# Assessing Cybersecurity Readiness within SMEs: Proposal of a Socio-Technical based Model

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

[1] *Università C. Cattaneo – LIUC, Italy*
[2] *University of Southampton, Southampton Business School, UK*

**Abstract**

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

**Keywords**

Cyber Security, Socio-technical system, Readiness model, Small and medium-sized enterprise, SMEs

## 1. Introduction

Advances in interconnectivity, devices, and digital technologies have benefitted organizations in numerous ways, including reduced operating costs, increased speed of communication, efficiency, and system accessibility. Nevertheless, organizations undergoing digital transformation, accelerated by the Covid-19 pandemic, continue to face the risk of cyber-attacks and threats [1], resulting in significant losses for companies, not just financially but also in terms of valuable information [2]. Therefore, studies on the threats of cyber-attacks have moved towards a landscape that aims at the prevention of the same [4].

It used to be a common thought that large companies are more vulnerable to cyber-attacks than small and medium sized enterprises (SMEs) [5]. On the contrary, while the rise in cybercrime is evident across businesses of all sizes, one particular group that is increasingly being targeted is SMEs [6]. The reality is that, in the face of the inauguration of the so-called new digital age caused by Covid-19 [7], SMEs need urgent support in order to reduce or mitigate the risk associated with their vulnerability.

Italy is shaped by a large number of SMEs. Recently, it has been one of Europe's top targets for cyber-attacks. The number of cases, and the severity of these incidents, have increased in the past few years. For example, 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 argued that if cybersecurity readiness is absent or low, it will be challenging for businesses to acquire the necessary resources to achieve an appropriate level of cybersecurity to protect its digital assets.

Unlike large-size organizations, SMEs typically suffer owing to a lack of knowledge, skills, and resources [8,9]. The current status of cybersecurity preparedness and maturity of SMEs, contrary to popular opinion, can be extremely low. These organizations seldom conduct a comprehensive cyber-risk assessment, and their IT and business leadership teams are frequently at odds when it comes to

8th International Workshop on Socio-Technical Perspective in IS development (STPIS 2022), 19-21 August, 2022, Reykjavík, Iceland
EMAIL: ha01.perozzo@stud.liuc.it (Haiat Perozzo); aravarini@liuc.it (Aurelio Ravarini); fatema.zaghloul@soton.ac.uk (Fatema Zaghloul)
ORCID: 0000-0002-3114-9727 (A Ravarini); 0000-0002-8626-807X (F Zaghloul)


cybersecurity risk management. With limited IT teams and insufficient security expenditures, SMEs are often at a disadvantage when it comes to dealing with cyber-attacks [10].

Despite the significance of cybersecurity readiness, and given the fact that SMEs play a significant role in the Italian economy (e.g. viewed as vehicles for job development and employment), current research focusing on SMEs is scarce [11]. This paper presents research-in-progress. We present a review of the existing models aimed at assessing the adequacy of a cybersecurity system (CSS), or – more precisely – the readiness of an organization to face a cyberattack. We review both the scholarly and practitioner literatures and highlight their weaknesses. Based on this, and via adopting the lens of a Socio-Technical System (STS) approach, we propose a new model, the Cyber Security Readiness Model (CSRM), and apply it to three SMEs in the manufacturing sector in Italy.

## 2. Literature Review

### 2.1 Cybersecurity readiness models developed by consultancy firms

Cybersecurity has always been an important issue. Being a complex reality that evolves in symbiosis with digitization, every year consultancy firms, researchers and analysts take action to propose advice and models useful for managing the world of computer security [9]. In particular, Covid-19 and the consequent massive adoption of digital technologies has made even more evident the characteristic lag of SMEs in adopting of IT security resources and policies. Despite this emergency situation for SMEs, it is interesting to note that the majority of the models in this field has been dedicated to, and designed for, large companies. Only recently they have been readjusted in the attempt to adapt them to the application in SMEs.

The current literature already appears to trace the profile of SMEs affected by cyber-attacks. Following a survey involving 310 companies from different sectors, it was possible to note that the companies that received a larger volume of attacks are those of services and manufacturing [12]. Since the first wave of COVID-19, the literature also states that the degree of responsibility is low. This stems from a belief that since these are small businesses, they are not attractive targets for cyber-attacks [13]. With regard to technical skills, among the causes of the increased exposure of small businesses are factors ranging from the inexperience of small businesses with technology to the global skills shortage in cybersecurity [14,15]. In addition, dependence on third parties is proving to be high after COVID – 19, due to an increase in the outsourcing of processes related to cybersecurity [16]. The literature argues that the availability of protection systems is low [17]. Finally, empirical research does not seem in any way to be unbalanced about legal issues.

