have teams of IS professionals to mitigate the risks and to ensure that they can counter a data breach, SMEs lack such structures, awareness, and, therefore, cybersecurity readiness (D'Arcy et al., 2009). Organizations usually recognize that cybersecurity is a challenge that they need to manage, but they often still do not know how to deal with it (Sangani & Vijayakumar, 2012). SMEs seem to have a weak understanding of IS, security technologies, and control measures; they seem to ignore risk assessments and the development of security policies (Kuusisto & Ilvonen, 2003). Most SMEs depend on IS for their business activities without knowing how to safeguard their information or data from cyber-attacks (Gafni & Pavel, 2019; Park et al., 2008). Furthermore, smaller organizations have for many years not truly valued their information and its security (Smith & Rupp, 2002). The crux of their IS has always been the budget costs of their design, development, and implementation (Tawileh et al., 2007). SMEs usually lack technical expertise, funds, specialized knowledge, and security architectures to protect their systems against cyber-attacks (Paulsen, 2016; Vijayakumar, 2009). The latter is due to SME owners, managers, and decision-makers often being more worried about everyday business and neglecting cybersecurity issues, making them more vulnerable to cybercrime (Bhattacharya, 2013). Currently, cybersecurity is, therefore, the most pervasive challenge that SMEs face. According to Bell (2017), cybersecurity requires a budget, specialist knowledge, and competencies to be operational. Given this perspective, SMEs commonly face the same problems that larger organizations face. However, as mentioned before, it is noteworthy that there are significant differences—depending on the size of the organization under attack—in their approach to cyber threats (Gupta & Hammond, 2005). Currently, little is known about SMEs' cyber context; this requires more research since they cannot be regarded as scaled-down versions of large organizations. According to Tisdale (2015), a multi-dimensional approach needs to expand the technical outlook favoring a systems-complexity orientation and a knowledge management foundation. A new approach is mainly necessary due to the use of IS becoming more widespread, and organizations relying on IS as it would be impossible to manage their business without technology solutions (Gupta & Hammond, 2005; Paananen et al., 2020).

As a first approach, SMEs need to develop cybersecurity awareness. Awareness refers to continuous and regular attention to safeguarding the organization (Safa et al., 2015). Cybersecurity awareness, better known as the Security Education, Training, and Awareness (SETA) program, is the first step toward protection against cyber threats (Angst et al., 2017). SETA has traditionally been viewed as an initial condition for organizational users to develop a deep consciousness of the corporate cybersecurity mission (Sabillon, 2021; Siponen, 2000). Furthermore, Martins and Elofe (2002) stated that SETA is the assumption of acceptable behavior related to the cybersecurity CIA-triad concepts. Awareness and knowledge are directly related to organizational culture (Schein, 1990) and, therefore, to cybersecurity culture (Schlienger & Teufel, 2002). SETA is thus, embedded in the organizational culture (Schein, 1990).

Developing an organizational cybersecurity culture involves knowledge sharing and learning mechanisms (Thompson et al., 2016). Moreover, such a culture relies on continuous training, communication, analysis, and evaluation to increase all employees' awareness, to improve their skills, fill their knowledge gaps, and ensure they are responsible and accountable (Macmillan, 2017). Many publications have pointed out that employees' behaviors are the root cause of organizational exploitation when cyberattacks occur (Leukfeldt, 2014). Furthermore, the end-user is often a critical backdoor into the corporate network, even if a high level of security is in place (Ani et al., 2019; Bulgurcu et al., 2009; Talib et al., 2010). Organizations need to face cyber-attacks and cybersecurity issues with a proactive approach. This approach will benefit organizations significantly; indeed, organizations learn from and adapt to adverse events. Nevertheless, organizations should no longer just focus on technologies but need a new learning approach to adverse events. Their goal should be to become resilient against cyber-attacks. Organizational Resilience (OR)—also in a cyber-learning environment—should be understood as an organization's ability to continue after an attack and to reorganize or recover while essentially maintaining their previous functions (Ates & Bititci, 2011). According to McDonald (2017), OR represents an organization's capacity to anticipate and manage risk effectively by appropriately adapting its employees' actions, systems, and processes to ensure that the organization's core functions are carried out using a stable and effective relationship with the environment. OR not only refers to the technological aspects that an adverse event affects but requires total involvement of the organizational actors, processes, and infrastructures. According to Horne and Orr (1998), "Resilience is a fundamental quality of individuals, groups, organizations, and systems as a whole to respond productively to significant change that disrupts the expected pattern of events without engaging in an extended period of regressive behavior" (p. 31). Even if the organization is vulnerable, it can nevertheless become more robust and resourceful after an attack (Vogus & Sutcliffe, 2007) by means of learning and change logic (Duchek, 2020). If organizations are oriented toward learning through adverse events, this will result in significant benefits when the organization moves from a defensive attitude to a proactive one. When a potentially harmful event occurs, organizations should take the opportunity to identify their flaws and to approach their environment more proactively (Somers, 2009). This will result in a greater ability to learn from and adapt to an adverse event. Given SMEs' importance and peculiarities in the cybersecurity domain, focusing on them is more than ever required.

By referring to technological and organizational issues, this study is the first multidisciplinary attempt in Italy to conduct an overall quantitative and qualitative assessment of SMEs' cyber organizational readiness to face cyber issues and navigate the cyber domain. The latter is crucial for a better understanding of the cybersecurity mechanisms that SMEs have in place and of related issues. The SMEs included in the study are situated in a specific central Italian region. The Italian industrial system is based on a constellation of very small organizations, often family-owned, specialized in manufacturing goods typically labeled "Made in Italy," such as fashion, furnishings, food, and mechanics. Indeed, 99.9% of all Italian organizations are considered SMEs and are responsible for 58% of the country's Gross Domestic Product (GDP) (EUROSTAT, 2019). It is, therefore, no wonder that cyber-attacks mainly target these organizations (Zappa, 2014). This paper is organized as follows: we first describe the methodology of the survey validation and the SMEs' organizational readiness assessment. After that, we present the results and highlight a few managerial implications of these.

Methodology

We conducted the assessment both quantitatively and qualitatively to obtain more detailed and meaningful information about SMEs' organizational cybersecurity readiness. The quantitative assessment consists of a survey structured into four sections. Each section investigates fundamental features with which to assess and improve organizational readiness within the cyber domain. Section A contains closed-ended questions primarily related to cybersecurity in the technical sense (e.g., critical data management), which we needed to understand whether organizations are aware of the importance and value of the information they hold and whether they have adequate data management processes in place. Furthermore, we investigated their cybersecurity training. Section B contains multiple-choice questions, mainly about management; these questions focus on managerial aspects, such as the best practices to avoid unauthorized access to hardware and software. Section C contains follow-up questions designed to investigate whether the organization has experienced cyber-attacks and whether there was an increase in these during the COVID-19 pandemic. These questions allowed us to place the survey within organizations' current and future scenarios. Section D contains questions about entrepreneurial organizational features, such as the number of employees, the annual turnover, the organization type, and the role that IT or cybersecurity plays. We assigned each question a code representing its section and number in terms of the survey's structure.

