Received 15 May 2023
Revised 1 June 2023
Accepted 2 June 2023

Organizational cybersecurity readiness in the ICT sector: a quanti-qualitative assessment

Martina Neri
Department of Economics and Management, University of Pisa, Pisa, Italy
Federico Niccolini
Department of Political Sciences, University of Pisa, Pisa, Italy, and
Luigi Martino
Department of Social and Political Sciences, University of Bologna, Bologna, Italy

Abstract

Purpose – Cyberattacks are becoming increasingly widespread, and cybersecurity is therefore increasingly important. Although the technological aspects of cybersecurity are its best-known characteristics, the cybersecurity phenomenon goes beyond the detection of technological impacts, and encompasses all the dimensions of an organization. This study thus focusses on an additional set of organizational elements. The key elements of cybersecurity organizational readiness depicted here are cybersecurity awareness, cybersecurity culture and cybersecurity organizational resilience (OR). This study aims to qualitatively assess small and medium enterprises' (SMEs) overall level of organizational cybersecurity readiness.

Design/methodology/approach – This study focused on conducting a cybersecurity organizational readiness assessment using a sample of 53 Italian SMEs from the information and communication technology sector. Informed mixed method research, this study was conducted consistent with the principles of the explanatory sequential mixed method design, and adopting a quanti-qualitative methodology. The quantitative data were collected through a questionnaire. Qualitative data were subsequently collected through semi-structured interviews.

Findings – Although many elements of the technical aspects of cybersecurity OR have yielded very encouraging results, there are still some areas that require improvement. These include those facets that constitute the foundation of cybersecurity awareness, and, thus, a cybersecurity culture. This result highlights that the areas in need of improvement are exactly those that are most important in fighting against cyber threats via organizational cybersecurity readiness.

The authors are thankful to their colleagues Rosario Pugliese, Gianluca Dini, Bernardo Manfriani and Giordano Ciappi. Their knowledge and expertise have been valuable in improving this research. This research was 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 €100,000).

Information & Computer Security
Vol. 32 No. 1, 2024
pp. 38-52
Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-05-2023-0084

Originality/value – Although the importance of SMEs is obvious, evidence of such organizations' attitudes to cybersecurity are still limited. This research is an attempt to depict the organizational issue related to cybersecurity, i.e. overall cybersecurity organizational readiness.

Keywords Small and medium enterprises, Cybersecurity, Organizational cybersecurity readiness, Organizational resilience, Cybersecurity awareness, Cybersecurity culture

Paper type Research paper

1. Introduction

The most recent national and international cybersecurity reports continue to emphasize that cyberattacks are becoming more widespread. Nowadays, cyberattacks seek to exploit vulnerabilities that are related to the human ones. In addition, cybersecurity is one of the risks that has worsened the most because of the COVID-19 pandemic, according to the World Economic Forum's Global Risk Report (2022). The cost of cybercrime grows higher each year, with an expected cost of $10.5tn by 2025 (Morgan, 2020). In the same way, global cybersecurity product and services spending "is predicted to exceed $1 trillion cumulatively over the five-year period from 2017 to 2021" (Mclean, 2021, p. 1). The term "cybersecurity" usually refers to the confidentiality, integrity and availability (CIA) compromission (Onwubiko and Lenaghan, 2007). The definition of cybersecurity has been enriched with the idea of:

> The protection of cyberspace itself, the electronic information, the ICTs (Information and Communication Technology) that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace (Von Solms and Van Niekerk, 2013, p. 101).

Although these are the major concepts defining cybersecurity, we focus on an additional set of organizational elements. According to Corradini (2020), there is a strong need to improve the current approach to cybersecurity via critical thinking and a multidisciplinary concept of this phenomenon. Because cybersecurity goes beyond the detection of technological impacts and involves all the dimensions of an organization, a new approach now involves the management and organizational area (Tejay and Klein, 2021). We focus on conducting a cybersecurity organizational readiness assessment, in line with this broader view of the elements that must be discussed when assessing cybersecurity in organizations. Cybersecurity awareness, cybersecurity culture and cybersecurity organizational resilience (OR) are the key elements of cybersecurity organizational readiness that we focus on in this study.

Cybersecurity awareness refers to organizational safeguarding (Safa *et al.*, 2015) and is delivered to organizational employees mainly via Security Education, Training and Awareness (SETA) program (*Angst et al.*, 2017). SETA programs are closely related to behaviors perceived to be acceptable to be compliant with the CIA triad concept (Martins and Eloff, 2002). According to Nurse (2021), cybersecurity awareness is "the level of appreciation, understanding, or knowledge of cybersecurity or information security aspects. Such aspects include cognizance of cyber risks and threats, but also appropriate protection measures" (p. 1). While addressing cybersecurity awareness, it is necessary to:

> Consider both the extent to which an organization's employees understand the importance and implications of information security, and the extent to which they behave in accordance with the organization's information security policies and procedures. (Parsons *et al.*, 2017, p. 41)

Indeed:

> Cybersecurity awareness and training programs inform employees about the security requirements that need to be in place to preserve critical data, and about company guidelines,

> policies and procedures for better management of cybersecurity issues. (Corallo *et al.*, 2022, p. 2)