The biggest consultancy firms worldwide (Deloitte, PwC, EY and McKinsey), have developed models to help organizations assess their exposure to the risk of cyberattacks. Such models consist of structured sets of questions that deal with the issues that are perceived as more relevant and pertinent. Our analysis shows that - although the structures of these models are slightly different - the main concepts and issues explored remain the same: they all focus on the following fundamental questions:

- "Have you developed an IT System Layer or an application map that allows you to view all the applications involved?";
- "Does your organization periodically conduct penetration tests?";
- "How does the organization act in the face of phishing attacks?".

### 2.2 Cybersecurity readiness models for SMEs in the academic literature

Reviewing the scholarly literature reveals three main readiness models for SMEs: Cyber Security Canvas [13]; SMECRA [18]; and Listemann's model [19].

Firstly, 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 manufacturing SMEs that, for example, 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 levels, and in this case we will focus on the first layer as it is dedicated to the prevention of cyber-

attacks. Indeed, the first level is about prevention and internal evaluation. It is no coincidence that the starting objective of the entire framework is the definition of the company's security objectives, not only with regard to information security and the IT security strategy, but also with regard to individual orientation and available resources (budget). The next step is to analyze whether the company has the internal know-how necessary for the implementation of the set objectives. The sub-objectives must be specifically distributed to the different employees so that everyone knows their role and responsibilities.

Secondly, SMECRA [18] is a tool that, first, analyzes the *cyber-postures* of an SME, and then simulates the effect of different investment strategies. The model provides for an evaluation of a qualitative nature, that can then be translated into quantitative evaluations. SMECRA has been developed considering a generic context of SMEs. Some questions that make up the SMECRA model are for example: "Third-party web services (social network, cloud computing, email, web hosting, etc.) are only used when strictly necessary", "Protection sosftware (antivirus, anti-malware, etc.) is installed wherever possible "," Password are adequately complex and different for every account ".

Finally, Listemann's model [19] is a model that has been used to support Listemann's SME, with a path towards greater digitalization. This model allows us to understand how the company needs support in terms of cybersecurity since it is involved in a constantly evolving process towards digitization. The model illustrates the potential deriving from digitization in the case of Listemann. In particular, among these there are for example:

- 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 SMBs 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.

## 2.3 Applying the STS model to cybersecurity readiness models

According to Bostrom & Heinen [20], an organization can be represented as a socio-technical system, as shown in Figure 1. The STS 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 STS system will maximize performance only if the interdependence of these subsystems is explicitly recognized [20].

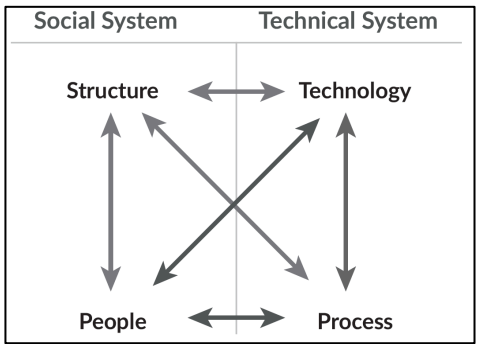


**Figure 1**: Socio-Technical system framework [20]

Confronted with this framework, all the models reviewed in sections 2.1 and 2.2 show a prevalent focus on the technical component, despite their claims of placing human resources at the center of the attention.

In particular, the models proposed by the consultancy firms simply do not address the social sub-system component, because they do not include the assessment of the implications on cybersecurity of the characteristics of the people and the structure of the organization.

Regarding the models available in the scholarly literature, they have limitations that can be explained through the socio-technical model too. 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.

The presence of technical models, in particular, could prove to be a problem especially if models proposed by the leading consultancy firms and the scholarly literature are to be made available to SMEs. Indeed, faced with too technical questions, SMEs could answer in a negative way, the negativity of which, however, could be synonymous with a notional gap and not with the actual absence of the element reported in the question. This makes it clear that the proposed models may therefore not be suitable for all SMEs.

