Cyber Resilience Strategic Planning and Self-assessment Tool for Operationalization in SMEs

Juan Francisco Carias, Saioa Arrizabalaga, Josune Hernantes

Cyber Resilience Strategic Planning and Self-Assessment Tool for Operationalization in SMEs

Juan Francisco Carias[1], Saioa Arrizabalaga[1,2] and Josune Hernantes[1]

[1] University of Navarra, TECNUN, School of Engineering, San Sebastian, Spain
2 CEIT-BRTA, San Sebastian, Spain
jfcarias@tecnun.es

Abstract. With the current high risks of cyber incidents either caused by malicious cyber criminals or by accidents, there is a latent need for cyber resilience. This discipline is a broader than the traditional cybersecurity concept as it aims to give companies an adaptability such that they are "safe-to-fail", i.e. that companies are capable of facing cyber incidents and still continue their operations or recover quickly. Although cyber resilience is a desirable capability in companies it is not easy to operationalize because it requires knowledge, experience, strategic planning and decision-making capabilities. These characteristics are not easily found in companies starting their cyber resilience building process such as SMEs. Moreover, the current literature offers documents to aid in the operationalization of cyber resilience by giving companies several actions or policies that build cyber resilience, but the information on how to strategize an effective cyber resilience building process is often scarce. Therefore, this article proposes a strategic planning and self-assessment tool to aid companies in the strategic planning of cyber resilience building. This tool contains the most important cyber resilience policies for SMEs and natural progressions for them obtained from the experience of 11 experts. With these progressions companies can obtain insights on what is their current state in each policy and what actions they can perform in order to improve that state. Thus, the tool can be helpful to develop effective action plans for cyber resilience building.

Keywords: Cyber Resilience; Strategic Planning; Self-Assessment Tool.

1 Introduction

Cyber incidents can be very costly for companies. Some studies estimate that the average annual cost per company is around the millions of euros [1]. This large costs are unsustainable for many companies and especially the smaller ones [2]. Although many Small and Medium-sized Enterprises (SMEs) disregard the possibility of being attacked. However, studies suggest that they are the most vulnerable because, as a group, they represent a high payload to the attackers [3]. Cyber incidents can have various causes, malicious or accidental, natural or caused by humans [4, 5]. Regardless, when the performance of the company's systems is compromised the company will suffer

losses. Therefore, disaster management is undoubtedly necessary in the field of cybersecurity.

Cybersecurity, however, as traditionally defined, does not usually consider the response and recovery after an incident [6]. For this reason, many experts have shifted towards a broader concept of cyber resilience [7-9]. This concept is considered to be the ability of a company to anticipate, detect, withstand, recover and evolve in order to improve their capability of facing adverse situations [10. 11]. Moreover, this concept is also broader in the sense that it requires strategic planning, definition of organizational processes, and more human involvement [8, 9] when traditional cybersecurity usually focused on technical solutions with minimum human interaction [6, 12].

Cyber resilience can be a potential solution to the dangerous cyber scenario in which companies live today. Once operationalized, cyber resilience is meant to make companies safe-to-fail [4]. In other words, cyber resilience intends to make companies flexible, adaptable, ready to face challenges and recover, learn from them and thrive. However, cyber resilience is prudential, not technical, making it difficult to operationalize by requiring strategic-level planning and decision-making which in turn require knowledge and experience in the field.

Although there are several tools meant to aid companies in the operationalization of cyber resilience (e.g. [7, 9, 13]), these tools are often extensive lists of policies, actions and/or metrics with virtually no guidelines on how to prioritize these policies, actions or metrics. Thus, these tools are designed for companies who already have the experience, knowledge, maturity and capacity to manage cyber resilience on their own by prioritizing these policies and strategizing their own cyber resilience building process. However, SMEs usually lack these characteristics due to low access to resources (specialized personnel, investment capability, tools, etc.). Therefore, companies like SMEs with scarce experience and prudential capabilities for decision-making in this field require tools to facilitate their strategic planning to effectively operationalize cyber resilience.

Thus, the purpose of this article is to propose a strategic planning and self-assessment tool in order to aid SMEs in the prioritization and strategy development. The developed tool permits target setting, and action plan development based on the natural progression of 33 policies identified as the most important for cyber resilience management in SMEs, therefore aiding companies in their strategy development process.

