Complex Systems Informatics and Modeling Quarterly (CSIMQ)
eISSN: 2255-9922
Published online by RTU Press, https://csimq-journals.rtu.lv
Article 185, Issue 33, December 2022/January 2023, Pages 53–66
https://doi.org/10.7250/csimq.2022-33.04

CyberSecurity Readiness: A Model for SMEs based on the Socio-Technical Perspective

Haiat Perozzo[1*], Fatema Zaghloul[2], and Aurelio Ravarini[1]

[1] Università Carlo Cattaneo LIUC, Corso G. Matteotti, 22, Castellanza, 21053, Italy
[2] University of Southampton Business School, Southampton, UK

hperozzo@liuc.it, fatema.zaghloul@soton.ac.uk, aravarini@liuc.it

Abstract. Like most companies, small and medium-sized enterprises (SMEs) have become reliant on digital technology for their day-to-day business operations. While valuable, this comes with challenges; one of which is the rise in cybercrime. In terms of their cybersecurity resilience and risk, SMEs are among the most vulnerable and least mature. This article addresses a gap in the literature that has neglected cybersecurity readiness in SMEs. The study proposes a CyberSecurity Readiness Model for SMEs (CSRM-SME) based on a Socio-Technical view of organizations. The model was applied to three SMEs to assess their cybersecurity readiness and further understand the environment and strategies adopted to prevent and manage cyber-attacks.

Keywords: Cyber Security, Socio-Technical System, Readiness Model, Small and Medium-Sized Enterprise, SMEs.

1 Introduction

Businesses, including small and medium-sized enterprises (SMEs), rely on digital technology for their day-to-day business operations. While valuable, this comes with challenges: the rise in cybercrime. Security or data breaches, hacker attacks, employee errors, espionage, and ransomware, are the leading causes of cyber incidents, and they are becoming increasingly costly and more prevalent. Businesses are becoming more susceptible to cyberattacks as a result of the increasing interconnectedness of the economy and the subsequent digital transformation expedited by the Covid-19 pandemic [1], [2]. Survey reports highlight a continual rise in the severity and frequency of cyberattacks [3]. The Allianz Risk Barometer (2022) [4], to which 2,650 risk management experts from 89 countries contributed, reflects this development: cyber incidents have replaced 'business and supply chain interruption' as the top risk. Furthermore, numerous previous studies revealed that SME respondents have reported cyberattacks (e.g., [5]). Consequently, businesses risk millions in damages, reputational losses [6], and business interruptions that jeopardize their continuity and sustainability. Therefore, research on the risks of

[*] Corresponding author

Reference: H. Perozzo, F. Zaghloul, and A. Ravarini, "CyberSecurity Readiness: A Model for SMEs based on the Socio-Technical Perspective," Complex Systems Informatics and Modeling Quarterly, CSIMQ, no. 33, pp. 53–66, 2022. Available: https://doi.org/10.7250/csimq.2022-33.04

Additional information. Author ORCID iD: F. Zaghloul – https://orcid.org/0000-0002-8626-807X, A. Ravarini – https://orcid.org/0000-0002-3114-9727. PII S225599222200185X. Received: 31 October 2022. Accepted: 29 December 2022.

cyberattacks has shifted towards a context that focuses on prevention, preparedness, and cybersecurity readiness [7].

It was once believed that large corporations were more susceptible to cyber-attacks compared to SMEs [8]. Contrarily, despite the fact that businesses of all sizes are facing an increase in cybercrime, SMEs are one particular sector that is increasingly being targeted [9]. In contrast to large-size organizations, SMEs typically suffer from a lack of knowledge, expertise, and resources [3], [10]. In general, due to their low level of awareness with respect to cyber threat reality, they seldom perform thorough cyber-risk assessments and have been shown to have poor cybersecurity adoption [5].

This situation in Italy is particularly critical: on the one hand, the high number of SMEs make them play a crucial role in the Italian economy; on the other hand, the number and the severity of cyberattacks have increased in the past few years. According to the Digital Attacks Observatory (OAD)[†] 2020, the number of attacks reported by SMEs went up from 0% in 2019 to 22.2% at the beginning of 2020. It is suggested that if cybersecurity readiness is lacking or inadequate, organizations will find it difficult to obtain the necessary resources to attain a sufficient degree of cybersecurity to protect their digital assets.

Despite these evidences, there is a dearth of research focusing on cybersecurity readiness in SMEs [11], [12]. While the literature offers some processes of operationalizing cybersecurity and resilience via self-assessment questionnaires, maturity models, and frameworks, these frameworks usually consist of detailed lists of actions and policies, without means of action prioritization or strategies on how to implement such actions within an organization [12]. These characteristics constrain the application of the existing approaches to large enterprises, making it difficult for SMEs, which lack the necessary skills and resources, to face the current challenges of cybersecurity threats.

In this article, we address this gap by outlining the limitations of current readiness models and thereby proposing a framework that seeks to consider a socio-technical perspective on the phenomenon.

The remainder of the article proceeds as follows: first, In Section 2, we review the existing cybersecurity readiness models developed both by consultancy firms and discussed in the scholarly literature, extending the discussion by applying the socio-technical system model to such readiness frameworks. The following Section 3 outlines the methodology and data collection approach, where we propose a new model for the assessment of the CyberSecurity Readiness in SMEs (CSRM-SME). We finally, in Section 4, apply this model to three SMEs in the manufacturing sector in Italy and discuss the outcomes both in terms of the effectiveness of the model and in terms of diversity in approaching the cybersecurity threats by the studied SMEs. We conclude the article in Section 5.