Despite this, there are still difficulties in finding a convergence between the different sources. In particular, this paper takes into consideration two categories of resources: non-academic and academic. Reviewing these have revealed that the former are less affordable in terms of conclusions but more reliable in terms of the instant in time considered, they are more up-to-date; the latter, on the other hand, are more affordable in terms of the thesis they offer, but less reliable in terms of updating information.

This conclusion allows us to affirm again that it is important to be able to find the right trade-off between the social part and the technical part that are characteristic of the socio-technical model. In particular, faced with the presence of these gaps observed in the discussion above could potentially cause damage to SMEs. Indeed, if SMEs used the models described above, they will certainly be able to bridge the gaps from a technical point of view, but the whole part linked to the organization and people would remain fragile. However, according to the socio-technical model, all the characteristic variables of the model are interdependent and precisely because of this interdependence they influence each other. Therefore the fragility of the variables linked to the social part weakens the strength of the technical part.

## 2.4 Research Question

Based on the discussion presented above, this study addresses the following research question: *what are the variables that help estimating cybersecurity readiness in a small-medium size organization*?

In the attempt to answer this research question, this study aims on the one hand, at overcoming the limitations of the previous technology-centric models available in the literature, and - on the other – at taking into account the cybersecurity issues arisen in recent times, during the pandemic. In fact, SMEs have experienced a significant evolution towards digitization following the advent of Covid-19, and this acceleration, paired with the limited resources and competences of SMEs, has increased the risk of effective cyberattacks.

# 3. Research Method

In order to come up to an answer to the research question, we identified a set of relevant (in the above-mentioned context) variables that we applied as part of a data collection protocol in a multiple case study. The overall set of these variables, represent in fact a possible model for assessing the readiness of SME to face cybersecurity. In this section we explain the logic we followed in designing this methodological approach.

A qualitative research approach was deemed most appropriate as researchers are able to "understand those being studied from their perspective" [21, p.23], and hence understand the phenomenon from the perspective of the SME. Indeed, they are "designed to help researchers understand people and the social and cultural contexts within which they live" [22].

This study uses semi-structured interviews with companies belonging to the manufacturing sector, in which questions are prepared ahead of time but not strictly followed during the interview [23]. Despite the fact that semi-structured interviews have a series of pre-determined questions, they normally unfold in a way that allows interviewers to dig deeper into or discuss themes they consider as essential or require further attention [24,25].

As to the methodology for the empirical investigation, this study makes use of the 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, p.97]. 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, p.13] and seek an in-depth understanding.

According to Stake [28], it is important to concentrate "on each single case almost as if it is the only one" and that multiple case studies should be investigated "one case at a time" (p.1). Therefore, our analysis involves developing a case report for each case study, followed by a cross-case analysis.

The data collection protocol was designed on the basis of the existing cybersecurity readiness models and on the attempt to overcome their limitations, as discussed in section 2. The variables that constitute such models have been partially included in the data collection protocol, and a few other variables have been added, as suggested by the literature review. The resulting set of variables represents a model to assess the ability of an SME to prevent cyber-attacks: the Cyber Security Readiness Model for SMEs (CSRM).

CSRM consists of eight variables (shown in Table 1) that can be assessed through a set of questions (detailed in Table 2).

**Table 1**

The structure of the proposed Cyber Security Readiness Model for SMEs

| VARIABLE | MOTIVATION | REFERENCES |
|---|---|---|
| **Company size** | Depending on the size of the company there will be a different economic and resource availability | Teufel, et al., 2020 |
| **Degree of responsibility (Governance)** | The greater the degree of responsibility possessed in the face of cyber security issues, and therefore the more suitable the leader in this sense, the greater the company's awareness of the importance of computer protection | Tam, 2020 |
| **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 | Tam, 2020 |
| **Tangible or intangible product** | The presence of a tangible product means less need for computer systems, rather than intangible ones | Bozzetti et al., 2021 |
| **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 | Bozzetti et al., 2021 |
| **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 himself | Tzu, 2020 |
| **Current availability of protection systems** | Starting from the degree of availability of the protection systems, it is possible to define the reference objectives | Pugnetti & Casián , 2021 |
| **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. | Pugnetti & Casián, 2021 |

The questions were derived partly from the academic models and partly from the models proposed by consultancy firms.