This article is structured in the following manner: section 2 contains a brief literature review on current tools for aiding companies in their cyber resilience building. Section 3 describes the methodology used to develop the self-assessment and strategic planning tool. Section 4 explains the results of this study. Section 5 contains a discussion on how the results can aid companies, how to use these results and the limitations of this study. Finally, section 6 contains the conclusions drawn from this study.

2 Literature Review

There is a plethora of tools in the literature that intend to aid companies in their cyber resilience building. Frameworks are one example of these tools that have proliferated

and that often include domains and policies to guide companies on what is needed in order to operationalize cyber resilience [7, 9, 13-15]. These frameworks are widely varied, containing from 4 domains [9, 16] into having over 30 of them [13]. There are similarities between some of these frameworks, but often they are not completely equivalent to each other on a policy to policy level or even a domain to domain level.

Similar to frameworks, there are standards that define actions and processes needed to achieve cyber resilience capabilities [17, 18]. These standards can have more strategic insight than frameworks [17], but are also extensive documents without roadmaps on where to start the cyber resilience building process nor how to progress.

On the other hand, there are several documents with cyber resilience Key Performance Indicators (KPIs) [19-22] meant to help companies control and optimize their cyber resilience by using these measurable characteristics of cyber resilience. However, these KPIs often limit to measuring technical capabilities[22] which may not cover all the strategic and human ins and outs in cyber resilience [8].

All of these previously mentioned tools (frameworks, standards and KPIs) often recommend the customization of the tool to adapt it to the company's circumstances and priorities [13, 18, 22]. The indication to customize these tools is reasonable since there is no "one-size-fits-all" solution to the operationalization of a prudential capability such as cyber resilience [13]. However, none of these tools gives insight on how to do this customization or how to prioritize their policies or KPIs. Therefore, these tools require the knowledge and experience to be able to customize them and make decisions in order to build cyber resilience through their usage.

Other tools available for companies to aid in their cyber resilience building process are maturity models [23, 24]. These can be defined as sets of characteristics that define a development in a certain field put sequentially in a limited number of stages or levels [25, 26]. Maturity models are often used to assess the current state of cyber resilience in an entity [10, 27] and due to their nature they are meant to aid companies progress after the initial assessment. However, the current literature only offers capability maturity models, which by nature are meant to describe already implemented processes and more specifically assess how ingrained these processes are in the company's culture [25]. Therefore, these tools can also require experience and an already begun cyber resilience operationalization in order to be fully used by companies since the descriptions of the maturity stages may not be relatable to a company that is at the beginning stages of the operationalization.

Another type of maturity model, the progression models, are descriptions of natural progressions of characteristics, attributes or policies over time from their most basic form into their most complex form sequentially and in a limited number of stages [25]. These type of maturity models are not currently a part of the cyber resilience literature. However, a cyber resilience progression with the natural progression for the different policies would be easier for companies starting their cyber resilience building process to relate to than the evolution of processes and capabilities which they have yet to implement. Therefore, this type of model would be a good tool to better assess the cyber resilience state of the companies and at the same time would give these companies insight on the natural progression that the policies should follow once they implement

them. The usage of these advantages of progression models could help address the current scarcity of resources towards aiding in the strategic management of cyber resilience in companies starting their cyber resilience operationalization.

3 Methodology

The methodology for this article can be explained in three main phases:

1. Development of a cyber resilience framework for SMEs.
2. Development of a progression model for each policy in the framework.
3. Development of the strategic planning and self-assessment tool based on the progression model.

These phases will be explained more in depth in the following subsections and a summary is of the methodology and its phases is shown in Fig. 1.

