12-2-2023

Policy Helix and Antecedents of Cybersecurity Policymaking Agility

Masoud Afshari Mofrad
Macquarie University, Australia, Masoud.afsharimofrad@hdr.mq.edu.au

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

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

Recommended Citation

Afshari Mofrad, Masoud; Abedin, Babak; and Amrollahi, Alireza, "Policy Helix and Antecedents of Cybersecurity Policymaking Agility" (2023). *ACIS 2023 Proceedings*. 4.
https://aisel.aisnet.org/acis2023/4

Policy Helix and Antecedents of Cybersecurity Policymaking Agility

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 cyber threat landscape is constantly changing, and organisations need to stay current with the dynamism of their internal and external environment. One important aspect is to be agile in cybersecurity policymaking (CSPM) to identify signals, devise proper policies, and mitigate risks. However, the literature in this aspect is still understudied, and this paper strives to fill this gap by investigating the notion of agility in cybersecurity policymaking and identifying its antecedents. The paper investigates the importance of agility as a means to counter emerging threats, contributing actionable insights and best practices to the ongoing discourse on cybersecurity policymaking. The findings emphasise the vital role of agility in pursuing cyber resilience and encourage policymakers and stakeholders to embrace this principle. Ultimately, this study deepens the understanding of the agile policymaking process and introduces asset management, vulnerability management, cyber risk management, and robust awareness processes as the antecedents of CSPM agility. The findings can provide insights for both the theory and practice of IS research by introducing the concept of agility in CSPM and identifying its antecedents.

Keywords Information Security, Policy Analysis, Agile Decision Making, Dynamic Cyber Environment

1 Introduction

The question for organisations is no longer "Will we be attacked by hackers?" but rather "When will we be attacked?" Meanwhile, the dark side of cyberspace looms large, with cyberattacks becoming increasingly sophisticated and pervasive. This escalating threat landscape necessitates proactive measures to safeguard the integrity, confidentiality, and availability of critical information systems and data (Dhillon et al., 2021). To do so, organisations need to create a balance between technology and people, and cybersecurity policy is the main tool to integrate the technological and social aspects of the organisation. Such policies should be able to adapt to the changing environment, and the policymaking process should be agile enough to identify signals and formulate/reformulate proper policies to face prioritised threats in a swift manner.

Conventional approaches that rely on reactive measures may be less efficient in combating the dynamic nature of cyber threats, leaving critical infrastructures and sensitive information exposed to potential breaches (Afshari-Mofrad et al., 2022). Therefore, the need for agility in cybersecurity policymaking has never been more urgent. Such changes in the policymaking process require organisational boards to understand that cybersecurity is not a problem that can be solved once and for all; it requires constant effort to mitigate or manage the risk. Although security frameworks typically have policy review cycles, such as annual or biannual, most threats do not adhere to an annual schedule and do not wait for organisations to remediate their policies based on new threats in the following year. This misalignment highlights the pressing need for policymakers to adopt a more agile approach to cybersecurity policymaking, one that can swiftly respond to emerging threats and adapt policies in a timely manner.

Furthermore, the consequences of failing to adapt to this rapidly changing cyber environment are profound. Cyberattacks can result in data breaches, financial losses, damage to an organisation's reputation, and potential legal ramifications (Naseer et al., 2023). The limitations of conventional cybersecurity policies become evident when they struggle to keep pace with the evolving tactics of malicious actors. In this context, the rigidity of traditional policies often obstructs the ability to address emerging threats effectively. These limitations and consequences underscore the urgency of exploring cybersecurity policymaking agility as a strategic imperative for modern organisations.

Although the necessity of agility in cybersecurity endeavours has been mentioned in a few previous studies in the information systems (IS) domain (Afshari-Mofrad et al., 2022; Siregar & Chang, 2019; Tam et al., 2021), there is still a need to focus on identifying the antecedents required to absorb, adapt, and transform in order to respond promptly to major shocks (Boh et al., 2023).