2 Literature Review

2.1 Cybersecurity: The Context of SMEs

SMEs are considered the backbone of the EU and, in particular, the Italian economy. The goal of cybersecurity is the protection of business IT infrastructure and the data necessary for day-to-day operations, in addition to its people, processes, and assets.

Since the first wave of Covid-19, studies highlight that SMEs do not consider themselves favorable targets for cybercrime since they are ‘small’ [5], [13]. Among the causes of the increased exposure of small businesses are factors ranging from low cybersecurity awareness of personnel,

[†] The Digital Attacks Observatory (OAD) is the only independent online survey in Italy concerned with collecting data regarding digital attacks on IT systems witnessed by companies and public bodies. The OAD 2020 survey is based on data collected during the entire year of 2019 and the 1st quarter of 2020 when the Covid-19 pandemic occurred.

inadequate protection of critical data, lack of IT cybersecurity specialists, budgetary issues, and low management support [14], [15]. Furthermore, dependence on third party organizations to deal with cybersecurity has increased after Covid-19, thereby shifting the work in IT environments out of the control of the SME [16].

With respect to the number of malware attacks, Italy ranked fourth in the world and first in Europe in 2021 [17]. According to the OAD 2020 survey [18], based on 310 companies from various industries across Italy, the largest volume of attacks were reported by businesses in the services and manufacturing sectors. Furthermore, more than 50% of SMEs lack the capacity to respond to emerging threats. One out of every five businesses does not have an investment strategy for IT security or merely allots resources as needed. Small business managers typically oppose IT security spending because they see it as a cost rather than an investment. Analysts in the sector anticipate increasing investments in SMEs as this mentality gradually shifts, as well as cybersecurity becoming a key element in Italy’s digital transformation strategy.

A limitation of current research is that the context frequently investigated is that of critical infrastructures and large organizations. It is imperative that SMEs take appropriate cybersecurity measures in light of the rising number of cyberattacks and the fact that these businesses frequently lack effective defenses against attackers due to their limited financial resources and lack of skilled security workers.

In response to the increasing risks of cybercrime, there has been a growing number of efforts to both limit the effects of cyber-attacks and prevent their possibility. On this second front, proposals for so-called readiness assessment models have multiplied; they are theoretical frameworks that aim to help companies, typically supported by external consultants, identify the factors that increase the chances of a successful cyber-attack against them. Given the differing approaches found in the practitioner versus academic literature, the literature review draws on both domains. Each perspective uncovers various insights and adopts different perspectives to cybersecurity readiness.

2.2 Cybersecurity Readiness: Consultancy Firms

The largest consultancy firms worldwide (Deloitte, PwC, EY, and McKinsey), have developed models to help organizations assess their exposure to the risk of cyber-attacks. Table 1 provides an overview of the models proposed by the consultancy firms.

The models consist of a structured set of questions that address the issues that are considered as significant in areas including business operations, risk and compliance, technology, strategy, and governance. Our analysis shows that, although the structures of these models differ, the key concepts and issues they address are mostly centered around technical assessments.

The consultancy models focus both on the management of the IT risk and on the allocation of a budget related to IT defense for risk mitigation. However, it is argued that these approaches lack the ability to integrate between multiple domains of cyber-physical systems and to grasp their complexity [19]. Additionally, they are static, unable to account for relationships between causes and effects and for the “dynamics of cyberattacks”, as well as fail to take uncertainty into account [20]. Any effort to manage resources to increase information security, according to Nazareth and Choi [21], must take into account the dynamic nature of security risks.

Table 1. Cybersecurity Readiness: Consultancy Firms

Deloitte	PwC	Ernst & Young (EY)	McKinsey
Do you adopt SSO or AD authentication?	How do cybersecurity automation systems enable your organization?	Does the organization adopt anti-malware or antivirus systems?	Are there any contacts defined when there is a need to discuss cybersecurity topics?
Are we focused and investing in the right things?	Does the organization have Super Users?	Has your organization conducted a risk assessment?	For Super Users, letters of appointment are recorded?
Have you developed an IT System Layer or application map?	Is the workforce in favor of cloud migration programs?	Have the effectiveness of cyber controls been incorporated into your program?	It has an activity tracking tool inside the company servers
Have you established an appropriate cyber risk escalation framework that includes our risk appetite and reporting thresholds?	Does the organization have a log tracking system?	Does the organization periodically conduct penetration tests?	Have you received a risk report in a specific area?
Are appointment letters recorded for super users?	Is cybersecurity integrated into M&A activities?	How does the organization deal with phishing attacks?	When did you last participate in a business continuity exercise?

2.3 Cybersecurity Readiness Models: Scholarly Literature

Reviewing the scholarly literature reveals three main readiness models for SMEs: Cyber Security Canvas [13]; SME Cyber Risk Assessment (SMECRA) [19]; and Listemann's model [22].

The Cyber Security Canvas [13] primarily follows a "one-size-fits-all" principle and is complemented with 'modular building blocks'. The model was developed to help to manufacture SMEs that, for instance, do not have their own IT specialist, and combines the relevant components of the three key models of cybersecurity (i.e., ISO/IEC 27001, NIST, BSI IT-Grundschutz). The model has five layers, and in this case, we will focus on the first layer as it is dedicated to the prevention of cyberattacks and internal evaluation. The starting objective of the framework is the definition of the company's security objectives, not only with respect to information security and their IT security strategy but also with respect to individual orientation and available resources (budget). The following step is concerned with analyzing whether the company has the internal know-how necessary for implementing the required objectives or requires external specialists. The sub-objectives must be specifically distributed to employees to ensure everyone is aware of their role and responsibilities. Although Canvas can be used to improve risk assessment and claims to offer a degree of dynamism, it remains a step-by-step top-down approach.