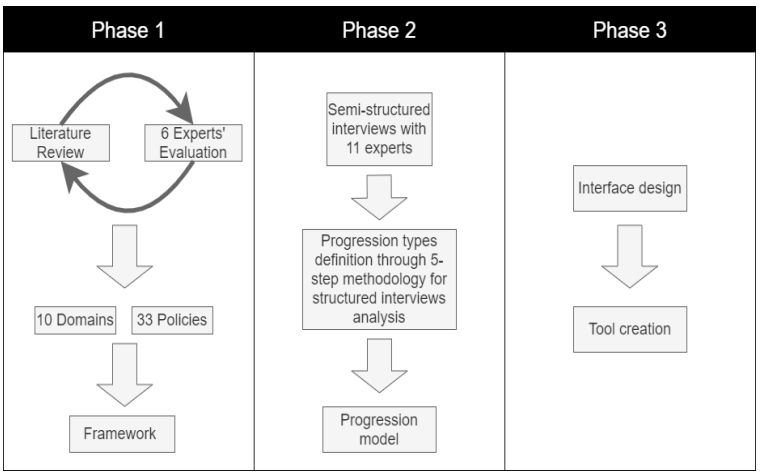

Fig. 1. Summary of the methodology

3.1 Phase 1: Development of the cyber resilience framework

Through a literature review with 65 cyber resilience documents including frameworks, KPIs, maturity models, etc. and the use of the grounded theory paradigm, an initial cyber resilience framework for SMEs was developed. This initial cyber resilience framework was evaluated and iteratively improved through the participation of six experts.

After four iterations of the experts' feedback a cyber resilience framework with 10 domains and 33 policies was developed. More details on the development of the cyber resilience framework can be found in [11].

3.2 Phase 2: Development of a progression model

For this phase, 11 experts participated in the semi-structured interviews. These experts were chosen for their vast experience in the operationalization of cyber resilience in their own context. The experts were from 3 possible profiles: organization practitioners (5), cybersecurity providers (3) or cybersecurity researchers (3). These three profiles were selected because practitioners have empirical experience on the implementation of cyber resilience policies in their own companies, cybersecurity providers have insights on how to effectively implement these policies in companies because they do it in a daily basis, and researchers have knowledge on the literature regarding cyber resilience and how it should be implemented. Thus, these profiles should complement each other and enrich the answers obtained in the interviews.

The interviews with these experts were designed in such way that the result of each interview was a progression model for the 33 cyber resilience policies found in previous research [11, 28]. To achieve this, experts were given a script in which the definitions considered for cyber resilience and progression model were explained, the 10 domains and 33 policies were listed and the explanation of the objectives of the interview.

During the interview, the experts had to define their progression model in two steps:

4. Define the starting maturity level from each policy on a 5-level scale where 1 was the least advanced and 5 the most advanced maturity state. This 5-level scale did not assign names to each maturity level besides the number of the level to avoid biasing the answers. Other maturity models in the literature use between 3-6 maturity levels [10, 23, 27] and some also choose not to define the names of each maturity level [10, 27].
5. Describe the progression of the policy from the defined starting maturity until the most advanced maturity state (e.g. if the starting maturity was 2, they had to describe how the policy manifested at that level, then level 3, then 4 and finally level 5).

The experts were asked to do these two steps for each of the 33 policies of the framework defined in the previous phase and were asked to be as realistic as possible while doing so. They were also allowed to skip intermediate maturity level descriptions when they considered the policy stayed the same as in the previous maturity level. All of these interviews were recorded in order to ensure correct transcription of the progressions the experts suggested, and the transcriptions were also sent back to the experts to ensure that their ideas were correctly embodied.

Once the transcriptions were ready, they were analyzed using the 5-step methodology for the analysis of semi-structured interviews as suggested in [29]. In other words, the transcripts from the interviews were carefully read to identify common concepts and characteristics among the progressions described by the experts. These common concepts were grouped in order to define categories or progression types that were later used to code each policy with the most fitting progression type or types. Once the policies and progressions were coded, the mode (most frequent) starting maturity and progression type (or types in case of bimodality) were calculated and this information combined with the experts' input was used to define a progression for each policy with its

most common starting maturity level and progression types. A summary of this 5-step methodology is shown in Fig. 2.