Having completed the above (from July to September 2020), we used the Delphi method within the expert panel to evaluate the survey overall (Fink et al., 1984). The Expert Panel is based on a multidisciplinary perspective that provides the most accurate and detailed overview of the issue under analysis; this evaluation methodology also allows researchers to "reduce groupthink influence while taking decisions" (Yousuf, 2007, p. 4). The Delphi method's main characteristics are its anonymity, interaction, supervised feedback, and statistical aggregation (Dalkey, 1967). These features significantly reduce the shortcomings of traditional tools used to pool group opinions (e.g., the influence that dominant individuals exert and the pressure to achieve consensus) (Dalkey & Rourke, 1972). The Delphi method is defined as "A methodology for structuring a group communication so that the process effectively allows individuals, as a whole, to address a complex problem" (Linstone & Turoff, 1975, p. 3). Furthermore, "This technique is useful when expert opinions are needed but time, distance, and other factors make it difficult or even impossible for the Panel to work together in the same physical location" (Yousuf, 2007, p.1). The global pandemic that COVID-19 caused, and the related social distancing rules meant that these features were crucial to achieving the research's goal. The Delphi method within the expert panel is also based on a multidisciplinary perspective to ensure an accurate and detailed overview of the research problem. Moreover, the Delphi method's main objective is for the opinions of the experts involved in the process (Gabel & Shipan, 2004) to converge; in fact, structured communication guides the experts toward a qualified interpretation of a specific issue so that the conclusions can be as shared as widely as possible (Dalkey & Helmer, 1963). Participants are selected for the survey's validation through expertise criteria, which allows for diversified, but complementary expertise. This latter is appropriate, especially if the research object is new and characterized by uncertainty (Skinner et al., 2015).

The Delphi method was, therefore, divided into the following six main phases (adapted from Pfeiffer, 1968):

1) *Preliminary phase*: The research purpose is defined and circumscribed in line with its characteristics and peculiarities.
2) *Expert Panel Selection*: The expert's selection is in line with the expertise criterion. Experts have high-quality knowledge and diverse skills. Panel selection is an essential process step, as "it is directly related to the quality of the results generated by the Panel" (Hsu & Stanford, 2007, p. 3). In our research, the expert panel comprised 20 cybersecurity and IT experts with direct experience in cybersecurity. In line with the research objective, we also included top managers and entrepreneurs to ensure that their kind of expertise was better represented. This expert panel's composition ensured a competency and heterogeneity level sufficient for evaluating the tool and satisfied scientific rigor's requirements.
3) *Exploratory phase*: We develop the first version of the survey by consulting the main literature on the topic, which included scientific articles, and national and European cybersecurity frameworks, such as the Italian Framework for Cybersecurity and Data Protection, International Organization for Standardization (ISO) 27001, the National Institute of Standards and Technology (NIST), and Control Objectives for Information and Related Technologies (COBIT) standards, as well as studies that Italian institutes, such as the National Institute of Statistics (ISTAT), published. As outlined above, the first survey version was organized into four main sections: A) closed-ended questions, which are primarily technical; B) multiple-choice questions, which are primarily organizational; C) in-depth questions, which are designed to investigate whether the organization has experienced cyber-attacks and whether there has been an increase in cyber-attacks due to the Covid-19 pandemic; D) technical-organizational questions, which are primarily designed to capture information about the organization type.
4) *Qualitative assessment*: Upon completion, we sent the survey's first version to the Experts Panel. This phase, called a qualitative adjustment, corresponds to the Delphi method's first round. The experts were asked to choose one of the following three possible actions in respect of each question in each section:
    a. Keep, if the question could be included unmodified in the survey.
    b. Adjust, if the question could be included in the survey, but first had to be modified.
    c. Remove, if the question had to be deleted from the survey.

In addition, the experts could make additional comments and suggestions regarding each question in each section. They could also suggest more questions for each section.

5) *Analytical phase*: We used the survey's qualitative assessment results to develop a new version.
6) *Quantitative assessment*: The Delphi method requires repeated administration until the variation in opinions reaches a small enough range to reach a sufficient convergence of opinions (Skulmoski et al., 2007). Afterward, we proceeded with the method's next phase by sending it to the expert panel again for a quantitative assessment, which corresponds to the Delphi method's second round. The Expert Panel had to create a holistic indicator of cybersecurity's organizational readiness, called the CyberSecurity Readiness Index (CSRI). In line with a Likert scale, the experts assign a score to each question, ranging from one (not at all important) to seven (extremely important) (Likert, 1932). During the survey's quantitative assessment, we repeated the process in respect of the first two sections, which were the most representative of the organizational levers under investigation.

The average of the scores that each expert assigned to each question represents the overall CSRI score. Thereafter, the indicator was used as a weight to associate each responding SME with a score indicating its cybersecurity organizational readiness. The experts' suggestions that emerged most frequently from the validation process can be grouped into the following three categories:

1. Definition, suggesting that the potential difficulties with interpreting a specific term or with revising or expanding the definition should be clarified.
2. Insight, suggesting that the topic that a question discusses should be expanded, or additional answers added.
3. Revision, suggesting that a question's wording should be revised.

The proposed survey is oriented toward Italian SMEs. Nevertheless, it can also be validly used in other countries to determine whether the regulatory adaptations and the context in which data collection occurs were adequately considered. In keeping with these requirements, we provide an English version of the survey (see appendix A). The Italian version was then translated into English and reviewed by native English speakers, who are also cybersecurity or organizational experts. These experts proposed minor wording adjustments. After that, the instrument was translated into Italian to search for possible misleading questions. Once the Expert Panel had reached a consensus, we sent the survey's final Italian version to the participating SMEs' key informants. We created the survey by using a data collection approach, called Computer Assisted Web Interviewing (CAWI), based on an online compilation. A comparative examination of the most common CAWI software based on various evaluation criteria (e.g., articulation, efficiency, reliability, and security), helped us select the software with which to implement the survey. Our investigation led us to ultimately choose LimeSurvey. We configured the software to send each participant a pre-written and personalized email message, inviting the organization to complete the survey. In addition, the message included a token, which acted as a unique identifier of the organization within the survey. The token is, in fact, a security method that restricts access to the survey, therefore, preventing data contamination. After the survey was compiled, each respondent received a summary file. The summary provides comments on SMEs' cybersecurity organizational readiness. A speedometer shows the final score, which is the sum of all the scores assigned to the answers. Furthermore, the summary contains a recommendation for a global cybersecurity improvement plan. Where partial countermeasures are suggested, these are associated with specific subgroups of the survey questions. After the quantitative assessment, we asked each SME's key informant to participate in the study's second stage, namely the qualitative assessment, comprising semi-structured interviews. Before proceeding with the interviews, each participant was first asked to sign a consent form. The interviews were "conversations with a purpose" (Burman, 1994). The interviewer followed a protocol, but could vary the sequence of questions, go in deep, and ask more questions about a specific topic. The interviews lasted 60 minutes at most and were held on the Google Meet platform. We transcribed the data verbatim and manually, after which we sent the interview transcription to the organization's key informants to ensure the respondent validation and the criteria's credibility (Bell et al., 2018). A single interviewer administered the interviews, but two other researchers also participated to ensure that the interview interpretation was shared as accurate as possible. Furthermore, each researcher had to read and validate the interview transcription.