SMECRA [19] is a system dynamics methodology and tool (based on the NIST framework and the literature) that, first, analyzes the cyber-postures of an SME, and then simulates the impact of different investment strategies. The model was developed based on a generic context of SMEs.

Finally, Listemann's model [22] is a model that has been used in the case of Listemann, an SME Manufacturing Service Provider. In its path towards increased digitalization, the company recognized the need to improve its cybersecurity management. The most relevant potential sources of threats deriving from digitization, in this case, are the following:

- Web portal, website, and social media: The web portal and the website are a solution adopted mainly by those companies that have a medium or high degree of servitization;
- New Data Management Solution: Most SMEs often found themselves archiving most of their documents in structured folders;

- New technologies and techniques: New digital technologies such as IoT, process mining, etc., see the involvement of numerous data belonging to different business functions, as well as the customer.

These models discussed above present a series of limitations that can be effectively highlighted through the lens of the socio-technical perspective.

2.4 Cybersecurity Readiness: A Socio-Technical Perspective

According to Bostrom & Heinen [23], an organization can be represented as a socio-technical system, as shown in Figure 1. The socio-technical system can be subdivided into a technical subsystem, including the devices, tools, and techniques necessary to transform inputs into outputs of the organization (i.e., technology and tasks); and a social system, including employees at all levels, the knowledge, skills, attitudes, values, and needs they bring to the work environment, as well as the reward system and authority structures that exist in the organization and the formal and informal rules and regulations that govern the organization's relations with society at large (i.e., people and structure). The socio-technical system will maximize performance only if the interdependence of these subsystems is explicitly recognized [23]. We extend this discussion, based on [24], [25], by arguing that it is becoming increasingly difficult to clearly differentiate between the technical and social subsystems in the sense that the technological aspect may also consist of social elements such as user acceptance and usability, further reinforcing the importance of considering the social dimension, compared to placing greater weight on the technological dimension.

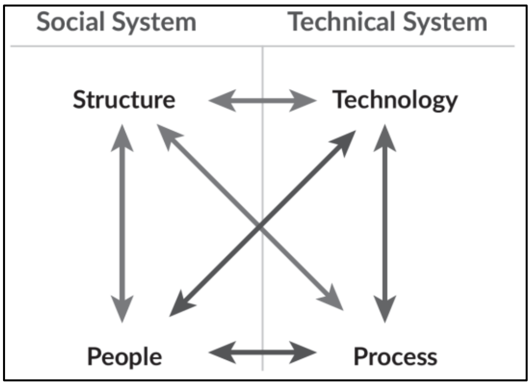

Figure 1. Socio-Technical System Framework (STS Framework) [23]

Based on this discussion and the socio-technical system perspective, the models reviewed above highlight a prevalent focus on the technical component, despite their claims of placing some focus on the human aspect. In particular, the models proposed by the consultancy firms simply do not address the social component as they do not include an assessment of the implications of cybersecurity of the characteristics of the people and the structure of the organization.

With respect to the models available in the scholarly literature, they have limitations that can be explained through the socio-technical model. For example, the limitations of the Cybersecurity Canvas become evident since it has been created starting from the most well-known computer security standards, such as NIST, ISO 27001, etc. These are indeed very strict standards, which therefore limit the dynamism of the model [13]. This signifies that this model places great emphasis on the technical part of the socio-technical model.

The SMECRA model is a model purely oriented to the estimation of an economic nature, thus already proposing a final result, namely the investment, without considering the growth and awareness component of the company. This allows us to observe how the model is linked to the "social" part of the model, in particular, the 'structure'. However, it is clear that the model does not guarantee interdependence with the variable linked to ‘people’. Furthermore, the model still presents a notable component of technicality, making the technical part of the socio-technical model prevail.

Particularly, the use of technical models could be problematic for SMEs. Assessing cybersecurity readiness or conducting cyber-risk assessments using overly technical questions/evaluations may result in inaccurate responses, which could potentially be synonymous with a notional gap rather than the actual absence of a specific element in question. This suggests that the models discussed above may, therefore, not be suitable for all SMEs. If they had been adopted, they would potentially be able to address the issue from a technological standpoint, but the aspects related to the organization and people would remain unaddressed. Hence, it is crucial that the inter-dependence between the social and technical components are addressed.

3 Methodology

3.1 Approach

Since the focus of this research study was to explore cybersecurity readiness in SMEs, we pursued a qualitative multiple case research method. In this context, case research is particularly appropriate for exploratory research of this nature.

We adopt a multiple case study approach, following the principle that “the case study method explores a real-life, contemporary bounded system (a case) or multiple bounded systems (cases) over time, through detailed, in-depth data collection involving multiple sources of information… and reports a case description and case themes” [26]. The purpose of adopting a case study approach is the ability to explore a specific phenomenon in a bounded system, i.e., multiple bounded systems over time, “within its real-life context” [27] and seek an in-depth understanding of people and the cultural and social contexts within which they live.