Training and cybersecurity policies are two critical components of this approach. People in an organization represent one of the weakest links in the cybersecurity sphere, and therefore they need proper training and sufficient resources (Chatterjee, 2019). Cybersecurity training "needs to target people's risk perception to motivate employees to take preventive and precautionary actions" (He *et al.*, 2019, p. 204). Indeed, according to Pattinson *et al.* (2019), focussing only on training activities as a source of cybersecurity awareness could be an inefficient strategy if it is not linked to individuals' matched learning styles. Regarding the cybersecurity policy issue, Li *et al.* (2019) investigated the impact of a cybersecurity policy on employees' behavior. Their results indicate that both implementation and awareness of cybersecurity policy have a positive impact on employee's beliefs about and behavior directed at cybersecurity. According to Kortjan and Von (2014), awareness and education are two main factors of cybersecurity culture. Indeed, Van Niekerk and Von Solms (2006) state that information security only exists when knowledge does. Because awareness and knowledge are embedded in cybersecurity culture (Schlienger and Teufel, 2002), the same applies to SETA programs. In line with this theoretical understanding, Da Veiga *et al.* (2020) defined cybersecurity culture as:

> Contextualized to the behavior of humans in an organizational context to protect information processed by the organization through compliance with the information security policy and an understanding of how to implement requirements in a cautious and attentive manner as embedded through regular communication, awareness, training and education initiatives. (p. 19)

The importance of SETA programs has been recognized as necessary for developing a cybersecurity culture (Parsons *et al.*, 2015). However, for a SETA program to become an effective tool for shaping cybersecurity culture, an extensive approach, which involves attitude, perceptions and new skills, is necessary (Alshaikh *et al.*, 2018). According to several frameworks for assessing an organization's cybersecurity culture, key elements of such a culture also include management support and leadership (e.g. having dedicated figures, such as the chief information security officer [CISO]) and learning to build and disseminate knowledge (Da Veiga *et al.*, 2020; Huang and Pearlson, 2019). In conducting a review of the concept of cybersecurity culture, Uchendu *et al.* (2021) identified top management support, leadership or involvement, security policy, security awareness and security training as the most cited factors among those that encompass a cybersecurity culture. Many of the elements mentioned so far are key features of the goal that all establishments should pursue, which is to be cyber resilient organization. The concept of OR, also in the context of cybersecurity, implies a proactive and learning approach to an adverse event. Indeed, while a cyberattack occurs, resilient organization could bounce forward (Clément and Rivera, 2017) and engage in learning and change processes (Duchek, 2020). The concept of OR encompasses more than merely reacting to a cyberattack. It also includes preparing for and learning from such an event. Indeed, the broadest definitions of resilience, both in the organizational and cyber domains, include the concepts of anticipating, resisting, adapting and learning (Hillmann *et al.*, 2018; Linkov *et al.*, 2013; Ortiz-de-Mandojana and Bansal, 2016). To be resilient to cyberattacks, various functions of preparation must be included. For example, a business continuity plan (Duchek, 2020; Ferdinand, 2015), vulnerability assessment and training (Sepúlveda Estay *et al.*, 2020). As stated before, training activities are also the critical components of cyber awareness and cyberculture. During a cyberattack, response is conveyed through clearly defined roles and responsibilities, as well as easily accessible and appropriate resources (Tsen *et al.*, 2022). Dedicated cybersecurity resources

serve as facilitators. After a data breach incident, organizations can optimize processes and improve future responses by reflecting on what happened and learning from it (Annarelli *et al.*, 2020; Linkov *et al.*, 2013).

In line with what reported in prior research, this study focuses on assessing the cyber organizational readiness of a sample of 53 Italian small and medium enterprises (SMEs) in the Italian information and communication technology (ICT) sector. This research focuses on SMEs for several reasons. It is necessary to point out that SMEs are increasingly targeted by cyber criminals; indeed, according to Segal (2021), "small businesses are three times more likely to be targeted by cybercriminals than larger companies" (p. 1). In line with this discussion, Bada and Nurse (2019) point out that cybercrime and cyberattacks are becoming more focused on SMEs. Although small and large businesses share some commonalities regarding cybersecurity (Tam *et al.*, 2021), SMEs have some specific characteristics that should be discussed. According to the European Union Agency for Cybersecurity (ENISA, 2021), SMEs are now facing cybersecurity challenges such as low budgets, lack of cyber skills and a major increase in cyberattacks. These elements were also reported by several research studies, which point out how SMEs have difficulty sourcing budgets and cyber experts, and lack awareness and policy (D'Arcy *et al.*, 2009; Kuusisto and Ilvonen, 2003; Paulsen, 2016). Bada and Nurse (2019) showed that SMEs face the same issues as large companies, but with less resources. SMES are vital to the economy of many European countries, including Italy. Most organizations in this country are small or very small, and often family owned. Although the importance of SMEs is widely acknowledged, "few studies have sought to gauge SMEs' attitude toward cybersecurity" (Wilson *et al.*, 2022, p. 397). We focus on the ICT sector, as the report on cybersecurity in Italy (Associazione italiana per la Sicurezza Informatica, 2022) indicated that it ranks second among all the sectors that are targeted by cybercriminals, with a strong increase in the number of attacks in the past four years. This paper is structured as follows: first, a detailed description of the sample and method is provided (Section 2). The results and related discussion (Section 3) are then presented.