Sample description

This study focuses on a specific set of 728 SMEs within a central region of Italy. The survey was administered between December 2020 and February 2021. At the end of the survey administration phase, 165 of 728 SMEs had participated, giving a 22.6% response rate. After that, we invited each organization to participate in the qualitative assessment, with a total of 19 or 11.51% of the SMEs agreeing to do so. The sample classification is based on the following attributes: A) the sector; B) the organization size according to its yearly turnover and number of employees; C) the years of activity. We collected this information through the survey's section D. We describe the first two attributes below. To identify the first attribute (i.e., the sector), we used codes associated with a specific economic activity (i.e., ATECO codes) in Italy. Figure 1 shows the organizations' percentage distribution by sector.

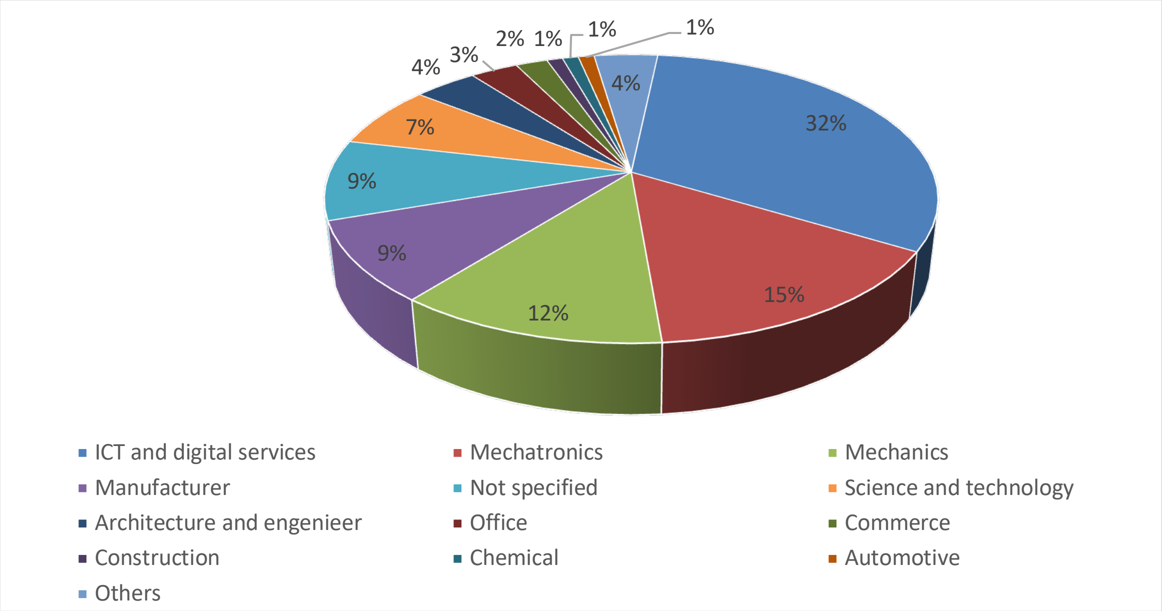

Figure 1. Organizations' Percentage Distributions by Sector (N=165)

The ICT and the digital services sector comprised the largest SMEs respondents' group (i.e., 53 of the 165 and more than 30% of all the responses). On analyzing the sample, we noticed that subdividing it into ICT organizations and non-ICT ones, which could be done during a future stage, would provide a helpful insight into the results and eliminate possible distortions. The response rates revealed that ICT and digital services were the most prevalent industry in the reference sample and had the greatest response rate (46.5%). We assumed that this result reflected the ICT and digital services sectors' sensitivity regarding cybersecurity issues, as they may have knowledge of or be more familiar with cybersecurity issues. Despite being the second-largest respondent sector, SMEs belonging to the mechatronics sector had a much lower response rate (i.e., 12.9%). According to the sample description, the study's sectoral representation is incomplete since it does not represent critical sectors, such as tourism and pharmaceutical. Consistently with the European Union classification, this study distinguishes between micro, small, and medium-sized enterprises based on their number of employees and their annual turnover (See Table 1).

Table 1. Organizations' distributions according to EU dimensional classification

Organization	**%**
Micro	33
Small	49
Medium	18

Results

We present our results below, dividing them into quantitative and qualitative assessments. The most relevant questions in both sections of the survey are highlighted.

Quantitative Assessment

As mentioned above, a survey was used as the instrument for the quantitative assessment. Table 2 highlights each section's results.

Table 2. Result highlights from Sections A, B, and C of the survey

Code	Questions	Yes	No
A05	Does the organization manage critical, business-relevant information (e.g., industrial drawings, product development plans, information related to internal processes and dynamics, including email or text messages, business plans, software/hardware prototypes, employee or personal user data)?	79.4%	20.6%
A07	Vulnerability refers to a system component in which security measures are lacking, reduced or compromised. A malicious user can therefore exploit the system's weakness to undertake unauthorized actions in the computer system. Have the vulnerabilities in the organization's tools and resources (e.g., its hardware, software, data, devices, insiders) been identified and are they regularly documented?	50.3%	49.7%
A08	Has a vulnerability plan been developed and implemented?	46.6%	53.4%
A09	Have the potential business impacts of a loss of confidentiality, integrity, or the availability of the company data, information, or services due to a cyber-attack been identified and analyzed?	42.4%	57.6%
A11	Threat refers to all counter-intuitive actions that can be carried out in and through cyberspace, therefore damaging the organization and its elements. Is there an ongoing process for monitoring and identifying internal and external threats?	57.5%	42.5%
A12	Risk refers to the probability that a threat will exploit vulnerabilities to allow an attack. Are the threats, vulnerabilities, and associated probabilities of occurrence, as well as the resulting impacts used to determine the risks?	42.5%	57.5%
A15	Does the organization implement and communicate a cybersecurity policy?	30%	70%

A17	Are the organization staff and relevant third parties aware of and trained in cybersecurity?	57%	43%
B02	Have all the cybersecurity-related rules and regulations applying to the organization been identified and implemented?	55%	45%
B02a	If yes, which ones?		
	Regulation UE 679/2016 (General Data Protection Regulation - GDPR)	95%	5%
	ISO/IEC 27001:2013 (the International Standard for Information Security)	19%	81%
	Documents that ENISA (European Union Agency for Cybersecurity) regularly published on cybersecurity and risk analysis	0.7%	99.3%
	Critical Security Controls for Effective Cyber Defense, a document that the Center for Information Security (CIS) issued	0.3%	99.7%
	COBIT (Control Objectives for Information and Related Technologies) framework applied in IT governance and management's best practices	0.2%	99.8%
	NIST (National Institute of Standards and Technology) framework	0.5%	99.5%
C01	Has your company been a target of cyber-attacks in the last year (either attempted or successful)?	14%	86%
C02	Has your organization increased its number of digital operations, processes, and transactions since the start of the global pandemic due to Covid-19?	77%	23%