The data collection was undertaken through semi-structured interviews and reviews of secondary and internal documentation. Interviews lasted on average 45 minutes and each interview was recorded, transcribed, and annotated. Participants were selected based on their role, knowledgeability of the study topic, and experience. We aimed to interview subjects from different business functions (e.g., general manager, IT administrator, managing director, production manager) to understand differing perspectives; those directly involved in the IT field and those who are far from it (but may indirectly be affected by decisions and/or changes).

Three SMEs, belonging to the manufacturing sector in Italy, took part in the study. These companies have different dimensions, different approaches to security and, consequently, different types of cybersecurity awareness and readiness.

1. Company A designs and produces technical articles in rubber and silicone;
2. Company B designs and creates a range of machinery for the paper industry, bookbinding and box factories;
3. Company C deals with the processing of marble.

3.2 CyberSecurity Readiness Model for SMEs (CSRM-SME)

To develop the research instrument to run the interviews we identified a set of variables by integrating the models we had found in the reviewed literature and selecting the variables that match the socio-technical perspective. In the resulting protocol that we developed, we recognized a possible model for assessing the cybersecurity readiness of SMEs, which we name the CyberSecurity Readiness Model (CSRM-SME).

CSRM-SME consists of eight variables (shown in Table 2) that can be assessed through a set of questions (detailed in Table 3). The questions were derived partly from the academic models and partly from the models proposed by consultancy firms.

Table 2. The structure of the proposed CyberSecurity Readiness Model for SMEs

Variable	Motivation/ Description	Reference to STS Framework	Reference
Company Size	Depending on the size of the company there will be different economic and resource availability.	Context	[13]
Degree of responsibility (Governance)	Governance outlines the procedures and policies to manage cybersecurity from a strategic perspective. Therefore, this variable highlights the top management involvement and how cybersecurity is managed in the company.	Social	[12], [14], [15]
Technical skills	Depending on the technical skills possessed by the company, and therefore depending on the presence of specialized human resources or not, it will be able or not to exploit the IT resources currently supplied and organize the company accordingly.	Technical	[14], [15]
Tangible or intangible product	The presence of a tangible product means less need for computer systems, compared to intangible products.	Context	[18]
Degree of servitization	Faced with a greater degree of servitization, the probability that there is a purely online business activity is high. This implies greater vulnerability.	Social	[18]
Dependence on third parties	The degree of cybersecurity depends directly on the suppliers. The degree of protection of a supplier can directly affect the customer.	Social	[16]
Current availability of protection systems	Starting from the degree of availability of the protection systems, it is possible to define the reference objectives.	Technical	[28]
Legal Environment and Compliance	Companies in certain industries are obliged to take appropriate technical precautions to protect their infrastructure and must, for example, be certified according to an ISO system.	Social	[28]

The variables chosen for inclusion in the CSRM-SME framework were selected with consideration for the socio-technical system perspective, which looks at both the social and technical aspects of an organization that may affect cybersecurity systems and practices.

The “Degree of responsibility” and the “Legal Environment and Compliance” belong to the social area of the socio-technical model. In particular, the “Degree of Responsibility” variable alludes to the presence of the management of cybersecurity practices, while the “Legal Environment and Compliance” to the legal constraints that drive cybersecurity management. On the other hand, the variables “Technical skills” and “Current availability of protection systems” belong to the technical area of the socio-technical model: the first variable alludes to the availability of technical skills, while the second to the presence of technologies dedicated to IT security.

Table 3 presents the list of questions corresponding to each of the variables. The identification of the questions took place according to the following process. Firstly, we searched in the consultancy models the questions that were compliant with the variables we had identified (listed in Table 2), and we rephrased them in order to increase their clarity in the context of the application of a SME, e.g. removing technical and (or consultancy) jargon. In other words, the questions have been modified to the context of a SME, with the assumption that SME managers may not have an in-depth understanding of cybersecurity and/or digital technologies in general.

Table 3. The detailed content of the CyberSecurity Readiness Model for SMEs

Degree of responsibility (Governance)	**Low**	**Middle**	**High**
Is due diligence, ownership, and effective management of cyber risk demonstrated? [Deloitte]	1 (Absent)	2 (Present but with gaps)	3(Present)
Do we have the right leader and organizational talent? [Deloitte]	1 (Absent)	2 (Present but not suitable)	3 (Present)
How is the effectiveness of our organization's cyber risk program evaluated? [Deloitte]	1 (Absent)	2 (Present but not very effective)	3 (Present and effective)
Have cyber risks and responses been separately incorporated into your crisis management program?	1 (Absent)	2 (incorporated but unsuitable)	3 (Present)
Has the organization implemented a data governance program beyond the basic classification? [EY]	1 (Absent)	2 (Present but lacking)	3 (Present)
How would your workforce describe remote work? [PwC]	Bad (creates discomfort)	Mediocre	Good
Technical skills	**Scarce**	**Mediocre**	**Good**
It is proven through the verification of the successful training on cybersecurity issues every year/at each new entry (direct verification in company documents)	1 (No training)	2 (One-time or incomplete training)	3 (Formation present)
Tangible or intangible product	**Intangible**		**Tangible**
Degree of servitization	**Low**	**Middle**	**High**
Dependence on third parties	**Low**	**Medium**	**Strong**
Is there the presence of outsourcers?	No (0 outsourcer)	Yes	
Is the management of the servers on site or entrusted to a third party?	On site	Entrusted to third parties	
Do you present exclusive contracts with any third party?	No	Yes	
Has your organization conducted a recent third-party cyber risk assessment and/or joint venture? [EY]	1 (Never conducted)	2 (Yes, but not updated every year)	3 (Yes and updated every year)
Current availability of protection systems	**Low**	**Medium**	**Large**
Have you ever suffered attacks?	1 (=0)	2 (>=2 per year)	3 (<2)
Does your cybersecurity feature support cloud migration initiatives? [PwC]	1 (Nope)	2 (Depends)	3 (Yes)
Are cybersecurity and privacy a feature of your products and services? [PwC]	1 (Nope)	2 (Only some products/services)	3 (Yes)
Has your organization conducted a recent enterprise-wide cyber risk assessment? [EY]	1 (Nope)	2 (Yes, but not updated/Scheduled)	3 (Yes)
Legal Environment AND Compliance	**Not in accordance with**	**Compliant but with gaps**	**To standard**
Does your organization handle requests for data subject rights from the customer for data disclosure or deletion? [PwC]	1 (Nope)	2 (Sometimes)	3 (Always)

