12-7-2022

Old Keys May Not Open New Doors: The Necessity of Agility in Cybersecurity Policymaking

Masoud Afshari-Mofrad
Macquarie Business school, Macquarie University, Sydney, Australia,
Masoud.afsharimofrad@hdr.mq.edu.au

Babak Abedin
Macquarie Business school, Macquarie University, Sydney, Australia, babak.abedin@mq.edu.au

Alireza Amrollahi
Macquarie Business school, Macquarie University, Sydney, Australia, ali.amrollahi@mq.edu.au

Old Keys May Not Open New Doors: The Necessity of Agility in Cybersecurity Policymaking

Full research paper

Masoud Afshari-Mofrad
Macquarie Business school, Macquarie University, Sydney, Australia
Email: Masoud.afsharimofrad@hdr.mq.edu.au

Babak Abedin
Macquarie Business school, Macquarie University, Sydney, Australia
Email: babak.abedin@mq.edu.au

Alireza Amrollahi
Macquarie Business school, Macquarie University, Sydney, Australia
Email: ali.amrollahi@mq.edu.au

Abstract

The volatile and dynamic nature of cyberspace has raised concerns over security and organisations are trying to make policies to protect their digital assets. However, policymaking in this field is still using traditional methods, which are slow and incompatible with the pace of change in the environment. Thus, it is vital to increase the speed of policy development in an agile and flexible manner. The question is, what does agility mean here and why is it important for organisations? To answer these questions, this study uses a systematic literature review approach and investigates 42 selected papers. By analysing the selected papers, a definition of cybersecurity policymaking agility is provided, and its importance in combating new cyberthreats is discussed. Building on and extending the organisational agility, policymaking and cybersecurity management research streams, the findings of this study propose new research opportunities for future studies.

Keywords: Agile, information security policy, strategy, cybersecurity management, organisational agility

1. Introduction

According to Forbes (2022), cyberthreats are the biggest concern for firms globally, and the results of the Allianz Risk Barometer show that cyberattacks, such as ransomware, are of greater concern for businesses than challenges such as business interruption or the COVID-19 outbreak. It has been reported that companies lost more than US$6 trillion because of cyberattacks in 2021 (Eling et al., 2021). In addition to their major economic damage, cybersecurity threats are changing rapidly. As the nature of cyberthreats now includes ransomware, malicious emails, malware (Hogan-Burney, 2021) and social engineering (Klimburg-Witjes & Wentland, 2021), the trend is that technological development is shifting towards more sophisticated and cloud-based services (Panetta, 2021).

To face the challenge of cyberthreats and to protect their assets against cyberattacks, organisational leaders have started developing or revising cybersecurity policies. However, the dynamic and fast-moving nature of cyber risks created by agile, motivated and smart people have cast doubts on the slow approaches of cybersecurity policymaking (CSPM) (Baskerville et al., 2014; De Bruijn & Janssen, 2017; Siregar & Chang, 2019) because most organisations seem to be better equipped to defend against static and predictable cyberthreats than new, dynamic and unpredictable ones (A. Naseer et al., 2021).

To address this issue, there is a growing interest in understanding and implementing cybersecurity policy agility. Scholars and practitioners attempt to improve the policymaking process in a way that it can react promptly and properly when policy stability is challenged or the expected outcomes of current policies are at risk (Howlett et al., 2018). Policy agility enables policymakers to adapt to the turbulence in the environment properly and adjust policies according to the emerging patterns or anomalies (Capano & Woo, 2018). In a simple definition, agility is the ability to change direction both swiftly and accurately and agile organisations are those that can facilitate timely responses to changes in their environment (janssen & van der Voort, 2020). This is particularly important in a cybersecurity environment where cyberthreats are severe and unpredictable and the introduction of new technologies brings new vulnerabilities and opportunities (Jalali et al., 2019), thus, cybersecurity policy agility is of great importance to face the dynamic environment.

Although previous studies have investigated some aspects of cybersecurity policies, such as development (Paananen et al., 2020), organisational learning through cybersecurity management (Ahmad et al., 2019), cybersecurity incident management (He et al., 2022) and cybersecurity incident response processes (He et al., 2022; H. Naseer et al., 2021), further studies are still needed to scrutinise the way such policies should be developed in an agile manner (Cram et al., 2017; Dhillon et al., 2021; Paananen et al., 2020; Siregar & Chang, 2019). Reviewing the literature reveals that, while there is implicit consensus among scholars about the novelty and importance of 'cybersecurity policymaking agility' (Harnesk & Lindstrom, 2011; H. Naseer et al., 2021; Siregar & Chang, 2019; Tam et al., 2021; Tisalde, 2016), no consensus exists about what 'cybersecurity policymaking agility' precisely is and how it should be theoretically approached.