To overcome this shortcoming, this paper delves into the realm of cybersecurity policymaking (CSPM) agility, exploring its significance as a strategic imperative in the modern organisation. By analysing the key factors that shape agility in this domain, we aim to provide a comprehensive understanding of the concept. Moreover, we will investigate the antecedents required to enhance the agility of cybersecurity policymaking, empowering decision-makers to stay current with the ever-evolving threat landscape. Hence, the paper strives to answer the following questions through interviewing cybersecurity experts:

- What does agility in CSPM entail?
- What are the antecedents of cybersecurity policymaking agility?

Through this exploration, we aim to underscore the importance of agility in cybersecurity policymaking as a means to effectively counter emerging threats. By shedding light on best practices and offering actionable insights, this paper aims to contribute to the ongoing discourse on cybersecurity policy, encouraging policymakers and stakeholders to embrace agility as a vital principle in the pursuit of cyber resilience. Our paper contributes to the current IS literature by delving deep into the agile policymaking process and identifying its antecedents. To fulfil this aim, the rest of this paper is organised as follows.

In section 2, we briefly provide some background literature on digital and organisational agility and the policymaking process as the foundations of our work. We then explain the research methodology in section 3. Section 4 presents the findings of the analysis of interview transcripts, and finally, some concluding remarks are provided in section 5.

2 Background

Digital agility is crucial for the survival and prosperity of firms, encompassing the ability to detect, interpret, and respond swiftly to signals in the environment and respond swiftly to both opportunities and threats (Pinsonneault & Choi, 2022). To do so, organisations should be able to react effectively once they have sensed and recognised environmental cues in a thoughtful, timely, and accurate manner (Park et al., 2017). Managers play a vital role in sensing weak signals, analysing them to distinguish between noise and important indicators, prioritising them based on the organisation's crown-jewel assets, and responding in alignment with strategic goals.

This holistic approach to agility necessitates the reconfiguration of organisational processes to achieve the defined objectives. By unpacking the sensing element and understanding its nuances, managers can better equip themselves to navigate the complex landscape of signals, ensuring a proactive and effective response to both opportunities and threats (Queiroz et al., 2018).

Achieving digital agility involves adopting a modular approach to design and leveraging packaged skills. It entails prioritising platforms over traditional linear pipelines, enabling concurrent processes and empowering individuals through data. Additionally, fostering a digital culture that that promotes ambidexterity is crucial (Grover, 2022).

Considering information security as a digital-strategic issue (Dhillon et al., 2021) and acknowledging cybersecurity as a fundamental aspect of an agile organisation (Zaini et al., 2020), one can contend that the foundations of cybersecurity policy agility can be traced back to the literature on digital agility and organisational agility.

In addition, discussing cybersecurity policymaking entails exploring the concept of policymaking processes. Policymaking is a complex interactive and iterative process that involves various stakeholders (Janssen & Helbig, 2018). Although many different models have been developed over the past decades, the longest-standing conceptual framework is the ‘policy cycle’, which involves sequential, cyclical phases or ‘stages’ of organisational problem-solving. Since the advent of this notion, researchers have proposed different stages for inclusion in the cycle. For instance, Lasswell’s (1956) seven-stage model (intelligence-gathering, promotion, prescription, invocation, application, termination, appraisal) differs from that of Brewer’s five/six-stage model (invention/initiation, estimation, selection, implementation, evaluation, termination) (Brewer, 1974). However, the model ultimately has evolved into the now ubiquitous ‘cycle’ construct of five main ‘stages’: agenda-setting, policy formulation, decision-making, implementation and evaluation (Howlett et al., 2017). Thus, in this paper, we have selected the policy cycle as our theoretical lens for analysing the process of policymaking in cybersecurity.