For the questions, which do not originate from the consultancy models. in the following, we mention the source of each question, and explain the reason underlying their inclusion in the model:

- *“Have cyber risks and responses been separately incorporated into your crisis management program?”*: Consistent with some scholars (e.g., [29]), it is important to question SMEs’ employees regarding their ability to prevent cyber-attacks in line with their crisis management plan/practices.
- *“It is proven through the verification of the successful training on cybersecurity issues every year/at each new entry (direct verification in company documents)”*: This question was deemed crucial because, in the face of th Covid-19 pandemic, the gaps related to training for those people who deal with cybersecurity have emerged even more. Indeed, due to the dearth of existing studies, many companies find it difficult to manage cyber-attacks and train employees on how to prevent them. So, usually, there is a negative relationship between security trainings and the occurrence of cybersecurity incidents [30].
- The questions that fall under the *“Dependence on third parties”* section, are relevant questions that aim to expand on the question posed by EY. In particular, the desire to ask these questions derives from the fact that more and more SMEs managers believe that by relying on third party organizations, they no longer need to question aspects related to cybersecurity [31].
- *“Have you ever suffered attacks?”*: This is an introductory question to the following ones, to enable a better understanding of the profile of the reference company.

3.3 Data Analysis

We followed established “grounded theory” guidelines to ensure rigor in our analysis [32]. Following Glaser and Strauss’s [33] suggestion, our analysis went through numerous iterations to formulate a consistent and coherent story. Following the hermeneutic circle principle to case study development [34], the cases took shape with each iteration cycle. Interview data was fully transcribed and analyzed using NVivo software, following a process of coding and explanation building.

4 Empirical Findings, Discussion, and Implications

Based on the interviews, it was possible to understand the degree of responsibility of the three companies: Company A appeared superficial to the phenomenon of cyber-attacks as it believed it was too small to be of interest to cyberattacks; Company B, on the contrary, while presenting gaps proved to be certain of its IT security as it was entrusted to third parties, while Company C proved to be better prepared in terms of IT security. These ‘SME profiles’ or ‘ideal types’ were developed based on data obtained with respect to ownership, the management of IT risk, training of employees in terms of IT security, and the presence or absence of an internal leader. The development of these ideal types can be seen as reference models for SMEs that want to understand their status in terms of cybersecurity, thus wanting to act to prevent cyber-attacks or manage them in an effective manner. Identifying with certain ideal types will therefore make it easier to understand which strategy to implement.

Company A is characterized by a total unawareness of cyber risk. In addition to not presenting IT security tools, the company identifies itself as ‘too small’ to be a target of cybercrime. The company constitutes the ideal type of what we propose to name as a *dangerously unconscious* organization.

Company B, on the other hand, is confident in its potential in terms of computer security as it relies entirely on a third-party organization to fulfill this aspect. The model illustrates that the company does not actually possess any solidity and internal awareness. In addition, the company’s trust in the third party is such that it does not lead the client company to carry out checks on the IT security of the supplier itself. The ideal type generated by this company can be called *cybersecurity–dependent* on third parties.

Finally, Company C, despite its medium size and its manufacturing nature, proved to be prepared for cyberattacks. Indeed, the company has proven to be in line with the criteria defined by the CSRM-SME model. However, it cannot be considered exempt from cybersecurity risks, having achieved only a medium level in the “availability of protection systems”. The profile generated for this type of company can be termed as a *realist*.

The interviews revealed that the ideal type of SME emerging by the available literature is too simplistic to provide a correct picture of the cybersecurity related issues that SMEs face. The cases investigated in our study suggest that it is essential–in the first place–to differentiate small businesses from medium-sized enterprises, as well as to consider a set of variables whose values lead to delineate at least the three different profiles described above. Figure 2 portraits a graphical representation of both the three identified ideal types and the profile of SME emerging by the literature.