Table 3. Most significant findings (from Section D of the survey)

Annual turnover	**% of organizations**
Fewer than 2 million euros	52
From 2 to 10 million euros	35
From 11 to 50 million euros	13
Number of employees	
Fewer than 5	13
From 5 to 9	22
From 10 to 29	39
From 30 to 49	10
From 50 to 249	16
Years of activity	
Fewer than 5	44
From 5 to 9	35
From 10 to 19	17
More than 20	4

Section A. The survey replies confirmed that most SMEs hold critical information. In the qualitative assessment, we extend our examination to understand what exact vital information SMEs manage. While organizations store critical information, they do not take all the appropriate measures to secure it. Indeed, many SMEs seem unprepared to face the risk perceptions, vulnerabilities, and potential impacts of such information. During the interviews, we addressed the budget issue explicitly. Our question about implementing a cybersecurity policy received the lowest number of positive responses. Although SMEs know what actions to take in the event of a cyber incident, most organizations lack a cybersecurity policy. Our qualitative assessment aimed to understand the reasons behind these results. We also found that formalized cybersecurity processes are rare, with existing cyber countermeasures primarily based on informal, unstructured activities related to the Chief Executive Officer's (CEO's), the manager's, and the Information Technology (IT) services manager's sensitivity to cybersecurity issues. Our observations included the training SMEs employees received on cybersecurity issues. We explored the various training types, their targets, and content in a qualitative assessment from which stimulating considerations emerged.

Section B. Almost all the organizations that responded positively to the question about whether they identify and comply with applicable cybersecurity laws, rules, and standards, stated that they followed the GDPR. Far fewer organizations follow the ISO/IEC 27001:2013 standard. Further, most enterprises rarely use frameworks and standards (e.g., COBIT and NIST), which could be described as more operational and non-mandatory —a significant indication.

Section C. Most businesses reported experiencing no attempted or suffered cyber-attacks in the last year. Nevertheless, it is unclear whether SMEs can detect a cyber-attack. Further, most organizations have increased their digital activities and processes.

Section D. According to the survey results, most organizations have a turnover of fewer than two million euros (i.e., 51.5%). Regarding the number of employees, most organizations have less than 30 employees. Another interesting detail that we identified analyzing was the number of years the organizations had been active. Most of the organizations had been in business for more than five years and had experienced the digital revolution directly.

Qualitative Assessment

This section presents the most important and meaningful findings from the semi-structured interviews. As described above, each participant was asked to sign a consent form and accept a transcription of their interview. The interviews' results are presented as quotes.

First, a key question referred to critical information. Most organizations stated that they manage and store this kind of information, and, during the interviews, we explored the specific type of critical information that they handle. An IT system manager clearly described what they regarded as critical information:

> *"We do not handle personal data with a high level of sensitivity. The few sensitive data we handle refer to the first and last names of customers, suppliers, and employees and their respective wages. On the other hand, we manage sensitive and strategic information about our products (e.g., projects, industrial drawings, etc.), which can be considered critical information. This is our know-how that needs to remain internal."*

This understanding also emerged from another IT system employee who reported:

> *"On the manufacturing side of the organization, we have the machine designs that we produce on behalf of a customer. In addition, the organization also has its industrial property, which is obviously critical."*

Employees' critical information is included in the list of critical information; in fact, according to an IT manager:

> *"The organization holds sensitive employee information. In addition, there is other critical information, such as the schematics of prototypes, technical specifications, and our software manuals."*

Our decision to analyze the critical information issue in depth and not just be satisfied with a simple definition proved valuable. Most organizations do not just hold data, such as names or salaries, but also crucial information on prototypes or industrial property. SMEs should therefore focus closely on such cybersecurity issues. The loss of such critical data would impact these organizations significantly in many ways (e.g., economically and in terms of reputation). We examined cybersecurity management in-depth, asking each SME's key informant whether this was done internally or by third parties. The answers were that, in terms of cybersecurity management, organizations rely on themselves or on their partnership with third parties. According to a CEO:

> *"Since we are all computer specialists (engineers, mathematicians, and computer scientists), we handle most technical issues in-house. We also use the knowledge of qualified external people, who help us configure a specific service and check whether we meet all the requirements."*

On the other hand, third parties also seem to be a valuable option, with a computer system representative mentioning:

> *"We rely on third parties for the basic setup and then continue our own. However, given the latest cybersecurity news and two past experiences with ransomware, I've asked the company owner to look at third-party support options so that we can be better protected."*

This could indicate a lack of appropriate and formalized cybersecurity solutions. However, the limited budget available for such services could prevent organizations from outsourcing cybersecurity to a third party. Some organizations want to systematize their operations better by turning to third parties when they become more aware of the cyber world's challenging requirements. Once again, awareness of cyber issues emerged as a critical element.

The budget allocated to cybersecurity services was another important point that had to be explored, as it was critical for understanding the value assigned to the above issues and how they are managed from an economic perspective. From the semi-structured interviews' findings, it is evident that there is no budget solely devoted to cybersecurity. More specifically, cybersecurity requirements are frequently incorporated into IT budgets or generated on an as-needed basis. It is worth noting that the budget is rarely determined annually. According to a CEO:

> *"Since Information technology is at the core of the company's operations, there is no separate budget for cybersecurity. There is, however, specific expenditure allocated for software and hardware management in the annual budget. Still, this is also part of the company's operation and, therefore, of the productive infrastructure."*

According to an IT specialist, unstructured budgets appear to be a trend:

> *"There are no funds designated for cybersecurity. They are, in general, ICT-related funds. Hardware is a high-priority area for investment. Extra budget required for a project must always be approved and reported to the management."*

Moreover, according to another IT manager:

> *"We don't have a fixed budget, but we prioritize necessities. 'Spend little and make everything work well,' the advice goes. As a result, we have a good trade-off."*

These observations implicitly show a low level of cybersecurity awareness, with cybersecurity not conceived as a core part of the organization. Furthermore, the results reveal that cybersecurity might be perceived as a cost rather than a strategic investment, with lump sum interventions based on immediate needs and not on systematic budgetary planning.

Training on cybersecurity issues was another fundamental aspect that we investigated by means of the interviews. This also relates to the quantitative assessment results, with the responses almost splitting the sample in half. Some SMEs rely on their own expertise. One CEO stated:

> *"Because the team is highly skilled in digital security and cybersecurity, the company does not provide specific cybersecurity training. Three of the administration's 50 employees are not IT professionals, although they have limited access to digital services."*

The interviews also clarified that training is still unstructured. An IT employee stated that:

> *"Employees get some training. Still, there is no formal training strategy in place. I mostly train on critical issues and dangerous (cyber) habits. The training is provided as and when needed and has a good level of effectiveness."*

Sometimes, the need for a training process and best practices is clear. However, it is still unstructured. According to an IT specialist, training is specifically oriented

> *"Toward our employees to inform them of the possible risks. We have best practices that we communicate with all our employees. We can also provide a few hours of training to support somebody with a special need, but there is no defined number of hours committed to this activity."*

Training analysis shows that unstructured processes are used instead of systematic strategies. Training activities are therefore managed internally as part of the overall cybersecurity issues. In this scenario, however, an essential awareness of the need for appropriate, although informal, training activities emerges clearly. Consequently, we maintain that training activities are not conceived as structured programs devoted to improving awareness of cyber risks. It is worth noting that in the quantitative assessment, we asked whether employees and stakeholders (e.g., clients and suppliers) were being trained or not. We ascertained that only employees are trained or informed about cybersecurity issues.