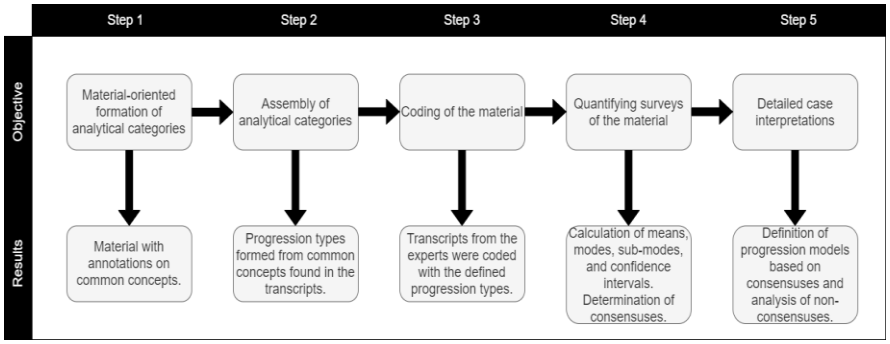

Fig. 2. Transcript analysis methodology summary

3.3 Phase 3: Development of the strategic planning and self-assessment tool

With the progression model, Microsoft Excel was used to define an interface in which companies could self-assess, then set goals for each policies maturity, and finally define action plans in order to achieve those goals.

The interface was designed to make the tool as user-friendly as possible by using different sheets to self-assess and using a color code to indicate the cells that the user had to modify in each sheet (green background), cells that were defined in previous sheets (blue background), cells from the framework (yellow background) and informative cells (white background).

With the information from the framework, the progression models for each policy and the interface decisions, the self-assessment tool was constructed.

4 Results

Through the use of the methodology described in the previous section, the developed cyber resilience strategic planning and self-assessment tool was based on the 10 domains and 33 policies of the cyber resilience framework for SMEs. With this framework 11 experts were asked to define their own progression model for each if the 33 policies. With the transcripts of the interviews, the common progression types were identified and defined in order to later code the transcriptions with the corresponding progression type for each policy and for each expert. The identified progression types in this step were the ones shown in Table 1.

After the transcripts were analyzed to determine which progression types described each of the expert's progression for each policy better. The most common starting maturity level and progression types for each policy were determined.

Table 1. Identified progression types and their definitions

Progression type	Code	Definition
Investment Increase	II	This code was assigned when the expert's progression description was related to an increase in the resources (mainly economic resources) dedicated to implementing/operationalizing the policy.
Continuity	C	This code was assigned when the expert's progression description was based on the increase of frequency in which the policy's actions are performed in the company (i.e. it was done more and more frequently as the level increased).
Specificity	S	This code was assigned when the expert's progression describes an increase in level of detail in which the policy is done as the maturity of the company increases. (i.e. it started in a general way and became more detailed and specific as the level increased).
Expansion	E	This code was assigned when the expert's progression description included the expansion of the policy's action in the company (e.g. the action was performed in some sections of the company and it started being done in more sections as the level increased).
Formalization	F	This code was assigned when the expert's progression description referred to the documentation or systematization of the actions (i.e. when the policy's actions started being intuitive or informal and where standardized and documented as the level increased).
Independence	I	This code was assigned when the expert's progression description mentioned the decrease of dependency of the company from the help of cybersecurity providers or external entities to perform the tasks related to the policy.
Optimization	O	This code was assigned when the expert's progression description was based on the measurement and improvement of Key Performance Indicators (KPIs) to optimize the performance of the policy's actions.
Proactivity	P	This code was assigned when the expert's progression description represented a change of attitude from the company towards the policy's actions (e.g. from complying to pursuing it for their own perceived benefit). The mention of continuous improvement in actions that could not be quantified was coded under this category as well.
No progression	N	This code was assigned when the expert considered that the policy was implemented and had no further progression, or when the starting maturity was considered to be at level 5.
Technology	T	This code was assigned when the expert's progression description was related to an increase in technological solutions or required more advanced technologies for the progression of the policy.

Using the starting maturity level and the progression type, a progression model was built for each of the 33 cyber resilience policies. The summary of the starting level of maturity and progression types for each policy is shown in Table 2.