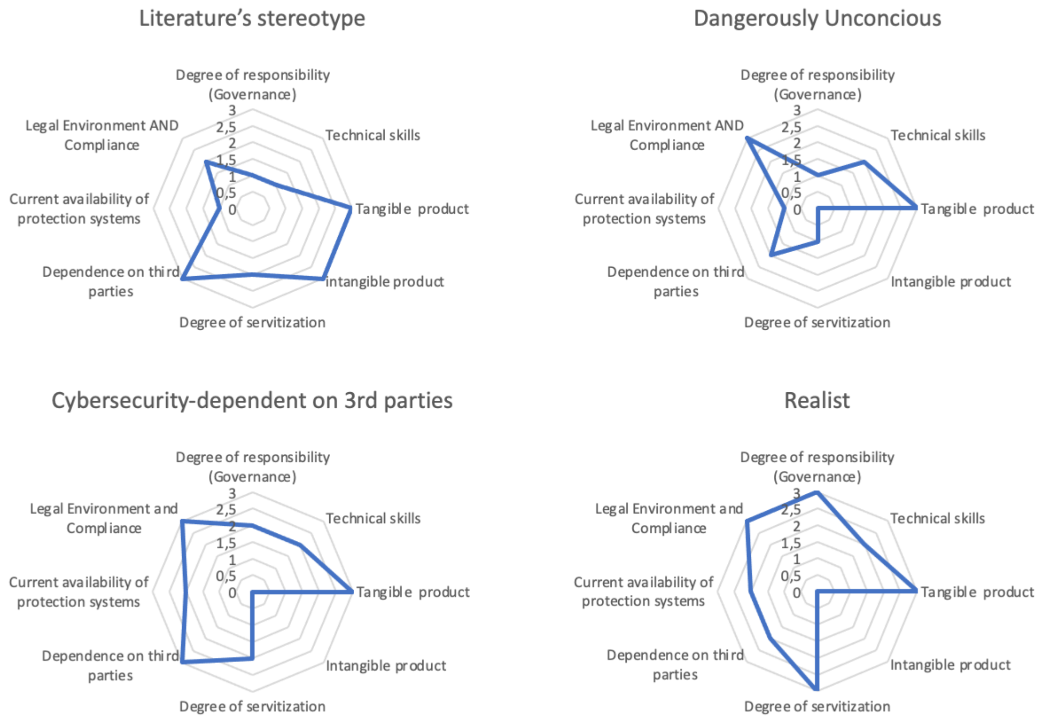

Figure 2. SMEs cybersecurity readiness ideal types

The analysis of the representations makes it possible to deduce other considerations. In particular, it is possible to note how the profiles of the company ‘dangerously unconscious’, that of the company ‘Cybersecurity – dependent on third parties’, and that of the company ‘realist’, appear as an initial type that can evolve into another. This suggests that if a company initially identified itself as *‘dangerously unconscious’*, taking as a reference the *‘Realist’* business reality it could improve to become the latter. It is therefore possible to say that the error of the search lies not so much in the identification of the variables, but more in their use.

It is important to underline that, considering the variables of the CSRM-SME model: ‘Tangible or intangible product’, ‘Third-party dependence’, and ‘Degree of servitization’, cannot be varied over time in the case of cybersecurity as characteristics of the business of each company. Indeed, a manufacturing company will hardly be able to evolve toward a business model focused on the development of intangible products. In other words, improving a company’s cybersecurity does not imply the evolution of the business model from a tangible product to an intangible product. The same reasoning applies to ‘Dependence on third parties’: the fact that a company transfers the management of its data to a third party, does not necessarily imply an improvement in the IT security of the company itself. Even for the 'Degree of servitization', if the company has a low degree of servitization, it does not necessarily result in an improvement in its IT security. All three variables, therefore, as they tend to be stable and intrinsic in the company profile, can be considered useful pivot for identifying an effective business strategy.

By way of example, it is possible to consider the case in which a company presents an intangible product, accompanied by a high degree of servitization and an absence of dependence on third parties. In this case, the advice that could be given to the aforementioned company would be to invest more in the degree of responsibility, technical skills, the availability of protection services, and legal aspects. This advice stems from the fact that the management of IT systems, essential elements for the delivery of business output, will be completely internal. It will therefore be essential that staff possesses the necessary skills, a high degree of responsibility, a high availability of protection systems, and legal compliance.

We can synthesize the above-mentioned discussion by subdividing the variables of the model in three sets: technological, social, and context variables. Technological variables would aggregate *technical skills* (i.e., presence of digital technology skills among the users), and *current availability of protection systems* (i.e., presence of technologies dedicated to CS). The social variables would aggregate the *degree of responsibility* (or governance) (i.e., presence of CS management practices), *dependence on third parties* (i.e., awareness and control of CS management), and *degree of servitization* (i.e., presence and dependency on online activity). The third set is represented by the context variables: *company size* (i.e., availability of financial/managerial resources), *tangible or intangible product* (as a proxy of the dependency of the business on IT), legal environment and compliance (i.e., presence of legal constraints driving CS management).

We can read these aggregations in light of the assessment of the risk related to cyberattacks. Managers can exert their decision-making power over the technical and social variables. By carrying out initiatives to modify the value of these variables, they can reduce the probability that an effective cyberattack could take place. On the contrary, the context variables describe more stable characteristics of the organization, and their values can be modified only in the long term. As such, they represent a proxy for the impact of an effective cyberattack. By combining the assessment of these three variables, it is, therefore, possible to estimate – qualitatively – the degree of risk (in general calculated as the product of probability and impact) of a cyberattack. Figure 3 proposes a graphical representation of the combination of the three sets of variables.