In the quantitative assessment, most SMEs stated that they do not implement a cybersecurity policy. According to the semi-structured interviews' results, there seems to be no specific issue that prevents them from implementing one. They simply believe that a cybersecurity policy is not essential and that their current practices are sufficient and in line with their requirements. The following statement from a CEO confirms that most SMEs are unaware that they might be a primary target for cybercriminals:

> *"There is no need (for a cybersecurity policy) given the kind of information we manage. We are, however, aware that we need some improvements. We are in an evaluation phase, but as a small company, we remain aware but flexible. These things could be done if we had our own IT division. When the company grows in that field, we will implement some improvements."*

Discussions, Conclusions, and Limitations

Our overall assessment suggests that Italian SMEs demonstrate certain strengths but also reveal some weaknesses. These SMEs appear to be aware of critical information's value. In addition, SMEs detected threats from both inside and outside the organization. Decision-makers are concerned with day-to-day activities; consequently, their long-term planning is limited. Their lack of a cybersecurity budget also confirms this. This lack of a dedicated cybersecurity budget prevents SMEs from taking the required proactive steps to prevent cyber-attacks, which could be due to a lack of awareness and a tendency to focus on corporate activities' more operational aspects. As previously observed, small businesses are less likely to consider themselves targets of cybercriminals. In terms of their weakness, while SMEs apply mandatory regulations (e.g., General Data Protection Regulation (GDPR)), their poor application of the regulations, standards, and frameworks related to the cybersecurity domain seems to be their most crucial vulnerability. This finding emphasizes legislation's critical role. The mandatory nature of regulations (e.g., GDPR) and the related penalties are essential for the widespread adoption of quality standards in the cybersecurity sector.

This highlights another potential weakness of the investigated business system: they do not apply more operational frameworks (e.g., NIST or COBIT), but favor mandatory regulations. These frameworks could be used as guidelines to address organizational vulnerabilities and to subsequently facilitate an effective formal cyber policy implementation. SME managers should therefore better understand the value that the proper implementation of such tools could provide. Furthermore, although SMEs do not have internal or external cybersecurity specialists to align them with the theoretical framework, they do recognize the value of relying on third parties to improve their protection against threats. Another critical vulnerability is the lack of systemic cybersecurity strategies and of structured processes oriented toward cybersecurity issues, while most lack a cybersecurity policy. This could be due to a policy being one of the most advanced managerial and strategic tools for managing cybersecurity risks effectively. Moreover, implementing a cybersecurity policy would require a significant allocation of time and money resources. Consequently, the number of SMEs that systematically carry out cyber risk management and cyber vulnerability identification is deficient. As mentioned before, budget allocation appears to be a critical issue for SMEs. Our qualitative assessment's results reveal that no budget is explicitly allocated to cybersecurity. Once again, cybersecurity is not part of these SMEs' systemic strategy but is managed to meet an organization's specific needs. This finding confirms that SMEs seem to neglect undertaking risk assessments or developing security policies. Training is another key issue that falls under the lack of structured processes. Training should not comprise a simple one-time training course, but employees should receive adequate cybersecurity training, especially before accessing critical assets. The inefficiency of one-off, informal courses is also related to cyber threats and technology's continuous evolution. The need for constant training should not be neglected. Employees should also be regularly updated on the evolving cybersecurity risks, with training being the principal vehicle to achieve an adequate awareness level. Training should be considered an investment in the human factor, which involves going beyond the outdated idea that cybersecurity is just another expenditure for the organization. This is especially relevant because cybercriminals exploit not only technological vulnerabilities but also human ones. The approach to cyber-attacks should therefore be integrative and collaborative, involving all the organizational units. The system vulnerabilities should consequently be safeguarded and best practices adopted to prevent damage.

Most organizations stated that they had not experienced any cyber-attack last year. In line with these results, it is reasonable to presume that their current defenses are adequate. On the other hand, SMEs may simply not be aware that they were victims of cyber-attacks. This issue is related to the nature of the self-reported answer to the question. The results could also imply a lack of monitoring systems and, in a broader sense, a low level of awareness. Since the COVID-19 pandemic, almost all SMEs have increased their digitized activity, which indicates how crucial cybersecurity is currently and will be in the future. This is particularly true about SMEs' critical information. Further, the results obtained from the survey's validation called attention to and supported the theoretical framework. The need to clarify specific definitions and to eliminate those processes found to be too complex highlights that a lack of awareness about cybersecurity also characterizes SMEs (Paulsen, 2016). On the other hand, the lack of suggestions regarding the questions about the organizational nature (Section B) highlights that solutions of a technological nature are no longer sufficient to address the complexity of cybersecurity. Organizational levers, namely culture, resilience, and awareness, are fundamental drivers to remove the organization's vulnerabilities, which are often due to the human factor.

Cybersecurity is a constantly evolving phenomenon that will inevitably affect all sectors and is especially relevant given the digital acceleration due to COVID-19 and, more recently, the war in Ukraine, which could make certain industries cyberattack targets. The lack of structured processes, IT professionals, and limited budgets are frequently observed concerns. This study reinforces awareness of the vulnerabilities generally associated with small businesses in terms of IS and cybersecurity management. Besides these vulnerabilities, certain strengths, such as threat detection, suggest that SMEs are aware that they operate in a high-risk digital ecosystem. Furthermore, certain weaknesses, such as a lack of compliance with a cybersecurity policy, emerged as elements that SMEs value highly. Even though they are aware of the need to adopt cybersecurity mechanisms, the outcome of our assessment shows that high levels of organizational readiness must still be achieved. SMEs are now starting to set the stage for cyber readiness, which will allow them to navigate the high-risk digital ecosystem. Many more proactive steps should therefore be taken to address cyber issues. Future research on SMEs is needed for a more comprehensive and specific analysis of the above issues and for the best practices to be disseminated wider. As in all other studies, ours also faces limitations. The sample structure and research design prevent this study from generalizing the data. Future research should expand the assessment of SMEs to other Italian regions, as well as European and non-European states. This would allow researchers to investigate whether specific national policies might affect the assessment outcomes. Moreover, sectors with very critical information (e.g., the pharmaceutical industry) should also be included for an overall viewpoint.