2. Method

Informed by mixed method research ideas, this study is conducted consistent with the principles of the explanatory sequential mixed method design (Creswell, 2014). According to Hurmerinta-Peltomäki and Nummela (2006), mixed method research is valuable in increasing findings validity and informing second data source collection, resulting in a broad and deep understanding of the phenomena under investigation. Following these principles, this study adopted a quanti-qualitative methodology. The quantitative data were collected through a questionnaire, which refers to the cybersecurity organizational readiness assessment tool developed by Neri *et al.* (2022). This questionnaire allows an in-depth investigation of technical and organizational elements of cybersecurity organizational readiness. The questionnaire consisted of four main sections:

(1) technical questions;
(2) organizational questions;
(3) number of cyberattacks and main type; and
(4) organizational information (e.g. number of employees and annual turnover).

Although its first section focuses on technical features, in line with what found in prior research, each element can be allocated to one of the identified dimensions of cyber organizational readiness. Therefore, the first two sections were combined. Each section was assigned a code, specifically:

- TO (technical and organizational focus);
- CA (investigation of cyberattacks); and
- OI (organizational information).

Each question was then associated with the related code and an ascendent number. Subsequently, qualitative data were collected through semi-structured interviews. We generated a set of questions aimed at obtaining more insight into some of the points raised throughout the survey, in accordance with the idea that:

> The focus is on the interview guide incorporating a series of broad themes to be covered during the interview to help direct the conversation toward the topics and issues about which the interviewers want to learn. (Qu and Dumay, 2011, p. 246)

Key themes were related, but not limited to, training activities, management of critical information and barriers to cybersecurity policy implementation. Each interview lasted a maximum of 60 min and was transcribed verbatim. Each researcher was responsible for reviewing and interpreting each interview. This allowed the emerging themes to be shared as much as possible. In addition to this, after transcription, each interview was forwarded to the respective interviewees so that they could confirm the content and, if necessary, add missing information. Both stages of the research focused on gathering information from the SMEs' key informants, because they provide thorough knowledge of the object of research, given their personal experience. Within the scope of this research, we therefore referred to CISO, information technology (IT) specialist and chief security officer (CSO).

2.1 Sample

This research focused on an initial sample of 114 ICT SMEs. The survey for the quantitative analysis was administered between January and March 2021. A total of 53 SMEs answered the questionnaire. All completed questionnaires were considered valid for the analysis, resulting in a 46.49% response rate. Specifically, survey administration results show that the sample contains 10% medium-sized enterprises, 47% small enterprises and 43% micro enterprises (See Graph 1). The medium-sized sector is underrepresented in the distribution results. However, this is consistent with the composition of Italy's SME economic structure, of which 83.1% consists of small businesses, according to the most recent Cerved (2022) report. The quantitative questionnaire was administered to each organization's key informants. Both CEOs and IT managers could respond to the survey to conform to the scope of this research. In many cases, the respondents depended on the size of the organization: in smaller companies, roles frequently overlap. After the quantitative assessment, semi-structured interviews were conducted to investigate the themes from the survey and to gain insight into the motivations behind some responses. Sample description is consistent with the main characteristics provided by the European Union SMEs classification. Following these prescriptions, the sample is classified through and aggregate of yearly turnover and numbers of employees.

3. Results and discussion

Given the quantitative–qualitative nature of the research, the findings are discussed below through thematic aggregation. First, we examine the survey results. The insights gained from the semi-structured interviews are then presented. The answers to the questions covered in this section are provided in percentage form in Table 1.

Prior to the discussion of the key areas of cybersecurity readiness and related results, some interesting technical elements should be mentioned. As we stated previously, some survey questions are technical-organizational in nature, allowing us to analyze some aspects

Table 1.
Survey results

Code	Question	% Yes	% No
TO01	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.	85.2	14.8
TO02	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.	70.4	29.6
TO05	Does the organization manage critical, business-relevant information?	83.3	16.7
TO07	Are the vulnerabilities in the organization's tools and resources (e.g. the hardware, software, data, devices and insiders) regularly identified and documented?	55.6	44.4
TO08	Has a vulnerability plan been developed and implemented?	55.6	44.4
TO09	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 cyberattack been identified and analyzed?	50	50
TO10	Does the organization have a historical record of cyberattacks?	46.3	53.7
TO11	Is there an ongoing process to monitor and identify internal and external threats?	55.6	44.4
TO12	Are the threats, vulnerabilities and probabilities of an occurrence, and the resulting impacts used to determine the risk?	50	50
TO13	Does the organization refer to its previous cyberattack experiences when implementing cyber threat management and response procedures?	70.4	29.6
TO14	Does the organization have a recovery plan to execute during or after a cyberattack?	63	37
TO15	Does the organization implement and communicate its cybersecurity policy?	31.5	68.5
TO16	Where applicable, do all of your organization's devices run security software (e.g. antivirus, antimalware)?	90.7	9.3
TO17	Are the staff and relevant third parties aware of and trained in cybersecurity?	63	37
TO17a	Are the training activities mandatory?	38.2	61.8
TO22	Is access to resources (both hardware and software) allowed, given the risk of unauthorized access?	90.7	9.3
TO23	Have all the cybersecurity-related rules and regulations that apply to the organization been identified and implemented?	68.5	31.5
TO23a	If yes, which ones? Choose one or more of the following options:		
	Regulation UE 679/2016 (General Data Protection Regulation – GDPR)	100	
	ISO/IEC 27001:2013 (the International Standard for Information Security)	16.2	
	Documents regularly published by ENISA (European Union Agency for Cybersecurity) on cybersecurity and risk analysis	8.1	
	Critical Security Controls for Effective Cyber Defense, a document issued by the Center for Information Security	2.7	
	A COBIT (Control Objectives for Information and Related Technologies) framework applied in IT governance and management as a best practice	0	
	NIST (National Institute of Standards and Technology) framework	10.8	
TO25	Are the roles and responsibilities regarding cybersecurity defined and disclosed to staff and relevant third parties (e.g. customers, suppliers and partners)?	61.1	38.9