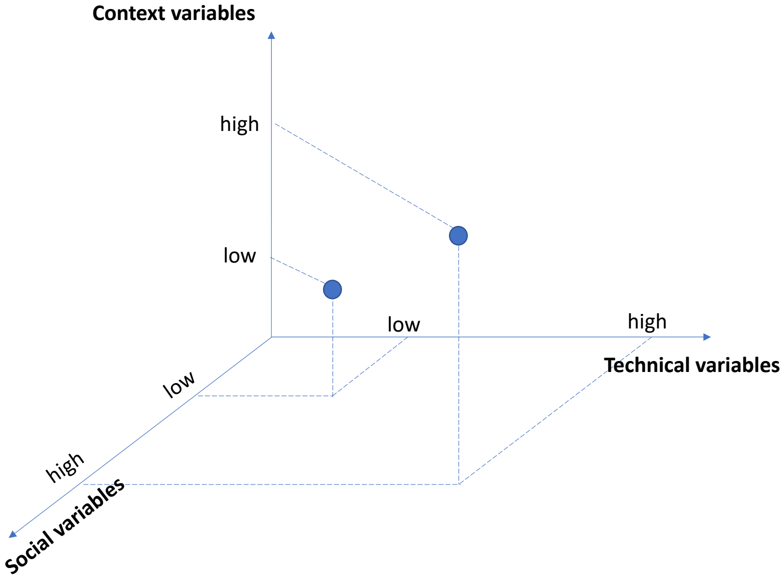

Figure 3. Graphically estimating the risk of a cyberattack using the variables of the model

Limitations: Several limitations need to be considered when interpreting the findings. The empirical study focuses on analyzing three companies belonging to the manufacturing sector via the CSRM-SME proposed. It is important to note that the three cases in question do not in any way summarize all the possible business realities. In addition, the focus on the manufacturing world leads to underline that, if other sectors were taken into account (for instance, agriculture, metalworking, etc.), the conclusions that would be drawn could be different. In addition, it is worth highlighting that the present study takes a snapshot at a precise moment in time. Thus, if a longitudinal analysis was conducted (e.g., pre- and post), it would be possible to observe changes over time.

5 Conclusion

Businesses are becoming more susceptible to cyberattacks as a result of the increasing interconnectedness of the economy and the subsequent digital transformation expedited by the Covid-19 pandemic. SMEs have lagged in their adoption of technology and the security protections necessary to effectively manage their risk. As cybersecurity readiness and awareness is crucial to survival and sustenance of today’s digital environment, SMEs cannot afford to disregard the matter.

This article, which extends the research presented in [35], addresses a gap in the literature that has neglected cybersecurity readiness in SMEs. Based on the shortcomings of the scholarly literature and the main consultancy firms reviewed, and by adopting a socio-technical systems analysis, we propose a model (CSRM-SME) that can be used to evaluate the readiness of SMEs in the context of cybersecurity. This can be used by companies or executives wanting to further understand their contextual environment, and current level of readiness, along with strategies they could adopt to potentially prevent cyber-attacks. Theoretically, we provide support to SMEs by allowing them to understand their company profile and, hence, increase their awareness of techniques that may be used to become more resilient in terms of preventing and managing cyber-attacks.

References

[1] V. Anant, J. Caso, and A. Schwarz, “COVID-19 crisis shifts cybersecurity priorities and budgets,” 2020. Available: https://www.mckinsey.com/business-functions/risk/our-insights/covid-19-crisis-shifts-cybersecurity-priorities-and-budgets

[2] OECD, “The Digital Transformation of SMEs,” 2021. Available: https://www.oecd-ilibrary.org/content/publication/bdb9256a-en

[3] M. Benz and D. Chatterjee, “Calculated risk? A cybersecurity evaluation tool for SMEs,” *Business Horizons*, vol. 63, no. 4, pp. 531–540, 2020. Available: https://doi.org/10.1016/j.bushor.2020.03.010

[4] Allianz, “Allianz Risk Barometer January 2022 Report,” 2022. Available: https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

[5] K. Renaud and J. Ophoff, “A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs,” *Organizational Cybersecurity Journal: Practice, Process and People*, vol. 1, no. 1, pp. 24–46, 2021. Available: https://doi.org/10.1108/OCJ-03-2021-0004

[6] M. R. Galbreth and M. Shor, “The Impact of Malicious Agents on the Enterprise Software Industry,” *MIS Quarterly*, vol. 34, no. 3, pp. 595–612, 2010. Available: https://doi.org/10.2307/25750693

[7] O. Khan and D. A. S. Estay, “Supply chain cyber-resilience: Creating an agenda for future research,” *Technology Innovation Management Review*, vol. 5, no. 4, pp. 6–12, 2015. Available: https://doi.org/10.22215/timreview/885

[8] D. Bhattacharya, “Evolution of Cybersecurity Issues In Small Businesses,” *Proceedings of the 4th Annual ACM Conference on Research in Information Technology*, pp. 11, 2015. Available: https://doi.org/10.1145/2808062.2808063

[9] A. Gupta and R. Hammond, "Information systems security issues and decisions for small businesses," *Information Management & Computer Security*, vol. 13, no. 4, pp. 297–310, 2005. Available: https://doi.org/10.1108/09685220510614425

[10] M. Bada and R. C. Jason, "Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs)," *Information & Computer Security*, vol. 27, no. 3, pp. 393–410, 2019. Available: https://doi.org/10.1108/ICS-07-2018-0080

[11] S. Kabanda, M. Tanner, and C. Kent, "Exploring SME cybersecurity practices in developing countries," *Journal of Organizational Computing and Electronic Commerce*, vol. 28, no. 3, pp. 269–282, 2018. Available: https://doi.org/10.1080/10919392.2018.1484598

[12] J. F. Carías, S. Arrizabalaga, L. Labaka, and J. Hernantes, "Cyber resilience progression model," *Applied Sciences*, vol. 10, no. 21, 2020. Available: https://doi.org/10.3390/app10217393

[13] S. Teufel, B. Teufel, M. Aldabbas, and M. Nguyen, "Cyber Security Canvas for SMEs," *Information and Cyber Security. ISSA 2020. Communications in Computer and Information Science*, Springer, vol. 1339, pp. 20–33, 2020. Available: https://doi.org/10.1007/978-3-030-66039-0_2