Thus, this paper systematically reviews the emerging literature on 'cybersecurity policymaking agility' to investigate the current state of knowledge on agile CSPM in terms of its importance and conceptualisation by answering the following questions:

- RQ1: What is cybersecurity policymaking agility?
- RQ2: What is the importance of agile cybersecurity policymaking for organisations?

To answer the above questions, the present paper attempts to introduce and conceptualise agility in cybersecurity policymaking by carrying out an in-depth systematic literature review of related articles. We argue that static approaches toward cybersecurity policymaking might affect the competitiveness of organisations through a shortage of required skills and capabilities to mitigate dynamic and unpredictable cyberthreats (Ikeda et al., 2019; A. Naseer et al., 2021). We also contend that agile CSPM helps organisations to manage cyber incidents more effectively by allowing them to continually redefine or enhance their abilities in detecting and responding to new cyberthreats. We assert that this concept has not been investigated before because its importance in sustaining value in organisations has not yet been studied in the literature. Finally, we discuss that CSPM agility could be a source of better cybersecurity policy compliance by employees because of its inclusive processes. The findings of the present study can give rise to further research on the process of developing cybersecurity policies and open new ways to make organisations more prepared for facing changes in their dynamic cyberthreat environment.

2. Background

Policymaking is a complex interactive and iterative process that involves various stakeholders (Janssen & Helbig, 2018). There are various models with different steps for policymaking, however, the most ubiquitous model is 'policy-cycle' that is made up of five main 'stages': agenda-setting, policy formulation, decision-making, policy implementation and evaluation (Howlett et al., 2017; Valle-Cruz et al., 2020).

In this model, agenda-setting is problem framing and exploring the need for a policy; policy formulation refers to developing policy alternatives; decision making is the selection of the final option among a range of alternatives; policy implementation means using regulation, planning or legislation to enact the selected policy; and, finally, policy evaluation refers to evaluating the effects of the implemented policy (Simonofski et al., 2021).

The policy-cycle has been used in different contexts to demonstrate the process of policymaking and information security is one of these contexts. For instance, Paananen et al. (2020) reviewed the literature to investigate the definitions of information security policy (ISP), explore its phases and examine the policy development process.

However, all previous reviews in the cybersecurity context have not concentrated on the policy development process. For example, Dhillon et al. (2021) conducted a literature review and proposed a socio-technical framework based on the gaps that they found between the findings of their review and interviews with practitioners. By reviewing the literature, Cram et al. (2017) proposed a policy research framework that shows the relationships between the ISP process and organisational security objectives. Another study focused on narrative reviewing of cybersecurity policy problems in small businesses and found that characteristics, such as large cohort size and piecemeal IT architecture, in such businesses increase cybersecurity. The authors have also emphasised that the agility of small businesses could be considered an opportunity to be able to adapt their endeavours to the changing cyberthreats in their environment (Tam et al., 2021).

Although these studies reviewed the literature on different aspects of information security or cybersecurity policy, none of them has focused on agility in cybersecurity policymaking. So, in this study, building on the findings of previous literature reviews, we review the notion of agility in the cybersecurity policymaking process. The next section explains our approach to reviewing the literature.

3. Literature review approach

We adapted the systematic literature review (SLR) procedure recommended by (Okoli, 2015). To do so, we first identified the purpose and intended goals of the study. As discussed earlier, the dynamic and ever-changing nature of the cyberthreat environment forces organisations to be agile in every aspect of their cybersecurity endeavours, and since prior studies have not provided a comprehensive definition of cybersecurity policymaking agility, we decided to fill the gap by investigating this concept. In the second step, research questions were raised and after in-depth discussions regarding each question, two research questions were finally agreed upon. Afterwards, the plan for conducting the study, including the databases that should be searched, the depth and scope of the review (business, management and accounting) and the search procedure and string, was built. Scopus database, the largest database for peer-reviewed papers in the field of IS (Niknejad et al., 2020), was used to find the relevant papers. According to the research protocol and based on the research questions, the following string was devised to search the title, keywords and abstract of the articles:

TITLE-ABS-KEY (Cybersecurity OR 'Information Security' OR 'cybersecurity' OR 'Cyber Security') AND TITLE-ABS-KEY (Policy OR Strategy OR Management).