The choice of the variables to be included in the model (i.e., in the empirical investigation) followed the principle of the socio-technical perspective: to take into account both the social and the technical components of the organization that can have an impact on cybersecurity systems and practices. Moreover, the formulation of the questions have been adapted to the context of an SME, with the assumption that SMEs managers may not have a deep knowledge in the field of cybersecurity, and in digital technology in general.

Table 2 shows the detailed list of the 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 1), and we rephrased them in order to increase their clarity in the context of application of an SME, e.g. removing technical and (or consultancy) jargon.

In Table 2 these questions can be identified by the name of the consulting firm whose cybersecurity readiness model they belong to. All the other questions, on the contrary, were found in the academic literature. In the following paragraphs we mention the source of each question, and we explain the reason why it has been included 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 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 is very important because, in the face of the 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 to train employees on how to prevent them. So, usually, there is a negative relationship between security trainings and the occurrence of cybersecurity incidents [30].
- As regards the questions that fall under the "*Dependence on third parties*" section, these 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 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 be able to better understand the profile of the reference company.

**Table 2**
The detailed content of the Cyber Security 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** | **Media** | **Loud** |
| 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** | **Media** | **Loud** |
| 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) |
| Is 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) |

The perimeter of the project includes three different SMEs operating in the manufacturing sector. More precisely, these are three companies characterized by three different dimensions, three different approaches to security and consequently three different types of awareness related to the latter. Especially:

1. The first company (Company A) deals purely with designing and producing technical articles in rubber and silicone;
2. The second company (Company B), on the other hand, is used in the design and construction of a complete range of machinery for the paper industry, bookbinding and box factories**;**
3. The last company (Company C) deals with the processing of marble.

## 4. Empirical Research Preliminary Findings

Following the interviews conducted using the CSRM model, it was possible to obtain a series of interesting data. The interviews aimed at the three companies in question saw the involvement of

subjects belonging to different business functions, thus also allowing to detect the *gap* between the staff directly in contact in the IT field and those who are far from it (but may indirectly be affected).

Referring to the variables identified for the development of the model, the three companies interviewed were analyzed starting from the identification of the number of employees. From this, it was revealed that the three companies were of different sizes: the first company was very small, the second small-medium-sized and the third medium-sized. Secondly, it was necessary to understand whether companies had a business oriented more towards tangible or intangible products, and whether these were enriched by the presence of services or not.

In total, 4 interviews were conducted: for the first company the general manager presented himself, for the second company the managing director and the IT administrator of the IT service provider, the third company was the production manager. Based on the responses obtained, 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 malicious people, company B on the contrary while presenting gaps proved to be sure 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 three different profiles were born in the face of a different due diligence, ownership, effective management of IT risk, training of employees in terms of IT security and the presence or absence of an internal leader.

## 5. Discussion and implications

Following the interviews conducted, it was possible to observe whether the stereotypes of SMEs defined by the research are also found. As shown in the previous section, the three companies outlined three different stereotypes (or profiles) of SMEs. The generation of the latter constitutes reference models for all those SMEs that want to understand their status in terms of cybersecurity, thus wanting to act to prevent cyber-attacks. Identifying with certain stereotypes 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 stereotype of what we propose to name 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 fulfil 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 stereotype 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 cyber-attacks. Indeed, the company has proven to be in line with the criteria defined by the CSRM 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 *realist*.

The interviews revealed that the stereotype 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 stereotypes and the profile of SME emerging by the literature.