Acknowledgments

We want to thank Professor Meir Russ and all anonymous reviewers for the valuable suggestions and important points raised that allowed us to improve the paper. We are thankful to our colleagues Gianluca Dini, Luigi Martino, Giordano Ciappi, and Bernardo Manfriani, who provided expertise that greatly assisted the research. This research is partially supported by the project "Cybersecurity Toscano per le PMI ed i professionisti - Assessment cybersecurity readiness," and co-funded by the POR FESR Toscana 2014-2020 - Azione 1.1.4 sub b) (the co-funding share of the Tuscany Region: 71.15%, corresponding to EUR 100,000).

Reference

Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: Evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology, 21*(1), 2-35. https://doi.org/10.1108/jsit-02-2018-0028

Annarelli, A., & Nonino, F. (2016). Strategic and operational management of organizational resilience: Current state of research and future directions. *Omega*, *62*, 1–18. https://doi.org/10.1016/j.omega.2015.08.004

Ates, A., & Bititci, U. S. (2011). Change process: A key enabler for building resilient SMEs. *International Journal of Production Research, 49*(18), 5601-5618. https://doi.org/10.1080/00207543.2011.563825

Bell, E., Bryman, A., & Harley, B. (2018). *Business research methods* (5th ed.) Oxford University Press.

Bell, S. (2017). Cybersecurity is not just a 'big business'issue. *Governance Directions*, *69*(9), 536-539. https://www.governanceinstitute.com.au/resources/governance-directions/archive/issue-9/cybersecurity-is-not-just-a-big-business-issue/

Bhattacharya, D. (2013). Evolution of information security issues in small businesses. *The Colloquium for Information System Security Education, 1*(1), 1-10. https://cisse.info/journal/index.php/cisse/article/view/5

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2009). Roles of information security awareness and perceived fairness in information security policy compliance. *Proceedings of the 15th Americas Conference on Information Systems*. California, USA. https://aisel.aisnet.org/amcis2009/419

Burman, E. (1994). Interviewing. In P. Banister, E. Burman, I. Parker, M. Taylor, & C. Tindall (Eds.), *Qualitative methods in psychology: A research guide* (pp. 49–71). Open University Press.

D'Arcy, J., Hovav, A., & Galetta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 1-20. https://doi.org/10.1287/isre.1070.0160

Dalkey, N. C. (1967). *Delphi*. The Rand Corporation.

Dalkey, N. C., & Helmer, O., (1963). An experimental application of the Delphi method to the use of experts. *Management Science*, *9*(3), 351-515. https://doi.org/10.1287/mnsc.9.3.458

Dalkey, N. C., & Rourke, D. L. (1972). Experimental assessment of Delphi procedures with group value judgments. In N. C. Dalkey, D. L. Rourke, R. & Lewis, D. Snyder (Eds.), *Studies in the quality of life: Delphi and decision-making* (pp. 55-83). Lexington Books.

Duchek, S. (2020). Organizational resilience: A capability-based conceptualization. *Business Research*, *13*(1), 215–246. https://doi.org/10.1007/s40685-019-0085-7

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, *53*(1), 23-40. https://doi.org/10.1080/00396338.2011.555586

Fink, A., Kosecoff, J., Chassin, M., & Brook, R. H. (1984). Consensus methods: Characteristics and guidelines for use. *American Journal of Public Health*, *74*(9), 979-983. https://doi.org/10.2105/ajph.74.9.979

Gabel, M. J., & Shipan, C.R., (2004). A social choice approach to expert consensus panels. *Journal of Health Economics, 23*(3), 543–564. https://doi.org/10.1016/j.jhealeco.2003.10.004

Gafni, R., & Pavel, T. (2019). The invisible hole of information on SMB's cybersecurity. *Online Journal of Applied Knowledge Management, 7*(1), 14-26. https://doi.org/10.36965/OJAKM.2019.7(1)14-26

Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for small businesses: An empirical examination. *Information Management & Computer Security*, *13*(4), 297-310. https://doi.org/10.1108/09685220510614425

Horne III, J., & Orr, J. (1998). Assessing behaviors that create resilient organizations. *Employment Relations Today, 24*(4), 29-39. https://doi.org/10.1002/ert.3910240405

Hsu, C.-C., & Sandford, B. A. (2007). The Delphi technique: Making sense of consensus. *Practical Assessment, Research, and Evaluation, 12*(10), 1-8. https://doi.org/10.7275/pdz9-th90

Khatibi, A., Thyagarajan, V., & Seetharaman, A. (2003). E-commerce in Malaysia: Perceived benefits and barriers. *Vikalpa*, *28*(3), 77-82. https://doi.org/10.1177/0256090920030307

Kuusisto, T., & Ilvonen, I. (2003). Information security culture in small and medium size enterprises. *Proceedings of E-Business Research Forum.* E-Business Research Forum.

Leukfeldt, E. R. (2014). Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization. *Cyberpsychology, Behavior, and Social Networking*, *17*(8), 551-555. https://doi.org/10.1089/cyber.2014.0008

Likert, R. (1932). A technique for the measurement of attitudes. *Archives of Psychology*, *22*(140), 1-55. https://psycnet.apa.org/record/1933-01885-001

Linstone, H. A., & Turoff, M. (1975). Introduction to the Delphi method: Techniques and applications. In Linstone, H. A. and Turoff, M. (Eds), *The Delphi Method: Techniques and applications* (pp. 3-12). Addison-Wesley Publishing Company. https://web.njit.edu/~turoff/pubs/delphibook/delphibook.pdf

Macmillan, S., (2017, March). The best defense against cyber-attacks: People not technology. *Human Resources Magazine*, *21*(4), 8-10. https://hrnz.org.nz/fileadmin/Magazines/2017-1_Autumn_-_Human_Resources_magazine.pdf

Martins, A. & Eloff, J. (2002), Assessing information security culture. In Ghonaimy, M. A., El-Hadidi, M. T., & Aslan, H. K. (Eds.), *Security in the Information Society: Visions and perspectives* (pp.1-14), Springer.

McDonald, N., (2006). Organisational resilience and industrial risk. In E. Hollnagel, D. D. Woods & N. Leveson, (Eds.), *Resilience engineering: Concepts and precepts* (pp. 155-179). Ashgate.

Morgan, S. (2020, November 13). *Cybercrime to cost the world $10.5 trillion annually by 2025*. Cybercrime Magazine. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Onwubiko, C., & Lenaghan, A. P. (2007). Managing security threats and vulnerabilities for small to medium enterprises (pp. 244-249). *Proceedings of IEEE International Conference on Intelligence and Security Informatics.* IEEE.

Paananen, H., Lapke, M., & Siponen, M. (2020). State of the art in information security policy development. *Computer & Security*, *88*(2020), 101608. https://doi.org/10.1016/j.cose.2019.101608

Park, J. Y., Robles, R. J., Hong, C. H., Yeo, S. S., & Kim, T. H. (2008). IT security strategies for SMEs. *International Journal of Software Engineering and its Applications*, *2*(3), 91-98.