(*continued*)

Table 1.

Code	Question	% Yes	% No
TO25a	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	42.4	
	A systems vulnerability analyst whose role is to analyze the system to identify potential vulnerabilities	33.3	
	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	78.8	
	An information security manager whose role is to improve the organization's security from a technical and management perspective	30.3	
	The employees know what to do in the event of a cyberattack	57.6	
	Roles and responsibilities are coordinated and shared with external partners	33.3	
	Customers are adequately informed of cybersecurity requirements (e.g. privacy, data processing and data retention)	54.5	
CA01	Has your company been a target of cyber-attacks in the past year (attempted or suffered)?	25.9	74.1
CA01a	What kind? Choose one or more of the following options:		
	Information, such as about users or computer systems, obtained due to human interaction (phishing)	42.9	
	Hackers blocking the system's use to obtain money (ransom) (ransomware)	21.4	
	Viruses, Trojan horses and generic malicious software (malware)	42.9	
	The network or services being saturated, making them inaccessible or unreachable (DDoS)	35.7	
	Administrator credentials being extracted from the network (APT – advanced persistent threat)	0	
	Database content being accessed and extracted (SQLi - structured query language injection)	7.1	
	Large amount of information obtained about the system, such as how it works or the data it contains (hacking)	0	

Source: Authors' own creation

relating to the technological side of cybersecurity. These are the aspects that obtained the highest result rate. This could be related to the increase of engineering or IT skills within the ICT sector. According to survey results, almost all SMEs catalogue their hardware and software systems. Moreover, similar results could be noted for both hardware and software inventory, which is stated to be updated regularly or when a change occurs (e.g. adding/removing users, adding/removing managers and a change in the physical location). It is important to have a thorough awareness of organizational assets (e.g. hardware and software systems) and to update it regularly, especially when preparing for a cyberattack. Indeed, asset management needs to be implemented to understand which assets needs to be protected. Asset management is one of the functions found in the identification of many cybersecurity standards, such as International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001:2013, National Institute of Standards and Technology (NIST) and Control Objectives for Information Technologies (COBIT) frameworks. Encouraging results can then be observed in the areas of security software, which receive the highest rate of affirmative responses. Installing security systems undoubtedly provides a foundational level of organizational protection, especially for SMEs. However, from a technical perspective, the:

> Days have gone when your antivirus alone protected your system single handedly removing all threats classified in its rule book as malicious. Modern day cyberattacks are far more advanced than the traditional attacks. (Sibi Chakkaravarthy *et al.*, 2019, p. 3)

Forms of risk prevention from unauthorized access received 90.7% affirmative responses. In line with several cybersecurity frameworks (e.g. NIST and COBIT), the survey listed forms of protection that are useful for implementing the necessary measures to ensure the protection of the enterprise's assets. Continuing with this primary technical discussion, a brief focus on the regulations and standards adopted by the SMEs under analysis is useful. Although good practices included in frameworks such as NIST and COBIT, or even ISO:IEC 27001:2013, have yielded positive results, the same cannot be said for the overall formal implementation of these frameworks. The mandatory General Data Protection Regulation (GDPR) is the main regulation framework that has been adopted, according to survey results. These analyses suggest that frameworks and nonmandated standards are not equally valued and implemented by SMEs, despite being extremely useful tools. This could be a useful indication of how these, too, might hope to become more than just schemas to refer to in the future, but actual regulations to be implemented. Although many of the survey questions are referenced in a wide range of security standards and frameworks, they are examined below in terms of their contribution to each of the key constituent areas of cybersecurity readiness, and the organizational implications of those areas.