In the third step, the inclusion and exclusion criteria of papers were selected. In this step, papers that focus on information security or cybersecurity policy, or strategy development were included in the study. In the selection process, articles had to be relevant to the idea of making swift decisions regarding cybersecurity policies and formulate/reformulate policies considering the changes in the cyber environment. Therefore, in the first round, titles of papers were investigated and papers that focused only on technical aspects (for example, developing algorithms to detect intrusion) or studied aspect of cybersecurity that is not related to policy (such as audit or vulnerability management) were excluded. In the second round, abstracts of papers

were studied and articles that did not investigate the policy development process (for instance, concentrating on regulatory and legal issues) or studied cybersecurity policy from another point of view (e.g., the perceptions of top managers) were excluded. In the final round, selected papers were completely studied to understand their relationship to agility in CSPM. At this step, papers that had no potential to contribute to the conceptualisation of CSPM agility (for instance worked-on traditional types of CSPM using ISO or COBIT models) were excluded from our pool of studies.

Using the above search string, 973 papers were found. Out of these papers, 113 papers were selected in the first round, then 62 papers were selected by reading their abstract. After a careful study of all 62 papers, 27 papers were found relevant for answering the research questions. We then conducted forward and backward referencing, which resulted in 15 more papers, making up the total of 42 reviewed papers. Of these 42 papers, 22 papers were empirical and 20 papers were conceptual.

Next, information was extracted from each paper based on the research questions to be served as the raw material for the synthesis step. NVIVO 12 was used to code and store the details required for answering the research questions. Using this approach, 37 unique primary excerpts were obtained from the reviewed papers. The excerpts were synthesised and combined to find answers to the research questions. In the final step, the procedure and findings of the literature review were written and published in this paper.

4. Findings

Reviewing the selected papers revealed that CSPM agility is a relatively novel concept and scholars have started developing its different dimensions in the past decade. Since 2010, the number of publications has increased, especially since 2019. However, the number of scientific publications on this issue is still very limited.

Based on the dispersion of selected papers in various fields, it can be argued that the notion of CSPM agility is a multidisciplinary subject living on the nexus of Information Systems (IS), Management Science and Computer Sciences disciplines.

CSPM agility is mostly rooted in IS, however, management science and computer science fields have made contributions by introducing agile principles and policy-cycle. The concept is built upon the foundations of three research streams, namely organisational agility, policymaking and cybersecurity management.

4.1. What is cybersecurity policymaking agility?

Agility is a concept coined in the field of software engineering that has gradually expanded to the field of organisational studies (janssen & van der Voort, 2020). Agile principles focus on breaking the processes down into smaller and more manageable parts and delivering prioritised tasks in shorter iterations. This can be considered in policymaking as well, where using new tools and techniques provide the possibility of giving feedback in each stage of the policy-cycle in almost real-time, increasing the speed of the policymaking process dramatically (Valle-Cruz et al., 2020). In agile principles, there is no need for a consequence between the tasks and activities can be performed in parallel. For instance, agenda-setting (for new policies) and evaluation (for previous policies) can take place at the same time (Valle-Cruz et al., 2020). Additionally, each stage of the policy-cycle could be evaluated faster, enabling policymakers to decide quicker on the re-formulation of policies.

Using the agile approach to cybersecurity policymaking and considering CSPM agility as one of the pillars of organisational agility (as argued by Zaini et al., 2020), the definition of agile CSPM can be extracted from that of organisational agility. Therefore, considering the definition presented by Queiroz et al. (2018), CSPM agility can be regarded as the firm's ability to detect and respond to opportunities and threats in the cyberthreat climate and reformulate cybersecurity policies with ease, speed and dexterity. This is also in line with the definition provided by Naseer et al. (2021) for agility in the cybersecurity field as the extent of efficiency and swiftness by which organisations can reconfigure their resources and processes to detect and respond to new cyberthreats (A. Naseer et al., 2021). Agility of CSPM entails that the principles underpinning cybersecurity policies should be adapted to the changes in the cyberthreat environment continuously (Ahmad et al., 2020).

Despite the novelty of the notion of CSPM agility that is avowed by a few scholars such as Tam et al. (2021), a consistent vocabulary has emerged in recent years. Increasing cyberthreat intelligence (H. Naseer et al.,

2021), using social media to issue cyber alerts (Syed, 2020), and raising cybersecurity awareness (Armenia et al., 2021) are some of the terms used in the reviewed literature to show the necessity of sensing the changes in the environment and responding to threats or seizing opportunities in a timely manner. These threats and opportunities should be categorised in different scenarios so that policymakers can incorporate the highest priorities into cybersecurity policies, which would in turn correspond to the first stage of policy-cycle: agenda-setting agility. In addition, the prominence of reformulating organisational cybersecurity policies based on the continuously changing environment and the necessity of considering all alternative solutions for cybersecurity policies was another theme in the selected papers (Abbas et al., 2011; Armenia et al., 2021). In doing so, having access to real-time analytics for creating actionable insights for cybersecurity policymakers in an agile way (H. Naseer et al., 2021) and providing dynamic models to help them formulate different intervention policies (Armenia et al., 2021) is of great importance and related to stage two of the policy-cycle: policy formulation agility. The emergence of new sophisticated and algorithm-based technologies (such as artificial intelligence) has facilitated the pace of change in characteristics and ideas that converge in the formulation stage (Valle-Cruz et al., 2020).