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, Paanen 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, as argued by Valle-Cruz et al. (2020), the policy-cycle in the age of modern technologies, such as AI, should be improved toward a dynamic policy-cycle, where organisations can change direction swiftly according to the major changes in their environment.

Hence, in this paper, we expand upon the concepts of digital and organisational agility and the dynamic policy cycle to conceptualise the idea of agility in cybersecurity policymaking and identify its antecedents.

3 Methodology

As mentioned earlier, the main objective of this study was to investigate the concept of agility in cybersecurity policymaking and its antecedents from the perspective of cybersecurity practitioners. We aimed to understand how this concept resonated with the everyday experiences of the practitioners, how they perceive its importance, and what prerequisites are needed to be in place to achieve agility in CSPM endeavours. We chose to conduct expert interviews because this approach allows our research to be firmly based on current practices and provides comprehensive and detailed information regarding the necessity of agility in cybersecurity policymaking processes (Silverman, 2019).

Hence, the study utilised an inductive and exploratory approach to uncover new and unforeseen discoveries (Gioia et al., 2013). Keeping in line with the exploratory nature of the investigation, we have so far conducted a total of ten semi-structured interviews with experts specialising in cybersecurity. The criterion for participant was a minimum of three years of experience in roles such as CISO, CTO, CIO, or other relevant positions in the field of cybersecurity. Table 1 presents the profile of participants.

	Code	**Work Experience**	**Roles**	**Sector**	**Time**
1	E1	12 years	COO, cybersecurity architect and advisor	Cybersecurity Solutions	46:42
2	E2	15 years	Cybersecurity board advisor, Enterprise Solutions Architect	ICT	56:09
3	E3	18 years	Chief Security Officer, Former CISO	ICT	45:10
4	E4	5 years	Accounts manager/ Former CISO	Cybersecurity solutions	50:28
5	E5	4 years	Cybersecurity Manager	Cybersecurity solutions	56:19
6	E6	22 years	Consultant, Former CISO	Cross industry	48:08
7	E7	11 years	Cybersecurity program manager, former senior cybersecurity manager	Finance	49:33
8	E8	11 years	Cyber Specialist (Data analyst), Former Cybersecurity Solution architect	Telecommunication	48:13
9	E9	22 years	Research Director, Former CTO and CISO	ICT	65:08
10	E10	7 years	CEO, Former Head of Cybersecurity Business Services	Telecommunication	43:45

Table 1. Interviewee Profiles

Eight interviews were conducted online using Microsoft Teams, while the other two interviews were conducted in person. We started our semi-structured interview with eight primary questions. We asked the interviewees questions about their understanding of CSPM agility, how their organisations try to stay current with threats in the cybersecurity landscape, how they learn from past policymaking experiences, how they cope with new types of threat, how their organisation gather intelligence regarding cyber threats, and what challenges they see in being agile in CSPM. The interviews were conducted after obtaining ethical approval from the university's ethics committee.

The online interviews were transcribed by the online transcription service of Microsoft Teams, and the in-person interviews were recorded and transcribed using Microsoft Word Dictate service. The transcripts were carefully reviewed and corrected by the interviewer. The interviews were conducted in May and June 2023. NVIVO12 was utilised to apply inductive coding to the transcripts. Thematic content analysis was employed to analyse the data. The raw qualitative data underwent a systematic transformation into theoretical interpretations following a three-stage process outlined by Gioia et al. (2013).

In the initial stage, we performed preliminary coding to extract primary concepts from the data, sticking closely to the participants' phrasing and terminology. In the subsequent stage, we utilised existing literature and our own expertise to analyse the data and develop explanatory concepts. While we had extracted some concepts from the literature review, we did not confine our primary codes to those concepts, and we extracted emerging concepts as well. By assuming the role of informed researchers, we reanalysed the data using researcher-centric concepts, while also focusing on the underlying core elements of the primary concepts, as well as their similarities and differences. This led us to condense the primary concepts into more abstract second-order themes. Moving on to the third stage, we further scrutinised the data to explore the possibility of aggregating the concepts identified in the second-order themes to construct higher-level and more abstract concepts known as aggregate dimensions. Table 2 demonstrates a few examples of emergent concepts and themes.