3.1 Cybersecurity awareness and cybersecurity culture

The majority of SMEs (63.7%) state that they undertake training activities. A preliminary analysis, however, revealed that only 38.2% make these activities mandatory. To investigate how training is actually performed, it was necessary to explore this topic during the semi-structured interviews. The interviews highlighted a recurring theme: training is handled autonomously by each employee, and regular courses are not available. Cybersecurity training is managed internally and in accordance with current demands:

> At the moment, there is an unorganized individual training path. Training is provided if it is perceived beneficial to the company. Self-training is also available. (CISO)

Only 31.5% of SMEs have a cybersecurity policy in place. The reasons for nonimplementation were investigated during the interviews. The policy was repeatedly replaced by more or less structured procedures, often unwritten:

> Yes, procedures are outlined to colleagues, but they are not actually documented as they should be by standard certification procedures. Everyone knows what to do in the event of a problem, but nothing is written down. (IT director)

It then emerged that the procedures put in place are frequently deemed to be sufficient to protect the organization, and the implementation of cybersecurity policy is perceived as unnecessary compared to organizational needs:

> We do not implement cybersecurity policies because the minimum level of security we provide is sufficient to ensure system security. (IT specialist)

According to what is reported in prior research, training and cybersecurity policy are critical components to develop both cybersecurity awareness and a cybersecurity culture. SMEs did not score satisfactorily in these two areas, which will require additional attention and improvement in future. Resource availability is another key consideration. The interviews enquired about the budgets for cybersecurity and related resources. In most cases, no dedicated resources are available, but the budget and requirements are approved on an as-needed basis, e.g. when a problem occurs:

> These things (cybersecurity) are pretty much included in what we spend on R&D (resource and development), we don't have a defined budget. (IT manager)

A dedicated budget and resources are related to some dimensions of both cybersecurity culture and cybersecurity OR. However, the lack of a defined budget is in line with the difficulties encountered by SMEs in dealing with the cyber environment.

3.2 Cybersecurity organizational resilience

More than half of SMEs identified organizational vulnerabilities and, as a result, implement a vulnerability plan. There are also encouraging findings in the areas of cyber risk and potential impact identification. According to what is reported in prior research, all these activities are related to the anticipatory phase of OR, in which the organization prepares for an unexpected event (e.g. a cyberattack). When these activities are performed synergically, they lead to an appropriate implementation of a cybersecurity strategy. Vulnerability assessment indeed ensures the "developing [of] a proactive approach to threat mitigation and enhancing [of] an organization's adaptive capacity" (Burnard and Bhamra, 2011, p. 5591). Many SMEs implement a system for monitoring external threats. This activity should be viewed as a precursor to developing situational awareness. This implies that the practice leads to identifying unexpected events sooner (Vogus and Sutcliffe, 2007), understanding cyberthreat frequency and sophistication better (Ferdinand, 2015) and detecting cyberattacks quicker, if implemented properly. When an attack occurs, roles and responsibilities become a key factor in responding effectively. The resilience literature embraces the idea of a structure that is not managed hierarchically. Roles and responsibilities become critical in terms of OR in the face of cyberattacks. In this regard, 61.1% of SMEs have identified cybersecurity roles and responsibilities, both internally and in relation to relevant third parties. The options for a cybersecurity specialist and a computer network administrator received the highest number of affirmative responses. The existence of these roles and of cybersecurity-focused responsibilities is beneficial in optimizing responses to cyberattacks. The specialized knowledge feature is also critical in

shaping a cybersecurity culture. After a data breach incident, it is necessary to reflect on what happened, and to ensure that the new knowledge is incorporated in future processes. In this regard, approximately half of SMEs have experienced cyberattacks. It is useful to document a data breach incident (including its causes and consequences) for future process optimization. Seventy percent of the respondents referred to previous cyber incident experiences when implementing cyberthreat management and response procedures. In addition, 63% of the participants stated that they implement a recovery plan to be executed in the event of a cyberattack. When compared to what is reported in prior research, these findings lead to the conclusion that SMEs are able to develop learning processes to initiate new practices and acquire new values, even when they have already been the target of a cyberattack.

3.3 Cyber threats: methodologies and main target

In addition to the key issues of cybersecurity readiness, it is interesting to focus on three other elements that allow us to provide an assessment of the cyber scenarios of ICT organizations. According to the findings, 25.9% of SMEs have been victims of a cyberattack. It is possible to put the results in a better context, thanks to the interviews, giving this result a different connotation. In fact, many organizations do not consider e-mail-based cyberattacks (such as phishing) to be cyberattacks at all, especially when no data is lost. It was mentioned several times during the interviews that e-mail cyberattacks are very likely to occur. This emphasizes the importance of using the mixed method when assessing cybersecurity readiness and cybersecurity issues. As an example, although it was not stated in the questionnaire, it later emerged during interviews that:

> [e]mails of this type (phishing) can sometimes get past spam and antivirus checks, but everyone knows that if there is even the slightest suspicion, it should be counter verified. (IT manager)

> Our system logs send us a security report every month in which malicious activities are detected. We are aware of spam, blocked IP (Internet Protocol) addresses, some form signup attempts, or admin username login attempts. [. . .] attack attempts are made daily, but nothing has ever broken through, nor have there been more elaborate attack attempts. (IT specialist)

The data on the types of cyberattacks is consistent with these considerations. Phishing and malware are indeed the categories with the highest scores. These forms of cyberattacks regularly take advantage of human behavior, and technology cannot always assumed to be the exclusive source of protection against them. These findings reinforce the idea that cybersecurity readiness is a necessary measure for protection when navigating the cyber domain effectively and safely. The data are also consistent with recent reports on cyberattacks, in which malware and phishing rank first and fourth in absolute numbers of attacks, respectively. Malware accounts for 41% of the total number of attacks recorded in Italy, according to the CLUSIT Report on cybersecurity in Italy. It is also worth noting that 83.3% of SMEs deal with critical information, which indicates that the information assets available to cyber criminals are vast and diverse, ranging from customer or employee data to patents and hardware prototypes. This became clear during the interviews:

> Prototype schematics, technical specifications, and user manuals for our software. (IT specialist)

> Data of a technical and design nature, as the solutions we propose is intellectual property protected. (CISO)

Whether or not this result is related to the number and type of attacks experienced by SMEs, it is clear that SMEs currently face significant economic and reputational risks, and that these information assets are valuable to cyber criminals.