Table 2. Summary of starting maturity and progression types for each policy

Domain	Policy	1	2	3	4	5
Governance	Develop and communicate a cyber resilience strategy.	Proactivity				
	Comply with cyber resilience-related regulation.	Expansion				
	Assign resources (funds, people, tools, etc.) to develop cyber resilience activities.			Optimization		

Risk Management	Systematically identify and document the company's cyber risks.	Formalization
	Classify/prioritize the company's cyber risks.	Formalization
	Determine a risk tolerance threshold.	Formalization
	Mitigate the risks that exceed the risk tolerance threshold.	Expansion
Asset Management	Make an inventory that lists and classifies the company's assets and identifies the critical assets.	Specificity
	Create and document a baseline configuration for the company's assets.	Formalization Technology
	Create a policy to manage the changes in the assets' configurations.	Formalization Technology
	Create a policy to periodically maintain the company's assets.	Proactivity
	Identify and document the internal and external dependencies of the company's assets.	Formalization Proactivity
Threat and Vulnerability Management	Identify and document the company's threats and vulnerabilities.	Formalization
	Mitigate the company's threats and vulnerabilities.	Optimization
Incident Analysis	Assess and document the damages suffered after an incident.	Formalization
	Analyze the suffered incidents to find as much information as possible: causes, methods, objectives, point of entry, etc.	Specificity
	Evaluate the company's response and response selection to the incident.	N
	Identify lessons learned from the previous incidents and implement measures to improve future responses, response selections, and risk management.	Formalization
Awareness and Training	Define and document training and awareness plans.	Specificity
	Evaluate the gaps in the personnel skills needed to perform their cyber resilience roles and include these gaps in the training plans.	Continuity
	Train the personnel with technical skills.	Specificity
	Raise the personnel's awareness through their training programs.	Formalization
Information Security	Implement measures to protect confidentiality (e.g. access control measures, network segmentation, cryptographic techniques for data and communications, etc.)	Technology
	Implement integrity checking mechanisms for data, software, hardware and firmware.	Technology
	Ensure availability through backups, redundancy, and maintaining adequate capacity.	Technology
		Expansion

Detection Processes and Continuous Monitoring	Actively monitor the company's assets (e.g. by implementing controls/sensors, IDS, etc.)			Technology
	Define a detection process that specifies when to escalate anomalies into incidents and notifies the appropriate parties according to the type of detected incident.			Formalization
Business Continuity Management	Define and document plans to maintain the operations despite different scenarios of adverse situations.			Expansion
				Formalization
	Define and document plans to respond to and recover from incidents that include recovery time objectives and recovery point objectives.			Expansion
				Formalization
	Periodically test the business continuity plans to evaluate their adequacy and adjust them to achieve the best possible operations under adverse situations.			Continuity
Information Sharing and Communication	Define information sharing and cooperation agreements with external private and public entities to improve the company's cyber resilience capabilities.			Formalization
				Proactivity
	Define and document a communication plan for emergencies that takes into account the management of public relations, the reparation of the company's reputation after an event, and the communication of the suffered incident to the authorities and other important third parties.			Specificity
	Establish collaborative relationships with the company's external stakeholders (e.g. suppliers) to implement policies that help each other's cyber resilience goals.			Formalization

The starting maturity level and progression types shown in Table 2 combined with the responses from experts, whose opinions were coherent with these characteristics, were used to create a progression model for each policy.

Using Microsoft Excel, and the progression model the tool was designed to have 4 sheets. The first sheet contains the self-assessment tool in which the input is the current maturity level of the company for each cyber resilience policy. In a second sheet, the managers can insert the goals for each policy. A third sheet for defining an action plan. And, finally, a fourth sheet for visual representation of the current state of the company and the targets that have been set.

In the self-assessment sheet, the progression models for each policy were inserted so that company managers could select the maturity level according to the description that they considered the company related the most. This sheet by itself already aids

companies to examine their current state and therefore can be helpful for them to address their weaknesses and reinforce or maintain their strengths. To select the maturity level, the manager has a cell with a combo box in which the maturity levels are selectable. Once the manager selected the current maturity level for the company, all other descriptions were formatted to have a gray background in order to give a visual cue that the selection had been registered and to highlight the selection to ensure it was aligned with the user's intentions.

Once the company has been self-assessed, the manager can go to the next sheet, the target-setting sheet. In this sheet, the current maturity level selected in the self-assessment is shown as reference for the manager to decide whether the company can progress to further levels or if they wish to maintain the current maturity level. As in the self-assessment, the descriptions for each maturity level are shown in the screen so that the managers can make a decision based on them. Moreover, the interface behaves similarly by formatting with a gray background the non-selected descriptions in order to highlight the selected goal. This sheet is very similar to the previous sheet with the only differences being that it contains the already-filled current maturity level and has a column for the manager to fill the targets. A section of the target setting sheet with the governance domain is shown in Fig. 3..