Interviewee Quotes	**1st Order Concepts**	**2nd Order Concepts**	**Aggregate Dimensions**
Many companies I have spoken with don't have an asset management system, which I find challenging. If	The necessity of asset management	Asset Management	Antecedents of CSPM agility

you're trying to formulate a cybersecurity policy or strategy and you don't know your assets, that's not going to go too far	before formulating policies		
knowing what the hackers will target, allows you to narrow down your crown jewels and then that's where you can have targeted programmes in keeping those assets safe and away from the hands of the threat actors	The importance of recognising organisations crown-jewels assets		
... organisations need to do a level of threat intelligence at level of threat hunting, understand where their biggest vulnerabilities are, and revise their policies accordingly.	The necessity of vulnerability management prior to policy formulation	Vulnerability Management	

Table 2. Examples of the stages of coding interviews

Although this paper is presented in a linear structure, it is important to note that our entire process of data analysis was iterative, aimed at enhancing insights and improving the generalisability of our findings. In other words, a constant comparative analysis was conducted, and the data analysis was performed after each interview, resulting in the evolution of our understanding and interview questions. Using this approach, four additional sub-questions were added to our primary set of questions over the course of interviews. It is worthy to note that the three stages of the Gioia et al. (2013) process were conducted by the first author and then confirmed by the other co-authors in weekly meetings.

By employing the data structure, we performed a revalidation process to ensure the coherence of the final concepts with the underlying data, thus establishing a clear link between the data, the emerging concepts, and the aggregate dimensions. This approach allowed us to maintain the perspectives of both the informants and the researchers, enabling us to meticulously develop precise and comprehensive definitions of the concepts based on the data. The findings of the analysis of transcripts are provided in section 4.

4 Findings

In this section, we present and substantiate the findings that arose from the analysis of the expert interviews. We aimed to understand what CSPM agility entails and what antecedents are required to be agile in this domain. The findings demonstrate that agile CSPM can be interpreted as a dynamic policy helix where data and information from both internal and external environment of the organisation can affect policy objectives or tools. Additionally, to be agile in CSPM, it is required to have asset management, vulnerability management, risk identification, and change management affairs in place. These findings are elaborated in more detail in this section.

4.1 Unravelling the Essence of CSPM Agility: A Closer Look

Policymaking is one of the crucial first steps in the realm of cybersecurity. Organisations must be agile to react promptly and proactively to emerging threats because threat actors thrive in this domain, consistently outpacing the learning curve of cybersecurity vendors through their rapid innovation. Hence, and firstly, it is imperative to recognise that delaying the process of policy update until a set deadline, such as annual or biannual review, might not be sufficient due to the dynamic nature of the threat landscape. For instance, Expert 1 noted that "*... and obviously we know that most risks, you know, don't follow an annual process, they change very fluidly in the environment*".

Moreover, when new technologies emerge, attempting to retrofit existing policies often proves ineffective. Applying outdated policies to new technology simply does not work. In this regard, policies should not be regarded as the ultimate objective. Policies are not an ideology that cannot be changed; they should instead be perceived as a means to facilitate the harmonious integration of technology and people, and they should be updated according to the changes in the risks and opportunities. That is why the notion of CSPM agility is important.

Based on the analysis of interview transcripts, CSPM agility can be examined from two perspectives. First, the cybersecurity strategy and related policies should be adapted to the changes in the cyberthreat landscape. For instance, Expert 7 mentioned that "*... You will want to make sure that any changes in your environment that might affect your policy or strategy, should be considered in reformulating the policy accordingly, and re-prioritise the policy and resources required for it*". To effectively respond to changes in the cyberthreat environment, organisations must gather and analyse data, and develop robust intelligence. This capability can be obtained through outsourcing or by building in-house expertise, depending on the organisation's size and cybersecurity maturity. This way, organisations can be aware of the possible attack scenarios and proact upon it.