4. Conclusion

This research has identified some strengths in the field of SME cybersecurity readiness, as well as areas that need improvement. From a technical perspective, the surveyed SMEs showed encouraging results, which could be attributed to the IT skills of their employees working in the ICT sector. Many elements of OR when confronted with cyber-attacks, such as vulnerability assessment, roles and responsibilities and incident reporting, are also accounted for satisfactorily. Some factors, such as training and cybersecurity policy, require significant improvement. Training is limited and, when available, fragmented. If a cybersecurity policy is implemented properly, it consists of a set of best practices, but its value is generally not clearly acknowledged. These two features constitute the foundation of cybersecurity awareness, and, thus, a cybersecurity culture. The absence of a dedicated budget suggests a lack of specific and long-term planning, preventing the allocation of adequate resources. Many of the SMEs surveyed have been the victims of cyberattacks that involve techniques that take advantage of the human factor. This result, together with the type of information processed by SMEs, highlights that the areas in need of improvement are exactly those that are most important in fighting cyber threats. As is the case in other research, this study also has limitations. Although these could be seen as a gap, the authors see each limitation as an opportunity for future studies on cybersecurity organizational readiness. The focus on the Italian context prevents this research from comparison with other countries, and it precludes generalizability. The scope of this research justified this focus decision because of the access to sector key constituents (e.g. academic institution focused on the research topic) and the collaboration with professional ICT associations. In addition, Italy is particularly worth investigating because it is severely affected by cybersecurity issues and a massive increase in cyberattacks, according to various national and global reports as well as news reported by ANSA (National Associated Press Agency). Furthermore, the Italian economic system primarily consists of SMEs, which reflects sample choice and composition. The focus on the Italian ICT sector was relevant, given the increased investment in the Italian ICT market, especially after the COVID-19 pandemic. Future research could propose a comparison of the ICT sector in both European and non-European countries. It could also be valuable to broaden the sample and include SMEs from other sectors within the Italian context.

References

Alshaikh, M., Maynard, S.B., Ahmad, A. and Chang, S. (2018), "An exploratory study of current information security training and awareness practices in organizations", *HI International Conference on System Sciences*, doi: 10.24251/HICSS.2018.635.

Angst, C.M., Block, E.S., D'Arcy, J. and Kelley, K. (2017), "When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches", *MIS Quarterly*, Vol. 41 No. 3, pp. 893-898, doi: 10.25300/MISQ/2017/41.3.10.

Annarelli, A., Nonino, F. and Palombi, G. (2020), "Understanding the management of cyber resilient systems", *Computers and Industrial Engineering*, Vol. 149, p. 106829, doi: 10.1016/j.cie.2020.106829.

Assintel (2021), "Assintel report 2021", available at: www.assintel.it/osservatori-2/assintel-report/assintel-report-2021/

Associazione italiana per la Sicurezza Informatica (2022), "Rapporto clusit 2022 sulla sicurezza ICT in Italia", available at: https://clusit.it/wp-content/uploads/download/Rapporto-Clusit-marzo-2022_web.pdf

Bada, M. and Nurse, J.R.C. (2019), "Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs)", *Information and Computer Security*, Vol. 27 No. 3, pp. 393-410, doi: 10.1108/ICS-07-2018-0080.

Burnard, K. and Bhamra, R. (2011), "Organisational resilience: development of a conceptual framework for organisational responses", *International Journal of Production Research*, Vol. 49 No. 18, pp. 5581-5599, doi: 10.1080/00207543.2011.563827.

Cerved (2022), "Rapporto regionale PMI 2022", available at: https://research.cerved.com/rapporti/rapporto-regionale-pmi-a-rischio-la-ripresa-economica-nel-biennio-2022-23/

Chatterjee, D. (2019), "Should executives go to jail over cybersecurity breaches?", *Journal of Organizational Computing and Electronic Commerce*, Vol. 29 No. 1, pp. 1-3, doi: 10.1080/10919392.2019.1568713.

Clément, V. and Rivera, J. (2017), "From adaptation to transformation: an extended research agenda for organizational resilience to adversity in the natural environment", *Organization and Environment*, Vol. 30 No. 4, pp. 346-365, doi: 10.1177/1086026616658333.

Corallo, A., Lazoi, M., Lezzi, M. and Luperto, A. (2022), "Cybersecurity awareness in the context of the industrial internet of things: a systematic literature review", *Computers in Industry*, Vol. 137, p. 103614, doi: 10.1016/j.compind.2022.103614.