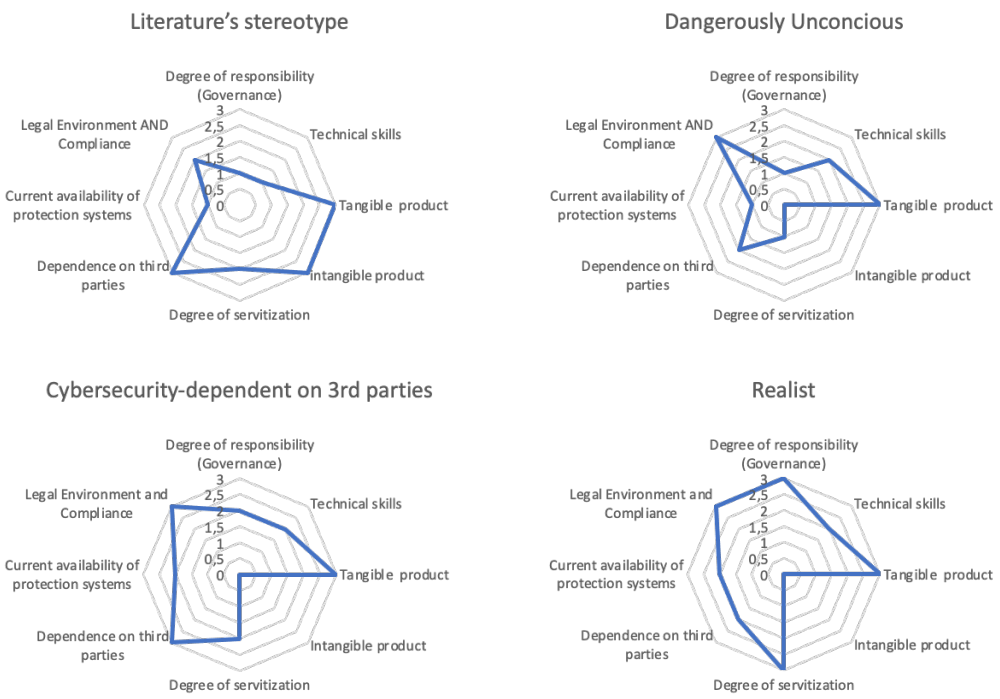


**Figure 2**: SME's cybersecurity readiness stereotypes

The graphical representations of the Literature's stereotype shows that the academic literature considers as "standard" those company that have a profile with intermediate characteristics with respect to the profiles of the companies interviewed during our study.

The analysis of the graphs makes it possible to deduce other considerations. In particular, it is possible to note how the profile 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 model: 'Tangible or intangible product', 'Third-party dependence' and 'Degree of servitization', these 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 towards 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, this 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, for example, not necessarily increasing the latter the expected result is the improvement of computer security. All three variables, therefore, as they tend to be stable and intrinsic in the company profile, can be considered the useful pivot for identifying the correct 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, in technical skills, in the availability of protection services and in 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 possess the necessary? skills, a high degree of responsibility, a high availability of protection systems and the legal part in accordance with the law.

The recommendations will therefore vary depending on these variables that are more related to the business world.

# 6. Conclusions

## 6.1 Contribution

Cybersecurity is a threat to a business' reputation, operations, and finance. COVID-19 has accelerated the adoption of digital technology, providing hackers greater opportunity to launch cyber-attacks. This paper addresses a gap in the literature that has neglected cybersecurity readiness in SMEs. The research findings have both practical and theoretical implications. Based on the shortcomings of the scholarly literature and the main consultancy firms analyzed, we propose a model (CSRM) that can be used to evaluate the readiness of SMEs in the context of cybersecurity. This can be used by companies wanting to further understand their contextual environment along with strategies they could adopt to potentially prevent cyber-attacks. Theoretically, we add support to SMEs for the presence of standard company profiles that allow interested companies to raise their awareness regarding the strategies that could be adopted to become more robust in terms of preventing cyber-attacks. In particular, by taking into consideration the socio-technical model, this robustness is due to the guaranteed balance between the social and technical parts.

## 6.2 Limitations and Future Developments

The present paper focuses on analyzing three companies belonging to the manufacturing sector via the CSRM developed in this study. The preliminary findings are based on four interviews, which will be extended upon to further explore and validate the emerging themes through additional semi-structured interviews with key participants.

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 example agriculture, metalworking, etc.), the conclusions that would be drawn could be different. It is important to highlight that the present project takes a snapshot in a precise moment in time. Thus, if a longitudinal analysis was conducted (e.g. pre- and post), it would be possible to observe changes overtime.

# 7. References


[1] Anant, V., Caso, J., & Schwarz, A. (2020). COVID-19 crisis shifts cybersecurity priorities and budgets. *Pridobljeno iz McKinsey & Company: https://www. mckinsey. com/business-functions/risk/our-insights/covid-19-crisis-shifts-cybersecurity-priorities-and-budgets*.

[2] Galbreth, M. R., & Shor, M. (2010). The impact of malicious agents on the enterprise software industry. *Mis Quarterly*, pp. 595-612.

[3] Pisanu, N., (2021). Attacchi cyber emergenza globale, ci costano il 6% del PIL: i dati del rapporto Clusit 2021. Online. [Available from: https://www.cybersecurity360.it/nuove-minacce/attacchi-cyber-emergenza-globale-ci-costano-il-6-del-pil-i-dati-del-rapporto-clusit-2021/]

[4] Khan, O., & Estay, D. A. S. (2015). Supply chain cyber-resilience: Creating an agenda for future research. *Technology Innovation Management Review*, *5*(4).