To make agile decisions, scholars have emphasised the importance of the ability of organisations to manage their information processing (Keramati et al., 2016; H. Naseer et al., 2021) and the utilisation of cybersecurity-based decision support tools (Abbas et al., 2011; Keramati et al. 2012; Nazareth & Choi, 2015). This corresponds to the third stage of policy-cycle, namely decision-making agility. By developing these capabilities, organisations will be able to respond to newly detected and unique internal or external risks in an agile decision-making process (Baskerville et al., 2014). Additionally, stage four of the policy-cycle, policy implementation agility, needs dynamic adaptation of security tasks and operations to the newest attack patterns (Repetto et al., 2021). Finally, continuous evaluation of cybersecurity policies is another necessity in agile CSPM, which would relate to stage five of the policy-cycle, policy evaluation agility. Long evaluation processes are a major problem in many organisations because when the evaluation is over, new threats have emerged, which makes the evaluation obsolete (Abbas et al., 2011). In this regard, there is a need for an iterative process through which different policy interventions can be evaluated rapidly (Armenia et al., 2021) to identify the gaps in current policies and recognise the areas that new policies should address (Stewart, 2022).

Based on the review of the selected papers, Table 1 demonstrates the key concepts used in the literature regarding the notion of CSPM agility.

Key terms	Highlights of results	Source
Iterative, successive process	Need for an iterative process for rapid evaluation of policy interventions	Armenia et al. (2021)
Continuous changes in threats and opportunities in the cyberspace	Agility of CSPM entails that the principles underpinning cybersecurity policies should be adapted to the changes in the cyberthreat environment continuously	Ahmad et al. (2020)
Making swift policy decisions	The prominence of reformulating organisational cybersecurity policies based on the continuously changing environment and the necessity of considering all alternative solutions for cybersecurity policies	Abbas et al. (2011)
Responding to the important changes	Organisations will be able to respond to newly detected and unique internal or external risks in an agile decision-making process	Baskerville et al. (2014)
Incorporating the decisions into organisational processes	The extent of efficiency and swiftness by which organisations can reconfigure their resources and processes to detect and respond to new cyberthreats (IR response agility)	Naseer et al. (2021)
Effectively evaluating and re-evaluating the cybersecurity policies	Each policy stage could be evaluated faster, enabling policymakers to decide more quickly on policy re-formulation	Valle-Cruz et al. (2020)

Key terms	Highlights of results	Source
Detect and respond to opportunities and threats with ease, speed and dexterity	Organisational agility definition	Queiroz et al. (2018)

Table 1. The sources used for defining CSPM agility

By synthesising the abovementioned findings in the selected papers, we pose the following description for CSPM agility:

An iterative, successive process of detecting continuous changes in threats and opportunities in the cyberspace, making swift policy decisions regarding the method of responding to the important changes, incorporating the decisions into organisational processes and effectively evaluating and re-evaluating the cybersecurity policies with ease, speed and dexterity.

4.2. The importance of CSPM agility

A review of the selected papers revealed that the importance of agility in cybersecurity policymaking has been highlighted in the literature by focusing on the changes in the cyberthreat climate that bring new types of threats and create an uncertain environment for policymaking. Previous studies contended that it is vital to adjust the policies to emerging risks and dynamically adapt processes and operations to constantly changing attack patterns (Abbas et al., 2011; Armenia et al., 2021; Repetto et al., 2021). In addition to cyberthreat patterns, changes in the technologies and emerging tools and devices for cyber defence force organisations to balance their policies (Garcia-Perez et al., 2021).

It has been revealed in the literature that most organisations are better equipped to defend against static and predictable cyberthreats and they are more vulnerable to threats that are new, dynamic and unpredictable (A. Naseer et al., 2021). However, as discussed earlier, the cyberthreat environment is dynamic and evolving. Thus, firms need to develop adaptive cybersecurity capabilities and make a balance between their reactive and proactive policies (Jalali et al., 2019). One solution to this challenge is being agile in cybersecurity policymaking because delays in cybersecurity decision-making can lead to ineffective investments (Jalali et al., 2019).

As argued by Line & Albrechsten (2015), adaptive and agile approaches are essential in complex and uncertain situations and they should, therefore, be well-matched for cybersecurity management (Line & Albrechtsen, 2015). The key factor to achieve this is the length of time taken from identifying major cyberthreats in the environment to respond to them. The longer the response time, the greater the probability of impact on the organisation. Thus, the success of cybersecurity depends on responding to threats before they cause any damage (A. Naseer et al., 2021). To be able to do so, cybersecurity policies should be restructured and optimised in a swift and timely manner to address the challenges posed by the new threats and remove the root causes of vulnerabilities in an organisation's security system (Ahmad et al., 2020).