Corradini, I. (2020), "Redefining the approach to cybersecurity", in Corradini, I. (Ed.), *Building a Cybersecurity Culture in Organizations: How to Bridge the Gap Between People and Digital Technology*, Springer International Publishing, pp. 49-62, doi: 10.1007/978-3-030-43999-6_3.

Creswell, J.W. (2014), *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*, 4th ed., Sage Publications, Thousand Oaks, CA, Vol. 10, p. 215.

D'Arcy, J., Hovav, A. and Galetta, D. (2009), "User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach", *Information Systems Research*, Vol. 20 No. 1, pp. 1-20, doi: 10.1287/isre.1070.0160.

da Veiga, A., Astakhova, L.V., Botha, A. and Herselman, M. (2020), "Defining organisational information security culture—perspectives from academia and industry", *Computers and Security*, Vol. 92 No. 1, pp. 1-23, doi: 10.1016/j.cose.2020.101713.

Duchek, S. (2020), "Organizational resilience: a capability-based conceptualization", *Business Research*, Vol. 13 No. 1, pp. 215-246, doi: 10.1007/s40685-019-0085-7.

ENISA (2021), "Cybersecurity for SMEs. Challenges and recommendation", available at: www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

Ferdinand, J. (2015), "Building organisational cyber resilience: a strategic knowledge-based view of cyber security management", *Journal of Business Continuity and Emergency Planning*, Vol. 9 No. 2, pp. 185-195.

He, W., Ash, I., Anwar, M., Li, L., Yuan, X., Xu, L. and Tian, X. (2019), "Improving employees' intellectual capacity for cybersecurity through evidence-based malware training", *Journal of Intellectual Capital*, Vol. 21 No. 2, pp. 203-213, doi: 10.1108/JIC-05-2019-0112.

Hillmann, J., Duchek, S., Meyr, J. and Guenther, E. (2018), "Educating future managers for developing resilient organizations: the role of scenario planning", *Journal of Management Education*, Vol. 42 No. 4, pp. 461-495, doi: 10.1177/1052562918766350.

Huang, K. and Pearlson, K. (2019), "For what technology can't fix: building a model of organizational cybersecurity culture", *Proceedings of the 52nd HI International Conference on System Sciences*, available at: https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/7083b12c-3069-42ec-ae0e-0ee6a3989437/content

Hurmerinta-Peltomäki, L. and Nummela, N. (2006), "Mixed methods in international business research: a value-added perspective", *Management International Review*, Vol. 46 No. 4, pp. 439-459, doi: 10.1007/s11575-006-0100-z.

Kortjan, N. and Von, S.R. (2014), "A conceptual framework for cyber-security awareness and education in SA: research article", *South African Computer Journal*, Vol. 52 No. 1, pp. 29-41, doi: 10.10520/EJC154952.

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

Li, L., He, W., Xu, L., Ash, I., Anwar, M. and Yuan, X. (2019), "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior", *International Journal of Information Management*, Vol. 45, pp. 13-24, doi: 10.1016/j.ijinfomgt.2018.10.017.

Linkov, I., Eisenberg, D.A., Plourde, K., Seager, T.P., Allen, J. and Kott, A. (2013), "Resilience metrics for cyber systems", *Environment Systems and Decisions*, Vol. 33 No. 4, pp. 471-476, doi: 10.1007/s10669-013-9485-y.

Mclean, M. (2021), "2023 Must-know cyber attack statistics and trends", *Embroker*, available at: www.embroker.com/blog/cyber-attack-statistics/

Martins, A. and Eloff, J. (2002), "Assessing information security culture", in Ghonaimy, M.A., El-Hadidi, M.T. and Aslan, H.K. (Eds), *Security in the Information Society: Visions and Perspectives*, Springer, Boston, MA, pp. 1-14, available at: https://digifors.cs.up.ac.za/issa/2002/proceedings/A026.pdf

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

Neri, M., Niccolini, F. and Pugliese, R. (2022), "Assessing SMEs' cybersecurity organizational readiness: findings from an Italian survey", *Online Journal of Applied Knowledge Management*, Vol. 10 No. 2, pp. 1-22, doi: 10.36965/OJAKM.2022.10(2)1-22.

Nurse, J.R.C. (2021), "Cybersecurity awareness", in Jajodia, S., Samarati, P. and Yung, M. (Eds), *Encyclopedia of Cryptography, Security and Privacy*, Springer, Berlin, Heidelberg, doi: 10.1007/978-3-642-27739-9_1596-1.

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

Ortiz-de-Mandojana, N. and Bansal, P. (2016), "The long-term benefits of organizational resilience through sustainable business practices", *Strategic Management Journal*, Vol. 37 No. 8, pp. 1615-1631, doi: 10.1002/smj.2410.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. and Zwaans, T. (2017), "The human aspects of information security questionnaire (HAIS-Q): two further validation studies", *Computers and Security*, Vol. 66, pp. 40-51, doi: 10.1016/j.cose.2017.01.004.

Parsons, K.M., Young, E., Butavicius, M.A., McCormac, A., Pattinson, M.R. and Jerram, C. (2015), "The influence of organizational information security culture on information security decision making", *Journal of Cognitive Engineering and Decision Making*, Vol. 9 No. 2, pp. 117-129, doi: 10.1177/1555343415575152.