[5] Bhattacharya, D. (2015). Evolution of cybersecurity issues in small businesses. In *Proceedings of the 4th Annual ACM Conference on Research in Information Technology* (pp. 11-11).

[6] Gupta, A., & Hammond, R. (2005). Information systems security issues and decisions for small businesses: An empirical examination. *Information management & computer security*.

[7] Amankwah-Amoah, J., Khan, Z., Wood, G., & Knight, G. (2021). COVID-19 and digitalization: The great acceleration. *Journal of Business Research*, *136*, 602-611.

[8] Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security*.

[9] Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*, *63*(4), 531-540.
[10] Howard, L. S. (2018). SMEs underestimate cyber risks which could prove 'fatal': Allianz report. *Insurance Journal*.
[11] Kabanda, S., Tanner, M., & Kent, C. (2018). Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, *28*(3), 269-282.
[12] Bozzetti, M. R., Olivieri, L., & Spoto, F. (2021). Cybersecurity Impacts of the Covid-19 Pandemic in Italy. In *5th Italian Conference on Cybersecurity, ITASEC 2021* (pp. 145-155).
[13] Teufel, S., Teufel, B., Aldabbas, M., & Nguyen, M. (2020). Cyber security canvas for SMEs. In *International Information Security Conference* (pp. 20-33). Springer, Cham.
[14] Tam, T., Rao, A., & Hall, J. (2020). The invisible COVID-19 small business risks: Dealing with the cyber-security aftermath. *Digital Government: Research and Practice*, *2*(2), 1-8.
[15] Tam, T., Rao, A., & Hall, J. (2021). The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses. *Computers & Security*, *109*, 102385.
[16] Paliotta, A.P., (2020). Information Security Governance e PMI: analisi critica di un modello di Risk Management. Online. [Available from: https://www.ictsecuritymagazine.com/articoli/information-security-governance-e-pmi-analisi-critica-di-un-modello-di-risk-management/]
[17] Pugnetti, C., & Casián, C. (2021). Cyber risks and Swiss SMEs: an investigation of employee attitudes and behavioral vulnerabilities.
[18] Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems*, *147*, 113580.
[19] Kamm, M. R., Wehking, C., Kaiser, L. F., Otto, M., & Brocke, J. V. (2021). Approaching Digitalization at an SME Manufacturing Service Provider. In *Digitalization Cases Vol. 2* (pp. 271-287). Springer, Cham
[20] Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: A socio-technical perspective. Part I: The causes. *MIS quarterly*, 17-32.
[21] Gorman, G. E., and Clayton, P., (1997). *Qualitative research for the information professional: A practical handbook*. London: Facet Publishing
[22] Myers, M. D., (1997). Qualitative research in information systems. *Management Information Systems Quarterly*, 21 (**2**), pp. 241-242
[23] Patton, M. Q. (1990). *Qualitative evaluation and research methods*. SAGE Publications, inc.
[24] Cassell, C., & Symon, G. (Eds.). (2004). *Essential guide to qualitative methods in organizational research*. sage.
[25] Saunders, M., Lewis, P., and Thornhill, A., (2015). *Research Methods for Business Students*, 7th edition, Harlow: Pearson
[26] Creswell, J. W., (2013). *Qualitative inquiry and research design: choosing among five traditions*. 3rd Edition, Thousand Oaks CA, Sage Publications
[27] Yin, R. K., (2013). *Case study research: Design and methods*. Sage publications
[28] Stake, R. E., (2006). *Qualitative Case Studies*. The Sage Handbook of Qualitative Research, Third Edition, Sage Publications, London (pp. 443-466)
[29] Hong, P., Huang, C., & Li, B. (2012). Crisis management for SMEs: insights from a multiple-case study. *International Journal of Business Excellence*, 5(5), 535-553.
[30] Kweon, E., Lee, H., Chai, S., & Yoo, K. (2021). The utility of information security training and education on cybersecurity incidents: an empirical evidence. *Information Systems Frontiers*, *23*(2), 361-373.
[31] Zec, M. (2015). Cyber security Measures in SME's: a study of IT professionals' organizational cyber security awareness. Linnaeus University, Kalmar.