Cybersecurity policy agility helps organisations to manage cyber incidents more effectively by allowing them to continually redefine or enhance their abilities in detecting and responding to new cyberthreats (Siregar & Chang, 2019). It assists firms in protecting their competitive advantage against a decline in performance through cyberattacks and can be considered a value-sustaining subject (A. Naseer et al., 2021; Tallon et al., 2019).

The agile philosophy has been successful in reducing large project failures through providing constant monitoring and quick feedback, ceaseless adaptation and continuous learning throughout the project. In addition, agile principles are open to changes in the requirements in the process (He et al., 2022). This is also the case in cybersecurity policies and helps organisations to reduce the harm from cyberattacks.

Another reason that makes CSPM agility critical in organisations is its emphasis on the inclusion of different stakeholders. Previous scholars have contended that in such agile systems, different stakeholders, including technical and non-technical professionals, need to work together. It is especially important to learn from previous incidents, where various stakeholders should be included to improve the policies for avoiding or

minimising the probability of future incidents. This inclusive approach could be considered one of the greatest benefits of agility in cybersecurity policymaking (He et al., 2022).

Reason of importance	Highlights of results	Source
Vulnerability to dynamic cyberthreats	The need to adjust the policies to emerging risks and dynamically adapt processes and operations to constantly changing attack patterns Vulnerability of firms to new and unpredictable threats	Abbas et al. (2011); Armenia et al. (2021); Naseer et al. (2021)
Improving cyber defence capabilities	Changes in the technologies and emerging tools and devices for cyber defence force organisations to balance their policies	Garcia-Perez et al. (2021)
Decreasing the possibility of harm	The longer the response time, the greater the probability of harm to the organisation	Naseer et al. (2021)
Proactive cybersecurity	The success of cybersecurity depends on responding to threats before they cause any damage Cybersecurity policies should be restructured and optimised in a swift and timely manner to address the challenges posed by the new threats	Ahmad et al. (2020); Naseer et al. (2021)
Improving the effectiveness of managing cyber incidents	Cybersecurity agility allows firms to continually redefine or enhance their abilities in detecting and responding to new cyberthreats	Siregar & Chang (2019)
Increasing the inclusion of stakeholders in policymaking	Various stakeholders should be included to improve the policies for avoiding or minimising the probability of future incidents	He et al. (2022)

Table 2. Highlights from previous studies on the importance of agility in CSPM

As shown in table 2, CSPM agility in the dynamic cyberthreat climate is essential for firms to respond to new threats and opportunities, improve their cyber defence capabilities, decrease the possibility of harm from cyberattacks, sustain competitive advantage, and increase the inclusion of stakeholders in the cybersecurity policymaking process. In sum, agility in CSPM is important because of the continuous changes in the environment. The agile CSPM makes it possible for organisations to be more prepared for new threats and act proactively in the cybersecurity.

5. Discussion

Since policy is one of the five key management practices through which cybersecurity protects the firm's digital assets (Ahmad et al., 2020), it is not surprising that researchers are moving toward investigating cybersecurity policymaking (Tam et al., 2021). In addition, as one of the components of organisational agility, agile cybersecurity policymaking is a necessity for firms to maintain their competitive advantage (Tallon et al., 2019; Zaini et al., 2020). Hence, in this study, we defined agility in cybersecurity policymaking and our findings revealed several reasons for its importance.

Utilising the systematic literature review approach and building on the agile principles and the concepts of organisational agility and policy-cycle, the present study showed that the traditional approach to cybersecurity management is not efficient for responding to the agile environment, and it is essential for firms to utilise agile principles in cybersecurity policymaking. The findings on the importance of CSPM agility augment the findings of previous studies (such as Baskerville et al., 2014; Siregar & Chang, 2019) that showed the importance of agility in cybersecurity. They are also in line with the findings of Tam et al. (2021) who realised that the agility of SMEs in adapting swiftly to the changes in their cyberthreat environment is their advantage over larger enterprises in securing their digital assets against cyberthreats. Similarly, the findings of Naseer et al. (2021) showing the better readiness of most organisations to defend

against static and predictable cyberthreats than new, dynamic and unpredictable ones, emphasised the significance of CSPM agility.