Once the manager has set the goals, by using the action plan sheet and comparing the descriptions of the current maturity level and the target maturity level, the manager can decide which concrete actions can be used to achieve the goal, set a date to achieve each action and set the resources that will be needed to achieve the action. For instance, looking at the filled information in Fig. 3. in the first governance policy "Develop and communicate a cyber resilience strategy", the action plan sheet would show the manager the descriptions of the maturity level 2 (the selected current state) and level 3 (the selected target maturity. The descriptions are the following:

- Maturity level 2: "Once the cybersecurity basics are met, the strategy centers on protecting the systems according to their risks (implement traditional cybersecurity)."
- Maturity level 3: "The cyber resilience strategy defines resilience requirements based on the risks of the company's assets. The company tries to comply with these resilience requirements to the best of their abilities. This includes having response plans in case of incidents that could harm the compliance with these requirements."

With these descriptions, the manager can get concrete actions needed to progress from level 2 to level 3. For example, "defining resilience requirements" could be the first and most important action needed to progress. Resilience requirements can be defined by classifying assets according to their criticality in the company's core processes. These requirements could also consider the associated risks for each asset. All these ideas can help the manager using the tool to define the actions that in this case would end up improving the company's cyber resilience strategy and cyber resilience capabilities. Therefore, the result of the complete process would be a concrete action plan for cyber resilience operationalization or cyber resilience improvement in the company.

Domain	Policy	Current Maturity Level	Target Maturity Level	1	2	3	4	5
Governance	**Develop and communicate a cyber resilience strategy.**	2	3	A simple strategy based on intuition and current knowledge is defined with the objective to cover the basic cybersecurity needs. In other words, in this level, companies should prioritize the policies and measures needed to define an effective strategy (asset management, risk management, etc.).	Once the cybersecurity basics are met, the strategy centers on protecting the systems according to their risks (implement traditional cybersecurity).	The cyber resilience strategy defines resilience requirements based on the company's assets. The company tries to comply with these resilience requirements to the best of their abilities. This includes having response plans in case of incidents that could harm the compliance with these requirements.	The company's strategy is detailed and tries to go in depth on how to make the systems and processes as resilient as possible with specific plans on how to recover in case the protection methods fail.	The strategy is continuously improved upon, trying to implement lessons learned from the company's previous iterations of the strategy and previous successes or mistakes.
	Comply with cyber resilience-related regulation.	3	4	The company has identified the cyber resilience related laws and regulations that directly concern their activity.	The company does its best to comply with the most cyber related laws and regulations.	The company tries to comply with the laws and regulations that have been identified by internally auditing which are being complied with and which are still in progress.	The company starts exploring laws and regulations that can complies with more indirectly concern their demanding activity and sees added value in complying with these laws as a way to improve their cyber resilience.	The company continuously driven by their own cyber resilience implementation and not simply with the intention of complying.
	Assign resources (funds, people, tools, etc.) to develop cyber resilience activities.	4	4			Specific, documented budgets and resources are assigned for the fulfillment of the cyber resilience strategy.	The investments in cyber resilience are controlled through KPIs that the company has selected to try to optimize their allocation of resources.	Resources are flexibly moved in order to maximize the benefits of the assigned and optimize the values of the company's KPIs.

Fig. 3. Target setting sheet section

Finally, for visual representation of the self-assessment and the set targets, the tool also generates radar graphs with the information filled in previous sheets. An example of a domain-level radar graph and the governance and asset management domains are shown in Fig. 4.

Fig. 4. Example visual representation (domain-level, governance and asset management)

Due to the nature of the tool, it can be used several times by the same company in order to check how the company is improving over time, check whether the actions are working as expected, and reset the goals after each assessment. The self-assessment, especially if it is done repeatedly over time can help the company gain awareness of their current situation and gain experience by trying to improve that situation. Therefore, the tool addresses the necessary profiling or customization required by other aiding documents (frameworks, KPIs, etc.) but in a way in which the manager can simply use the same suggested policies and progressions as a way to define the current company's profile and strategize on how to improve where they consider necessary.