Pattinson, M., Butavicius, M., Lillie, M., Ciccarello, B., Parsons, K., Calic, D. and McCormac, A. (2019), "Matching training to individual learning styles improves information security awareness", *Information and Computer Security*, Vol. 28 No. 1, pp. 1-14, doi: 10.1108/ICS-01-2019-0022.

Paulsen, C. (2016), "Cybersecuring small businesses", *Computer*, Vol. 49 No. 8, pp. 92-97, doi: 10.1109/MC.2016.223.

Qu, S.Q. and Dumay, J. (2011), "The qualitative research interview", *Qualitative Research in Accounting and Management*, Vol. 8 No. 3, pp. 238-264, doi: 10.1108/11766091111162070.

Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A. and Herawan, T. (2015), "Information security conscious care behavior formation in organizations", *Computers and Security*, Vol. 53 No. 2015, pp. 65-78, doi: 10.1016/j.cose.2015.05.012.

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

Segal, E. (2021), "Small businesses are more frequent targets of cyberattacks than larger companies: new report", *Forbes*, available at: www.forbes.com/sites/edwardsegal/2022/03/30/cyber-criminals/ (accessed 31 January 2023).

Sepúlveda Estay, D.A., Sahay, R., Barfod, M.B. and Jensen, C.D. (2020), "A systematic review of cyber-resilience assessment frameworks", *Computers and Security*, Vol. 97 No. 1, pp. 1-15, doi: 10.1016/j.cose.2020.101996.

Sibi Chakkaravarthy, S., Sangeetha, D. and Vaidehi, V. (2019), "A survey on malware analysis and mitigation techniques", *Computer Science Review*, Vol. 32 No. 1, pp. 1-23, doi: 10.1016/j.cosrev.2019.01.002.

Tam, T., Rao, A. and Hall, J. (2021), "The good, the bad and the missing: a narrative review of cyber-security implications for Australian small businesses", *Computers and Security*, Vol. 109, p. 102385, doi: 10.1016/j.cose.2021.102385.

Tejay, G. and Klein, G. (2021), "Organizational cybersecurity journal editorial introduction", *Organizational Cybersecurity Journal: Practice, Process and People*, Vol. 1 No. 1, pp. 1-4, doi: 10.1108/OCJ-09-2021-017.

Tsen, E., Ko, R.K.L. and Slapnicar, S. (2022), "An exploratory study of organizational cyber resilience, its precursors and outcomes", *Journal of Organizational Computing and Electronic Commerce*, Vol. 32 No. 2, pp. 153-174, doi: 10.1080/10919392.2022.2068906.

Uchendu, B., Nurse, J.R.C., Bada, M. and Furnell, S. (2021), "Developing a cyber security culture: current practices and future needs", *Computers and Security*, Vol. 109, p. 102387, doi: 10.1016/j.cose.2021.102387.

Van Niekerk, J. and Von Solms, R. (2006), "Understanding information security culture: a conceptual framework", *ISSA*, pp. 1-10.

Vogus, T.J. and Sutcliffe, K.M. (2007), "Organizational resilience: towards a theory and research agenda", *Proceedings of IEEE international conference on systems, man and cybernetics, NJ, USA*, IEEE, pp. 3418-3422.

Von Solms, R. and Van Niekerk, J. (2013), "From information security to cyber security", *Computers and Security*, Vol. 38 No. 1, pp. 97-102, doi: 10.1016/j.cose.2013.04.004.

Wilson, M., McDonald, S., Button, D. and McGarry, K. (2022), "It won't happen to me: surveying SME attitudes to cyber-security", *Journal of Computer Information Systems*, Vol. 63 No. 2, pp. 1-13, doi: 10.1080/08874417.2022.2067791.

Further reading

Assintel (2021), "Assintel report 2021", available at: www.assintel.it/osservatori-2/assintel-report/assintel-report-2021/

Associazione italiana per la Sicurezza Informatica (2022), "Rapporto Clusit 2022 Sulla Sicurezza ICT in Italia", available at: https://clusit.it/wp-content/uploads/download/Rapporto-Clusit-marzo-2022_web.pdf

World Economic Fortum (2022), "Global risks report 2022", available at: www.weforum.org/reports/global-risks-report-2022/ (accessed 27 January 2023).

About the authors

Martina Neri is a PhD candidate in Business Administration and Management at the Department of Economics and Management, University of Pisa, Italy. She obtained 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. She has

been a visiting PhD student at the Centre Universitaire d'Informatique, University of Geneva, Switzerland. Martina Neri is the corresponding author and can be contacted at: martina.neri@phd.unipi.it

Federico Niccolini is Associate Professor of Organizational Science at the Department of Political Sciences, University of Pisa, Italy. 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 PhD courses. He coordinated national and international (including EU-funded) projects. He has been a visiting scholar/professor at 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.

Luigi Martino is Assistant Professor at the Department of Political and Social Sciences of the University of Bologna, Italy. He obtained a PhD at the Scuola Superiore Sant'Anna, Pisa, with a research project on "Improve IT security for critical infrastructures in Italy: the public-private partnership model against cyber-attacks." His research interests include inter alia, cyber security, security studies and theories of international relations and the dynamics of cyberspace in the international system.