Additionally, we arrived at the definition of cybersecurity policymaking agility mentioned in section 4.1. Our definition considered CSPM agility as an iterative process in which the cyberthreat environment is constantly monitored at each stage of policymaking, threats and opportunities are recognised and prioritised and those with the highest potential impacts are incorporated into the process as input. As argued by (Hall et al., 2011), awareness of both internal and external situations (threats and opportunities) is essential for comprehensive policymaking. The definition addressed the notion that according to agile principles, the cybersecurity policymaking process needs to be broken down into smaller parts, i.e., policy stages, new tools and techniques for creating shorter policy iterations should be used. This is in line with the findings of Valle-Cruz et al. (2020) arguing that in the age of artificial intelligence, policy-cycle will evolve in a spiral fashion where feedback is provided in each stage of the cycle, and it will not be necessary to wait until the results of the implementation phase to be able to evaluate the policies (Valle-Cruz et al., 2020).

The definition also amplified the emphasis of previous scholars on the necessity of continuous reformulation of cybersecurity policies in response to the changes in the cyberthreat environment to find dynamic solutions for dynamic problems (Abbas et al., 2011; Armenia et al., 2021; Repetto et al., 2021). The prominence of agile decision making highlighted in our definition of CSPM agility corresponds with the notion of decision agility, acknowledged by Tallon et al. (2019), who revealed that sensing the change by organisations does not necessarily result in responding swiftly and in most cases, decision agility, which translates sensing into responding, might be a bottleneck in reacting to the changes in a timely fashion.

Finally, the importance of evaluating and re-evaluating cybersecurity policies in a timely fashion highlighted in our definition addresses the weakness of most firms in designing a long security evaluation process. As argued by (Abbas et al., 2011), such long processes make the evaluation outdated because of the emergence of new threats, hence, firms should be able to evaluate and reformulate their cybersecurity policies in an agile manner.

In summary, as argued in this article and according to the analysis of evidence gathered from the literature, the transition toward agile cybersecurity policymaking should be considered a necessity for firms. They will need to develop capabilities and competencies to be able to change the direction of policies according to the intelligence they collect from both internal and external sources. The agile process of policymaking would make them more prepared for encountering dynamic threats in their cyberthreat environment using new defensive technologies. In the meantime, agile principles in CPM will help firms to monitor and re-evaluate ill-defined or weakly designed policies that could be a source of intrusion by imposters.

6. Conclusion and recommendations for future research

A review of the selected papers revealed that previous studies have emphasised the importance of CSPM agility. However, the concept is still in its infancy and for its better theorisation, the following agenda can be followed in the future research:

- Given the roots of CSPM agility in different scientific fields, it can be analysed through the lens of related theories in these fields. For instance, Computational Learning Theory from the Computer Science discipline can be used to investigate the theoretical aspects of using machine learning in CSPM to extract policy insights from large amounts of data. The Contingency Management Theory from the management science discipline could also be used to theorise how Chief Information Security Officers (CISOs) understand and translate the changes in the cyberthreat environment and how they incorporate their insights into cybersecurity policies. Also, the Dynamic Capabilities Theory could be used by IS scholars to identify the capabilities required for firms to swiftly reformulate their cybersecurity policies according to the changes in threats/opportunities in their environment.
- The agile CSPM concept needs to be studied empirically to better understand its various aspects. Although the selected papers were a combination of conceptual and empirical studies, none of them had directly investigated the CSPM agility in action. For instance, Tam et al. (2021) had empirically approved that agility in SMEs to adapt to environmental changes is their advantage over larger companies, however, they did not explore the agility of CSPM. Therefore, there is a need for specific studies that analyse the notion of agile CSPM in action.

- Further theorisation of the CSPM agility requires developing conceptual frameworks to demonstrate its components, the capabilities required for firms to be agile in CSPM, the way it affects cybersecurity performance of the organisation and so on.

In the present study, we focused on defining the concept of CSPM agility and explained its importance. As discussed earlier, despite its limited number, the trend of publishing papers in this line of research is increasing. Our findings revealed that CSPM agility is a necessity for firms to sustain their competitive advantage and improve the effectiveness of cybersecurity policies. As one of the pillars of organisational agility, CSPM agility can help organisations to be better prepared for unpredictable and new cyberthreats and adapt their security behaviour with the changes in their environment. It can also be helpful in improving cybersecurity policy compliance through the increased inclusion of various stakeholders (including employees) in the policy learning processes. Finally, our definition of agile CSPM provides a foundation for further investigation of the introduced notion of CSPM agility and future studies can analyse different aspects of this concept both theoretically and empirically.