Second, organisations need to tailor their cybersecurity policies based on their current internal status, specifically the maturity of their technologies and systems. For example, expert 6 explained that "*... when you start to operationalise those policies, there is that element of what's actually going to work in practise and where you may come across legacy systems, where some of those policies may not be able to be applied straight away .... How do you come up with workarounds and other compensating measures and controls for a period of time and then start over time to build on that level of maturity and capability that you build and ultimately reach the policy requirements that you're after within an organisation ...*". In this perspective, it is crucial to modify policies to align with the characteristics of the organisation and receive feedback at each stage of the policymaking process. Therefore, CSPM agility encompasses both internal and external perspectives within organisations.

The data and information gathered from both internal and external environments of the organisation needs to be synthesised and filtered according to the priorities of the organisation. The priorities may arise from the intersection of asset management and vulnerability management practices. After analysing the need for change in the policies as a new agenda in the policymaking process, like any other organisational issue, the agenda should be in line with the priorities and risk appetite of the business. As noted by Expert 8, it is important to know "*... What are your business risks that you're trying to mitigate, and the way that you express those, is by effectively implementing a policy...*". Hence, based on the risk appetite of the organisation, the identified signals from both internal and external environments are filtered and sent to the next stage, which is policy formulation and decision-making, to consider a policy change to accept, avoid, mitigate, or transfer the cybersecurity risk.

Depending on the novelty of the cyber risk, the current policies in effect, and the risk threshold of the organisation, there may be a need to formulate new policies or incorporate new policy tools into the existing ones. In this regard, Expert 8 remarked that "*... and below that you then got practises, tools, standards and so forth. So, if you change tools of existing policies, that shouldn't have an impact on your policy*". If the decision is influenced by feedback regarding non-compliance with existing policies by employees, it is crucial to ensure that employees are familiar with the existing policies and procedures. If, despite their awareness, the non-compliance rate remains high, there may be a necessity to reformulate that policy. Finally, another source of change that might need agile decision-making is compliance with new government legislation or regulations.

Agility is not required for policy development only, but it also needs to be extended to policy dissemination and implementation. In certain cases, the policy might be formulated wisely, but the implementation may encounter challenges. It is vital to swiftly assess the effectiveness of the implementation stage and make changes if necessary. As addressed by Expert 1, changing technical policies might be easier to implement, because "*... they have less effect on the end user but in cases that the end user ... requires behavioural change, the implementation needs further attention*". Another crucial aspect of agile policy implementation is coordination and cooperation with other business departments. Since policy objectives or tools may undergo changes, it is vital to ensure that cybersecurity efforts are not perceived as obstacles to the business, but rather, as Experts 2 and 4 mentioned, "*... an enabler for the business to operate safely*." Policy awareness also holds significance in all cybersecurity implementation endeavours, particularly in agile policymaking. For example, Expert 1 shared a case of an incident where "*... There was nothing wrong with any of our control implementation ... so this one* *was really about security awareness and training, so we conducted additional security awareness training for them and also bought an awareness training platform.*"

The final step is to regularly evaluate existing policies and procedures based on the changes in internal and external environments, policy learning experiments, and previous successful and unsuccessful incidents and attacks. According to the experiences of Expert 2, 'top table experiments' could serve as valuable sources of insight for policy learning. In these experiments, the executive team of the organisation is gathered in a room, presented with a cyber-attack scenario, and asked to react based on the scenario and their current policies. Expert 2 highlights that "*100% of the time there are good learnings, and it is the fastest way to make someone learn... they'll immediately see a learning opportunity.*" Furthermore, based on the experiences of Expert 1, "*threats and incidents will be the primary source for policy making in the future*," which is the result of learning from previous policy endeavours.