Paulsen, C. (2016). Cybersecuring small businesses. *Computer*, *49*(8), 92-97. https://doi.org/10.1109/MC.2016.223

Pettit, T. J., Croxton, K. L., & Fiksel, J. (2013). Ensuring supply chain resilience: Development and implementation of an assessment tool. *Journal of Business Logistics*, *34*(1), 46-76. https://doi.org/10.1111/jbl.12009

Pfeiffer, J. (1968). *New look at education.* Odyssey Press.

Rezaei, J., Ortt, R., & Trott, P. (2015). How SMEs can benefit from supply chain partnerships. *International Journal of Production Research*, *53*(5), 1527-1543. https://doi.org/10.1080/00207543.2014.952793

Sabillon, R. (2021). Delivering effective cybersecurity awareness training to support the organizational information security function. In information resource management association (Eds.), *Research Anthology on Privatizing and Securing Data* (pp. 629-650). IGI Global. https://doi.org/10.4018/978-1-7998-8954-0.ch029

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T., (2015). Information security conscious care behavior formation in organizations. *Computer & Security*, *53*(2015), 65-78. https://doi.org/10.1016/j.cose.2015.05.012

Sangani, N. K., & Vijayakumar, B. (2012). Cyber security scenarios and control for small and medium enterprises. *Informatica Economica*, *16*(2), 58-71. http://revistaie.ase.ro/content/62/07%20-%20Sangani.pdf

Schein, E. H. (1990). Organizational culture. *American Psychological Association*, *45*(2), 109-119. https://doi.org/10.1037/0003-066X.45.2.109

Schlienger, T., & Teufel, S. (2002). Information security culture. In Ghonaimy, M. A., El-Hadidi, M. T., & Aslan, H. K. (Eds.), *Security in the Information Society* (pp. 191-201). Springer. https://doi.org/10.1007/978-0-387-35586-3_15

Siponen, T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31-41. https://doi.org/10.1108/09685220010371394

Skinner, R., Nelson, R. R., Chin, W. W., & Land, L. (2015). The Delphi method research strategy in studies of information systems. *Communications of the Association for Information Systems*, *37*(2), 31-63. https://doi.org/10.17705/1CAIS.03702

Skulmoski, G. J., Hartman, F. T., & Krahn, J. (2007). The Delphi method for graduate research. *Journal of Information Technology Education*: *Research*, *6*(1), 1-21. https://doi.org/10.28945/199

Smith, A. D., & Rupp, W. T. (2002). Issues in cybersecurity; Understanding the potential risks associated with hackers/crackers. *Information Management & Computer Security*, *10*(4), 178-183. https://doi.org/10.1108/09685220210436976

Somers, S. (2009). Measuring resilience potential: An adaptive strategy for organizational crisis planning. *Journal of Contingencies & Crisis Management, 17*(1), 12–23. https://doi.org/10.1111/j.1468-5973.2009.00558.x

Talib, S., Clarke, N. L., & Furnell, S. M. (2010). An analysis of information security awareness within home and work environments (pp. 196-203). *Proceedings of the 2010 International Conference on Availability, Reliability and Security.* IEEE. https://ieeexplore.ieee.org/document/5438096

Tarutė, A., & Gatautis, R. (2014). ICT impact on SMEs performance. *Procedia-Social and Behavioral Sciences*, *110*(2014), 1218-1225. https://doi.org/10.1016/j.sbspro.2013.12.968

Tawileh, A., Hilton, J., & McIntosh, S. (2007). Managing information security in small and medium sized enterprises: a holistic approach (pp. 331-339). *Proceedings of the ISSE/SECURE 2007 Securing Electronic Business Processes*. IEEE. https://link.springer.com/chapter/10.1007/978-3-8348-9418-2_35

Vijayakumar, U. (2009). Top management control functions for information systems in small and medium enterprises. *Informatica Economica*, *13*(4), 109-115. http://revistaie.ase.ro/content/52/11-%20Vijayakumar.pdf

Vogus, T. J., & Sutcliffe, K. M. (2007). Organizational resilience: Towards a theory and research agenda. *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics*. IEEE. https://doi.org/10.1109/ICSMC.2007.4414160

Walczuch, R., Van Braven, G., & Lundgren, H. (2000). Internet adoption barriers for small firms in the Netherlands. *European Management Journal*, *18*(5), 561-572. https://doi.org/10.1016/S0263-2373(00)00045-1

Yousuf, M. I. (2007). Using experts' opinions through Delphi technique. *Practical Assessment, Research & Evaluation*, *12*(4), 1-8. https://doi.org/10.7275/rrph-t210

Zappa, F. (2014). *La criminalità informatica ei rischi per l'economia e le imprese a livello italiano ed europeo.* Torino, Italia: United Nations Interregional Crime and Justice Research Institute. https://unicri.it/sites/default/files/2019-11/Publication%20(Italian%20Version).pdf

Appendix A – Survey English version

Section A – Open-Ended Questions	
Code	**Questions**
A01	Are the organization's hardware systems and their information catalogued? The latter includes each system's information about the manager(s), the user(s), the physical location, etc.
A01a	Is the hardware inventory updated whenever a change occurs (e.g., adding/removing users, adding/removing a manager, a change in the physical location) or, at least, regularly?
A02	Are the organization's software systems and their information catalogued? This includes each system's information about the manager(s), the user(s), the physical location, etc.
A02a	Is the software inventory updated whenever a change occurs (e.g., adding/removing users, adding/removing managers, a change in the physical location) or, at least, regularly?
A03	Does the organization have procedures that regulate the web service usage (e.g., social networking, cloud services, emails, webspace offered by third parties) for business operations and management?
A04	Are personal data (related to individuals who interact with the organization, whether employees, customers, or third-party stakeholders) identified, catalogued, and recorded?
A05	Does the organization manage critical, business-relevant information (e.g., industrial drawings, product development plans, information related to internal processes and dynamics, including emails, text messages, business plans, software/hardware prototypes, employee or personal user data)?
A05a	Are critical and business-relevant information treated, identified, catalogued, recorded, and protected?
A06	Are regular backups made of the business-critical information and data?
A06a	Are the backups stored securely?
A06b	Are the backups regularly verified to ensure that it is performed correctly?
A06c	Backups are made on: - an external drive, - a network attached to the storage. - a data center. - the business's cloud. - a third-party cloud. - Other.
A07	Vulnerability refers to a system component with lacking, reduced or compromised security measures; a malicious user can exploit the system's weakness to perform unauthorized actions on the computer system. Are the vulnerabilities in the organization's tools and resources (e.g., the hardware, software, data, devices, and insiders) regularly identified and documented?
A08	Has a vulnerability plan been developed and implemented?
A09	Have the potential business impacts of a loss of confidentiality, integrity, or of the availability of the company data, information, or services due to a cyber-attack been identified and analyzed?
A10	A cyber-attack refers to individuals' or organizations' actions concerning destroying, damaging or hindering of systems' and networks' normal functioning, and violating data/information's integrity and confidentiality. Does the organization have a historical record of cyber-attacks?
A10a	Does the organization have a historical record of losses due to cyber-attacks?
A11	Threat refers to all counter-intuitive actions carried out in and through cyberspace to damage an organization and its elements. Is there an ongoing process to monitor and identify internal and external threats?
A12	Risk refers to the probability that a threat will exploit vulnerabilities to carry out an attack. Are the threats, vulnerabilities, probabilities of an occurrence, and the resulting impacts used to determine the risk?
A13	Does the organization refer to its previous cyber-attack experiences when implementing cyber threat management and response procedures?
A14	Does the organization have a recovery plan to execute during or after a cyber-attack?
A15	Does the organization implement and communicate its cybersecurity policy?
A16	Where applicable, do all of your organization's devices run security software (e.g., antivirus, anti-malware)?
A16a	Has all of your organization's security software been updated with the latest version?
A16b	Are the security systems linked to the information or services' importance in order to safeguard the business management standards?
A17	Are the staff and relevant third parties aware of and trained in cybersecurity?
A17a	Are the training activities mandatory?