7. References

Abbas, H., Magnusson, C., & Yungstorm, L. (2011). Addressing dynamic issues in information security management. *Information Management & Computer Security*, *19*(1), 5-24. https://doi.org/doi.org/10.1108/09685221111115836

Ahmad, A., Desouza, K., Maynard, S., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, *71*(8), 939-953. https://doi.org/doi.org/10.1002/asi.24311

Ahmad, A., Desouza, K. C., Maynard, S. B., & Naseer, H. (2019). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, *71*, 939-953. https://doi.org/doi.org/10.1002/asi.24311

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*, 1-14. https://doi.org/doi.org/10.1016/j.dss.2021.113580

Baskerville, R., Spagnoletti, P., & Jongwoo, K. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & management*, *51*(1), 138-151. https://doi.org/doi.org/10.1016/j.im.2013.11.004

Capano, G., & Woo, J. J. (2018). Agility and robustness as design criteria. In *Routledge handbook of policy design* (pp. 420-434). Routledge

Cram, A., Jeffrey, P., & John, D. A. (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems*, *26*(6), 605-641. https://doi.org/10.1057/s41303-017-0059-9

De Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, *34*(1), 1-7. https://doi.org/doi.org/10.1016/j.giq.2017.02.007

Dhillon, G., Smith, K., & Dissanayaka, I. (2021). Information systems security research agenda: Exploring the gap between research and practice. *Journal of Strategic Information Systems*, *30*, 1-17. https://doi.org/doi.org/10.1016/j.jsis.2021.101693

Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, *24*(1), 93-125. https://doi.org/doi.org/10.1111/rmir.12169

Garcia-Perez, A., Sallos, M. P., & Tiwasing, P. (2021). Dimensions of cybersecurity performance and crisis response in critical infrastructure organisations: an intellectual capital perspective. *Journal of Intellectual Capital*, *ahead-of-print*. https://doi.org/doi.org/10.1108/JIC-06-2021-0166

Hall, J., Sarkani, S., & Mazzuchi, T. (2011). Impacts of organizational capabilities in information security. *Information Management & Computer Security*, *19*(3), 155-176. https://doi.org/10.1108/09685221111153546

Harnesk, D., & Lindstrom, J. (2011). Shaping security behaviour through discipline and agility Implications for information security management. *Information Management & Computer Security*, *19*(4), 262-276. https://doi.org/doi.org/10.1108/09685221111173076

He, Y., Zamani, E., Lloyd, S., & Luo, C. (2022). Agile incident response (AIR): Improving the incident response process in healthcare. *International Journal of Information Management*, *62*, 102435. https://doi.org/doi.org/10.1016/j.ijinfomgt.2021.102435

He , Y., Zamani, E. D., Lloyd, S., & Luo, C. (2022). Agile incident response (AIR): Improving the incident response process in healthcare. *International Journal of Information Management*, *62*, 1-15. https://doi.org/doi.org/10.1016/j.ijinfomgt.2021.102435

Hogan-Burney, A. (2021). *How cyberattacks are changing according to new Microsoft Digital Defense Report* Microsoft. https://www.microsoft.com/security/blog/2021/10/11/how-cyberattacks-are-changing-according-to-new-microsoft-digital-defense-report/

Howlett, M., Capano, G., & Ramesh, M. (2018). Designing for robustness: Surprise, agility and improvisation in policy design. *Policy and Society*, *37*(4), 405-421. https://doi.org/doi.org/10.1080/14494035.2018.1504488

Howlett, M., McConnell, A., & Perl, A. (2017). Moving policy theory forward: connecting multiple stream and advocacy coalition *Australian Journal of Public Administration*, *76*(1), 65-79. https://doi.org/ https://doi.org/10.1111/1467-8500.12191

Ikeda, K., Marshall, A., & Zaharchuk, D. (2019). Agility, skills and cybersecurity: critical drivers of competitiveness in times of economic uncertainty. *STRATEGY & LEADERSHIP*, *47*(3), 40-48. https://doi.org/10.1108/SL-02-2019-0032

Jalali, M., Siegel, M., & Madnick, S. (2019). Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *Journal of Strategic Information Systems*, *28*, 66-82. https://doi.org/doi.org/10.1016/j.jsis.2018.09.003

janssen, H., & van der Voort, H. (2020). Agile and adaptive governance in crisis response: Lessons from the COVID-19 pandemic. *International Journal of Information Management*, *55*, 102180. https://doi.org/doi.org/10.1016/j.ijinfomgt.2020.102180

Janssen, M., & Helbig, N. (2018). Innovating and changing the policy-cycle: Policy-makers be prepared. *Government Information Quarterly*, *35*, 99-105. https://doi.org/doi.org/10.1016/j.giq.2015.11.009

Keramati, A., Mojir, N., Afshari-Mofrad, M., Jahanandish, I., & Derakhshani, A. (2012). An artificial neural network-based DSS to prioritise information technology and its complementary investments in industrial firms. *International Journal of Business Information Systems, 9(2)*, 149-168.