Figure 1 provides a visualisation of the process of agile cybersecurity policymaking. The crucial aspect is that this process is dynamic and ongoing, and organisations cannot solely rely on adopting a policy from NIST, ISO, or SABSA frameworks without taking further action. To achieve this, it is essential to consider antecedents, which will be further elaborated upon in the next section.

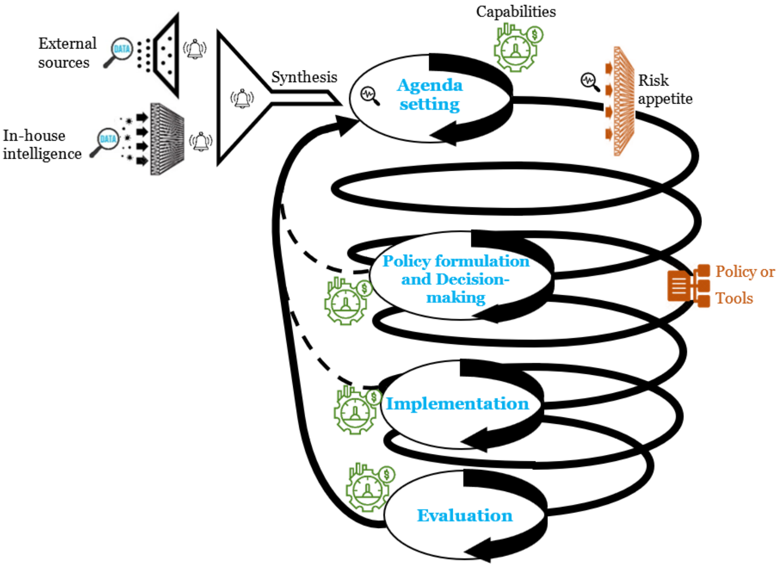

Figure 1. The dynamic cybersecurity policy helix (inspired from Valle-Cruz et al. (2020))

As the figure summarises the prior discussion, the intelligence for policy formulation/reformulation can come from both internal and external sources and create the basis for agenda-setting according to the risk appetite of the organisation. Then, policymakers will decide if there is a need for formulating a new policy or changing the existing policy tools. The changes need to be implemented and evaluated. The bold arrows indicate that evaluation can occur locally at each stage based on the new intelligence (for instance, at the implementation phase), and the dashed lines indicate that the results of the evaluation might return to the agenda-setting to update the policy in harmony with other policies or strategies of the organisation.

4.2 The Antecedents of Cybersecurity Policymaking Agility

Agility in cybersecurity policymaking is influenced by various antecedents that shape its implementation and outcomes. Analysing the interview data shows that these antecedents encompass a range of factors, including the mindset of decision-makers, stakeholder collaboration, policy intelligence, and adaptability to evolving threats. Understanding these antecedents is crucial for policymakers and organisations seeking to foster agility in their cybersecurity policy development processes. By examining and addressing these factors, policymakers can enhance their ability to respond swiftly and effectively to emerging cyber threats and ensure the resilience of their cybersecurity frameworks. Our analysis of the interviews revealed five significant antecedents, which are briefly elaborated upon below.

Awareness: Before employing an agile approach to CSPM, it is important that policymakers are aware of the changes in the cyber threat landscape and the necessity of adapting to the dynamic environment. Expert 4 asserted that "*... in my experience, the boards mostly don't have that ... experiences, that is why the first thing organisation should possess to be agile in policymaking is an informed board*." Also having a forward-looking cybersecurity team can play an important role in agile policymaking. As an example, Expert 6 emphasised that "*You need sort of a strategic mindset within your team so that they don't just think about the more immediate problem that's in front of them and a particular system or environment that's not adhering to a policy, ... but they need to think more creatively and a little bit outside of the box in terms of, well, what are some of the different ways that we can introduce compensating controls or uplift some of the controls within the environment to start to move towards that policy requirement?*."