5 Discussion

The main result of this paper is a tool that guides a company manager through a self-assessment and a cyber resilience strategic planning. This tool could contribute by giving some insight on how the natural progression of cyber resilience policies commonly looks and what specific states are common to go through when implementing one of these policies.

As discussed during this article there is usually scarce information on how the policy starts when first implemented by a company and how it progresses until it reaches the

most advanced state. Therefore, the descriptions of the initial state and natural progression of companies could be useful in three different scenarios:

1. When a company is starting a cyber resilience operationalization process from the very first steps because it describes in a realistic way the most common first manifestations of the policies.
2. When a manager wants to assess the current state of cyber resilience in a company with limited knowledge and experience in the field because managers can probably relate the current situation to these empirical descriptions.
3. And, when a manager wishes to plan at a strategic level what the next steps of the company should be because once the manager has identified the current maturity, the next levels can be set as goals to aim for, and the descriptions of these next levels should serve as insight on how to achieve them.

Building cyber resilience should also help companies face the current cyber scenario by making them flexible and adaptable towards the possible cyber incidents they may suffer. The adaptability associated with the cyber resilience capability can make companies better at continuing their operations despite adverse events. In other words, the process of building cyber resilience by strategically implementing cyber resilience should in turn increase the ability of a company of being "safe-to-fail".

Moreover, the results of this paper can be combined with previous research on the prioritization of the cyber resilience policies [11, 28]. These studies have attempted to define the priorities of the domains and policies in the presented cyber resilience framework by proposing implementation orders. Although the progression model can help assess the current maturity state of a company and plan future implementations, the implementation order is still necessary to prioritize the policies and decide which policies to start implementing for the most effective results. Having just the progression model while making the strategic plan would be an improvement over having just the list of policies but would still just have partial information on effective ways to prioritize. Where the progression model contributes the most is when defining actions to start the implementation of a policy or to improve upon an existing implementation, but the decision on which policies to implement first should be taken with the aid of an implementation order. Therefore, by combining the implementation order and strategic planning of cyber resilience operationalization, companies should have powerful tools towards an effective cyber resilience operationalization.

As limitation to this study, the experts' vast experience does not overcome their cultural baggage nor the limited sample size. Most of the experts were from the same geographical area, the Basque Country, Spain, an area rich in manufacturing companies. This cultural background could potentially affect their opinions on how the policies progress. For similar reasons, the opinions of a sample of 11 experts may not be generalizable to all companies, and further research should attempt to replicate these results with more experts and from more varied cultural backgrounds to increase the sample size of experts and to statistically validate the results obtained in this study. Furthermore, these results should also be validated and iteratively improved through testing in real situations to enrich the obtained results.

6 Conclusions

This study proposes a strategic planning and self-assessment tool based on a progression model built with data collected from semi-structured interviews to 11 experts. The usage of this tool intends to aid companies by structuring their strategic planning towards realistic goals found in the descriptions of the natural progression of policies that the progression model provides. Correct strategic planning is key to build cyber resilience in a cyber scenario that is noticeably dangerous for all types of companies, but especially for the ones that cannot afford to not be prepared for an unforeseen cyber incident such as SMEs.

Therefore, the tool is meant to help companies build cyber resilience capabilities by facilitating the process of self-assessing their current state while at the same time providing ideas on how to progress. The same tool lets companies set goals and define action plans in order to further assist them in the strategic planning.

Future lines of research should try to mitigate this study's limitations by attempting to replicate the results with more experts and with experts from different cultural backgrounds. Moreover, these results should also be tested in companies to iteratively improve the results by empirical trial and error that often highlights unforeseeable nuances.