Keramati, A., Afshari-Mofrad, M., Behmanesh, I., & Gholami, R. (2016). The impact of information technology maturity on firm performance considering the moderating role of relational maturity: an empirical research. *International Journal of Business Information Systems*, *23*(1), 23-43.

Klimburg-Witjes, N., & Wentland, A. (2021). Hacking Humans? Social Engineering and the Construction of the "Deficient User" in Cybersecurity Discourses *Science, Technology, & Human Values*, *46*(6), 1316-1339. https://doi.org/doi.org/10.1177/0162243921992844

Line, M. B., & Albrechtsen, E. (2015). Examining the suitability of industrial safety management approaches for information security incident management. *Information & Computer Security*, *24*(1), 20-37. https://doi.org/10.1108/ICS-01-2015-0003

Naseer, A., Naseer, H., Ahmad, A., Maynard, S. B., & Siddiqui, A. M. (2021). Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis. *International Journal of Information Management*, *59*, 102334. https://doi.org/doi.org/10.1016/j.ijinfomgt.2021.102334

Naseer, H., Maynard, S. B., & Desouza , K. C. (2021). Demystifying analytical information processing capability: The case of cybersecurity incident response. *Decision Support Systems*, *143*, 1-11. https://doi.org/doi.org/10.1016/j.dss.2020.113476

Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. *Information & management*, *52*, 123-134. https://doi.org/dx.doi.org/10.1016/j.im.2014.10.009

Niknejad, N., Ismail, W., Ghanib, I., Nazari, B., Bahari, M., & Bin CheHussind, R. (2020). Understanding Service-Oriented Architecture (SOA): A systematic literature review and directions for further investigation. *Information Systems*, *91*, 101491. https://doi.org/doi.org/10.1016/j.is.2020.101491

Okoli, C. (2015). A Guide to Conducting a Standalone Systematic Literature Review. *Communications of the Association for Information Systems Research*, *34*(1), 879-910. https://doi.org/10.17705/1CAIS.03743

Paananen, H., Lapke, M., & Siponen, M. (2020). State of the art in information security policy development. *Computers & Security*, *88*, 1-14.

Panetta, K. (2021). *A focus on privacy laws, ransomware attacks, cyber-physical systems and board-level scrutiny are driving the priorities of security and risk leaders*. https://www.gartner.com/en/articles/the-top-8-cybersecurity-predictions-for-2021-2022

Repetto, M., Striccoli, D., Piro, G., Carrega, A., Boggia, G., & Bolla, R. (2021). An Autonomous Cybersecurity Framework for Next-generation Digital Service Chains. *Journal of Network and Systems Management*, *29*(4), 1-34. https://doi.org/doi.org/10.1007/s10922-021-09607-7

Simonofski, A., Fink, J., & Burnay, C. (2021). Supporting policy-making with social media and e-participation platforms data: A policy analytics framework. *Government Information Quarterly*, *38*(3), 101590. https://doi.org/https://doi.org/10.1016/j.giq.2021.101590

Siregar, S., & Chang, K.-C. (2019). *Cybersecurity Agility: Antecedents and Effects on Security Incident Management Effectiveness* Pacific Asia Conference on Information Systems (PACIS), China.

Stewart, H. (2022). A systematic framework to explore the determinants of information security policy development and outcomes *Information & Computer Security*, *ahead-of-print*. https://doi.org/doi.org/10.1108/ICS-06-2021-0076

Syed, R. (2020). Cybersecurity vulnerability management: A conceptual ontology and cyber intelligence alert system. *Information & management*, *57*, 1-17. https://doi.org/doi.org/10.1016/j.im.2020.103334

Tallon, P., Queiroz, M., Coltman, T., & Sharma, R. (2019). Information technology and the search for organizational agility: A systematic review with future research possibilities. *Journal of Strategic Information Systems*, *28*, 218-237

https://doi.org/doi.org/10.1016/j.jsis.2018.12.002

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. https://doi.org/doi.org/10.1016/j.cose.2021.102385

Tisalde, S. (2016). *Architecting a cybersecurity management framework: Navigating and travesrsing complexity, ambiguity, and agility* Robert Morris University]. USA.

Valle-Cruz, David , Criado, J. I., Sandoval-Almazán, R., & Ruvalcaba-Gomez, E. A. (2020). Assessing the public policy-cycle framework in the age of artificial intelligence: From agenda-setting to policy evaluation. *Government Information Quarterly*, *37*, 101509. https://doi.org/doi.org/10.1016/j.giq.2020.101509

Zaini, M. K., Masrek, M. N., & Sani, M. K. J. A. (2020). The impact of information security management practices on organisational agility. *Information & Computer Security*, *28*(5), 681-700. https://doi.org/10.1108/ICS-02-2020-0020