[14] T. Tam, A. Rao, and J. Hall, "The good, the bad and the missing: A Narrative review of cyber-security implications for Australian small businesses," *Computers & Security*, vol. 109, 2021. Available: https://doi.org/10.1016/j.cose.2021.102385

[15] T. Tam, A. Rao, and J. Hall, "The Invisible COVID-19 Small Business Risks: Dealing with the Cyber-Security Aftermath," *Digital Government: Research and Practice,* vol. 2, no. 2, pp. 1–8, 2020. Available: https://doi.org/10.1145/3436807

[16] A. P. Paliotta, "Information Security Governance e PMI: analisi critica di un modello di Risk Management," 2020 (in Italian). Available: https://www.ictsecuritymagazine.com/articoli/information-security-governance-e-pmi-analisi-critica-di-un-modello-di-risk-management/

[17] International Trade Administration. "Italy – Cybersecurity," 2022. Available: https://www.trade.gov/country-commercial-guides/italy-cybersecurity#:~:text=In2021%2Cthecybersecuritymarket,increasinglytargetedbyransomwareattacks

[18] M. R. Bozzetti, L. Olivieri, and F. Spoto, "Cybersecurity Impacts of the Covid-19 Pandemic in Italy," *5th Italian Conference on Cybersecurity, ITASEC 2021*, pp. 145–155, 2021.

[19] S. Armenia, M. Angelini, F. Nonino, G. Palombi, and M. F. Schlitzer, "A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs," *Decision Support Systems*, vol. 147, 2021. Available: https://doi.org/10.1016/j.dss.2021.113580

[20] M.-E. Paté, P. Paté-Cornell, M. Kuypers, M. Smith, and P. Keller, "Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model and Three Case Studies," *Risk Analysis*, vol. 38, no. 2, 2018. Available: https://doi.org/10.1111/risa.12844

[21] D. L. Nazareth and J. Choi, "A system dynamics model for information security management," *Information and Management*, vol. 52, no. 1, pp.123–134, 2015. Available: https://doi.org/10.1016/j.im.2014.10.009

[22] M. R. Kamm, C. Wehking, L. F. Kaiser, M. Otto, and J. V. Brocke, "Approaching Digitalization at an SME Manufacturing Service Provider," *Management for Professionals*, vol. 2, pp. 271–287, 2021. Available: https://doi.org/10.1007/978-3-030-80003-1_14

[23] R. P. Bostrom and J. S. Heinen, "MIS Problems and Failures: A Socio-Technical Perspective. Part I: The Causes," *MIS Quarterly*, vol. 1, no. 3, pp. 17–32, 1977. Available: https://doi.org/10.2307/248710

[24] S. Alter, "Sociotechnical Systems through a Work System Lens: A Possible Path for Reconciling System Conceptualizations, Business Realities, and Humanist Values in IS Development," *Proceedings of the STPIS 2015 (1st International Workshop on Socio-Technical Perspective in IS Development) associated with CAISE 2015, Business Analytics and Information Systems*, pp. 1–15, 2015.

[25] S. Alter, "The Work System Method: Systems Thinking for Business Professionals," *Proceedings of the 2012 Industrial and Systems Engineering Research Conference, Business Analytics and Information Systems*, Paper 32, 2012.

[26] J. W. Creswell, *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. 3rd Edition, Sage Publications, 2013.

[27] R. K. Yin, *Case study research: Design and methods*. Sage publications, 2013.

[28] C. Pugnetti and C. Casián, “Cyber risks and Swiss SMEs: an investigation of employee attitudes and behavioral vulnerabilities”, 2021. Available: https://doi.org/10.21256/zhaw-21478

[29] P. Hong, C. Huang, and B. Li, “Crisis management for SMEs: Insights from a multiple-case study,” *International Journal of Business Excellence*, vol. 5, no. 5, pp. 535–553, 2012. Available: https://doi.org/10.1504/IJBEX.2012.048802

[30] E. Kweon, H. Lee, S. Chai, and K. Yoo, “The Utility of Information Security Training and Education on Cybersecurity Incidents: An Empirical Evidence,” *Information Systems Frontiers*, vol. 23, no. 2, pp. 361–373, 2021. Available: https://doi.org/10.1007/s10796-019-09977-z

[31] M. Zec and M. Kajtazi, “Cyber security Measures in SMEs: a study of IT professionals’ organizational cyber security awareness,” 2015.

[32] J. Corbin and A. Strauss, “Grounded theory research: Procedures, canons, and evaluative criteria,” *Qual Sociol*, vol. 13, no. 1, pp. 3–21, 1990. Available: https://doi.org/10.1007/BF00988593

[33] B. Glaser and A. Strauss, *The Discovery of Grounded Theory*. Routledge, 2017. Available: https://doi.org/10.4324/9780203793206

[34] H. K. Klein and M. D. Myers, “A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems,” *MIS Quarterly,* vol. 23, no. 1, pp. 67–93, 1999. Available: https://doi.org/10.2307/249410

[35] H. Perozzo, A. Ravarini, and F. Zaghloul, “Assessing Cybersecurity Readiness within SMEs: Proposal of a Socio-Technical based Model,” *Proceedings of the 8th International Workshop on Socio-Technical Perspective in Information Systems Development (STPIS 2022),* Ceur-ws.org, vol. 3239, pp. 22–32, 2022.