References

1. Tofan D, Nikolakopoulos T, Darra E (2016) The Cost of Incidents Affecting CIIs: Systematic review of studies concerning the economic impact of cyber-security incidents on critical information infrastructures (CII). ENISA, Athens, Greece
2. Damiano M (2017) VIPRE Announces Launch of VIPRE Endpoint Security - Cloud Edition | Business Wire. In: Bus. Wire. https://www.businesswire.com/news/home/20171002005176/en. Accessed 28 Oct 2019
3. Millaire P, Sathe A, Thielen P (2017) What All Cyber Criminals Know: Small & Midsize Businesses With Little or No Cybersecurity Are Ideal Targets. NJ, USA
4. Björk F, Henkel M, Stirna J, Zdravkovic J (2015) Cyber Resilience – Fundamentals for a Definition. Adv Intell Syst Comput 353:III–IV. https://doi.org/10.1007/978-3-319-16486-1
5. Luiijf HAM, Nieuwenhuijs AH (2008) Extensible threat taxonomy for critical infrastructures. Int J Crit Infrastructures 4:409. https://doi.org/10.1504/IJCIS.2008.020159
6. Schneier B (2014) The future of incident response. IEEE Secur. Priv. 12:96–97
7. Linkov I, Eisenberg DA, Bates ME, et al (2013) Measurable resilience for actionable policy. Environ Sci Technol 47:10108–10110. https://doi.org/10.1021/es403443n
8. Deutscher SA, Bohmayr W, Asen A (2017) Building a Cyberresilient Organization. Boston, MA, USA
9. World Economic Forum (2016) A framework for assessing cyber resilience. Geneva, Switzerland
10. INCIBE (2019) Indicadores para Mejora de la Ciberresiliencia (IMC). Madrid, Spain
11. Carias JF, Borges MRS, Labaka L, et al (2020) Systematic Approach to Cyber Resilience Operationalization in SMEs. IEEE Access 8:174200–174221. https://doi.org/10.1109/ACCESS.2020.3026063

12. Cranor LF (2008) A Framework for Reasoning About the Human in the Loop. In: Proceedings of the 1st Conference on Usability, Psychology, and Security. USENIX Association, San Francisco, CA, USA, pp 1:1--1:15
13. NIST (2018) Framework for Improving Critical Infrastructure Cybersecurity v 1.1. Gaithersburg, MD, USA
14. Center for Internet Security (CIS) (2019) CIS Controls V 7.1. NY, USA
15. Hong Kong Monetary Authority (2016) Cyber Resilience Assessment Framework. Hong Kong, China
16. Linkov I, Eisenberg DA, Plourde K, et al (2013) Resilience metrics for cyber systems. Environ Syst Decis 33:471–476. https://doi.org/10.1007/s10669-013-9485-y
17. International Organization for Standarization (ISO) (2013) ISO/IEC 27001:2013(en) Information technology — Security techniques — Information security management systems — Requirements. Geneva, Switzerland
18. International Standards on Auditing (ISA) (2009) ANSI/ISA–62443-2-1 (99.02.01) Security for Industrial Automation and Control Systems Part 2-1: Establishing an Industrial Automation and Control Systems Security Program. 1–170
19. NIST (2013) Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53 Rev. 4). Gaithersburg, MD, USA
20. Tang C (2017) Key performance indicators for process control system cybersecurity performance analysis. https://doi.org/10.6028/NIST.IR.8188
21. Nys J (2016) How to Steer Cyber Security with Only One KPI: The Cyber Risk Resilience. RSA Conf. 1–42
22. MITRE (2012) Cyber Resiliency Metrics. VA, USA
23. Department of Energy (DOE) (2014) Cybersecurity Capability Maturity Model (C2M2). Washington DC, USA
24. Pacific Northwest National Laboratory (2019) Buildings Cybersecurity Capability Maturity Model. Washington DC, USA
25. Caralli R, Knight M, Montgomery A (2012) Maturity models 101: a primer for applying maturity models to smart grid security, resilience, and interoperability
26. Carneiro A (2013) Maturity and Metrics in Health Organizations Information Systems. In: Handbook of Research on ICTs and Management Systems for Improving Efficiency in Healthcare and Social Care. IGI Global, Lisbon, Portugal, pp 937–952
27. Carnegie Mellon University (2016) Cyber Resilience Review (CRR). In: Dep. Homel. Secur. https://www.us-cert.gov/ccubedvp/assessments. Accessed 6 Feb 2018
28. Carias JF, Borges MRS, Labaka L, et al (2021) The Order of the Factors DOES Alter the Product: Cyber Resilience Policies' Implementation Order. pp 306–315
29. Schmidt C (2004) The Analysis of Semi-structured Interviews. In: Flick U, von Kardorff E, Steinke I (eds) A Companion to Qualitative Research, English. SAGE Publications, London, UK, pp 253–258