A18	Is cyber-attack information obtained through formal information sources (e.g., national television channels, national newspapers, or the Italian government's cyber threat sources)?
A19	Is cyber-attack information obtained through informal information sources (e.g., social media, blogs, forums, or personal sources)?
A20	Is there a plan for adaption and distribution of the data if those information sources were to report new attacks?
A21	Has the organization developed and applied processes to identify, assess, and manage the risk associated with its operations within the supply chain?
Section B – Multiple Choice Questions	
Code	**Questions**
B01	Is access to resources (both hardware and software) allowed, given the risk of unauthorized access?
B01a	How? Choose one or more of the following options: - Digital identities and access credentials are provided and verified before interactions. - Physical access to resources is safeguarded and administered. - Remote access to resources is administered. - Identities are verified, linked to credentials, and checked during interactions. - Each user can only access the information and systems they need or are responsible for. - Unused accounts are disabled.
B02	Have all the cybersecurity-related rules and regulations that apply to the organization been identified and implemented?
B02a	If yes, which ones? Choose one or more of the following options: - Regulation UE 679/2016 (General Data Protection Regulation - GDPR). - ISO/IEC 27001:2013 (the International Standard for Information Security). - Documents regularly published by ENISA (European Union Agency for Cybersecurity) on cybersecurity and risk analysis. - Critical Security Controls for Effective Cyber Defense, a document issued by the Center for Information Security (CIS). - A COBIT (Control Objectives for Information and Related Technologies) framework applied in IT governance and management as a best practice. - NIST (National Institute of Standards and Technology) framework.
B03	Resilience refers to the ability to cope positively with an adverse event by rapidly reorganizing the resources at one's disposal and returning to the initial conditions with a minimal impact on the system. Have mechanisms been implemented to achieve the resilience required during regular operation and in adverse situations?
B03a	If yes, which ones? Choose one or more of the following options: - Systems are designed to ensure that, in the event of an attack, any interconnected systems or those or operating in proximity of them are not compromised. - System components are replaced or fixed without restarting the system itself. - The approach to cyber-attacks is integrative and collaborative, involving all of the organizational units. - Information concerning cyber-attacks is disseminated across the organization. - The organization is fully involved in exercises that replicate a potential cyber-attack. - Other.
B04	Are the roles and responsibilities regarding cybersecurity defined and disclosed to staff and relevant third parties (e.g., customers, suppliers, and partners)?
B04a	If yes, which ones? Choose one or more of the following options: - A cybersecurity specialist whose role is to identify potential risks and implement prevention strategies. - A systems vulnerability analyst whose role is to analyze the system to identify potential vulnerabilities. - A computer network administrator whose role is to monitor the computer network and update its software adequately, allowing each resource to have appropriate defenses in place. - An information security manager whose role is to improve the organization's security from a technical and management perspective. - The employees know what to do in the event of a cyber-attack. - Roles and responsibilities are coordinated and shared with external partners. - Customers are adequately informed of cybersecurity requirements (e.g., privacy, data processing, and data retention).

	• Other.
Section C – Follow-Up Questions	
Code	**Questions**
C01	Has your company been a target of cyber-attacks in the last year (attempted or suffered)?
C01a	How many?
C01b	What kind? Choose one or more of the following options: - Information, such as about users or computer systems, obtained due to human interaction (phishing). - Hackers blocking the system's use in order to obtain money (ransom) (ransomware). - Viruses, Trojan horses, and generic malicious software (malware). - The network or services being saturated, making them inaccessible or unreachable (DDoS). - Administrator credentials being extracted from the network (APT - Advanced Persistent Threat). - Database content being accessed and extracted (SQLi - Structured Query Language Injection). - Large amount of information obtained about the system, such as how it works or the data it contains (hacking). - Other.
C02	Has your organization grown the number of digital operations, processes, and transactions since the start of the global pandemic caused by Covid-19?
C02a	Has your organization experienced an increase in the number of cyber-attack attempts due to Covid-19?
C02a1	Which kinds?
C02b	Has your organization implemented any actions to improve its cybersecurity?
C02b1	Has your organization taken steps to improve its IT security regarding remote working?
C02b2	Which kind?
Section D – Entrepreneurial questions	
Code	**Questions**
D01	Annual turnover: • Less than EUR 2 million • From EUR 2 to EUR 10 million • From EUR 11 to EUR 50 million
D02	Number of employees: • Fewer than 5 employees • From 5 to 9 employees • From 10 to 29 employees • From 30 to 49 employees • From 50 to 249 employees
D03	Years of activity: • Fewer than 5 years • From 5 to 9 years • From 10 to 19 years • More than 20 years
D04	What is the juridical from of your organization?
D05	In which area does your organization invest the most? • Training • Resources • Hardware systems • Software development • Consultancy • Upgrades (e.g., systems, processes, and resources)

Authors Biographies

Martina Neri is a Ph.D. candidate at the Department of Business Administration and Management at the University of Pisa. She obtained her master's degree *cum laude* in Strategy, management, and control at the University of Pisa. Her main research interest focuses on organizational resilience, cybersecurity, organizational culture, and knowledge management.

Federico Niccolini is an Associate Professor of Organizational Science at the Department of Political Sciences, University of Pisa. He has been an Associate Faculty at Colorado State University since 2007. Niccolini's research interests focus on knowledge management, organizational vision and culture, dynamics related to sustainable development, protected areas, sustainable tourism, and the organizational profiles of cybersecurity. He teaches undergraduate, Master's, and Ph.D. courses. He coordinated several national and international (including EU-funded) projects and working groups. He has been a Visiting Scholar or professor at certain US universities (including Stanford). He participated in the International Visitor Leadership Program of the US Department of State's Bureau of Educational and Cultural Affairs.

Rosario Pugliese is a Full Professor of Computer Science at the Department of Statistics, Computer Science, Applications, University of Florence. He received the Laurea degree in Computer Science from the University of Pisa and the PhD degree in Computer Science from the Sapienza University of Rome. Pugliese's research interests focus on formal methods and analysis techniques; formalization, analysis, and implementation of access control policies; verification of security properties for communication protocols; methodologies and tools for modeling, verifying, programming, and deploying distributed systems in domains like Network-aware Programming, Service-Oriented Computing, Autonomic Computing, and Collaborative Robotics.