Before implementing policy changes that may not function effectively, it is crucial to ensure that our employees are both informed about and adequately trained on these policies. It is especially important in cases where policies or procedures might change faster than normal, and as Expert 1 asserted, "*most of the times the technical team, the, the IT team knows what's going on, but our employees don't. So, if we cannot keep them updated, we will always call them the weakest link*." Also, expert 3 emphasised the prominence of policy awareness and training programs to reach a common language inside the organisation. The Expert shared an experience: "*I go to a firm, and they say: we can't do this thing because of X. I ask why not? and they say see, it is internal policy. Then you speak to five other people in the same organisation, and they say no, it's not. ... And then, everybody tries to find out where the policy is. Then maybe it is in there. But you look at the word in and the word in slightly ambiguous. So, I'd say that's probably the first piece that I think we massively have an issue with, is that understanding ... that is why training and awareness is important*". The iterative nature of agile CSPM increases the importance of training and awareness before and after employing agile approach for the CSPM.

Asset management: is the systematic process of identifying, organising, and managing the various assets within an organisation's information technology infrastructure. It helps organisations in identifying and prioritising crown-jewels assets and data. Expert 7 mentioned that "*Many companies I have spoken with don't have an asset management system, which I find challenging. If you're trying to formulate a cybersecurity policy or strategy and you don't know your assets, that's not going to go too far*." Also, Expert 2 mentioned that "*knowing what the hackers will target, allows you to narrow down your crown jewels and then that's where you can have targeted programmes in keeping those assets safe and away from the hands of the threat actors*."

Change management: Since CSPM agility might lead to change especially regarding the behaviour of employees, devising a change management programme can play a vital role. Expert 4 asserted that "*change management is necessary concerning attitudes, understanding, and education. All these aspects demand the entire organisation to collaborate harmoniously, comprehending the risks*." Expert 3 also mentioned that "*I think that's, you know, achieved through your appropriate change management and effective communication to really drive home the why is something changing or why something is being updated and to what end. So, is it a risk that you're mitigating? Is it something that you're doing to further streamline your operations? What is it that is being updated and how do you reflect that, you know, in your communication and bringing people on board?*".

Vulnerability management: can be referred to a structured and systematic approach to identifying, assessing, prioritising, and mitigating vulnerabilities within an organisation's IT infrastructure. It is a great idea to implement in the organisation because vulnerabilities are never ending, new systems are always put in the organisation, and there are always legacy systems in the organisation. Expert 8 mentioned that "*when you look at vulnerability in a strictly kind of IT sense, that's about running vulnerability scans across your organisation, getting that data back and then effectively prioritising how you're going to mitigate those vulnerabilities to prevent them from becoming risks*." Also, Expert 6 addressed the importance of vulnerability management by asserting that "*...organisations need to do a level of threat intelligence at level of threat hunting, understand where their biggest vulnerabilities are*".

Cyber risk management: Another important aspect is the continuous management of cyber risks rather than solely focusing on their identification. It is crucial to enable teams to raise cyber security risks when necessary and have a framework in place that facilitates the proper qualification and escalation of these risks to the appropriate level. Depending on the nature of the risks, they may be accepted, avoided, transferred, or mitigated. Therefore, as Expert 9 noted, "*there should be a well-*

defined mechanism within the cyber security domain to effectively manage these risks through a framework, ensuring seamless integration with enterprise risk management".

Having a risk committee and a chief risk officer could help organisations to be agile in CSPM. As Expert 8 noted "*… for me, that's about having the right corporate structure in place. So, you've got a risk committee or risk group that looks at this holistically. You know, chief risk officers are a relatively sort of new concept …*". Expert 9 also mentioned the importance of adding a Chief Risk Officer position to the structure of the organisation. The Expert emphasised that "*in terms of what's needed, the idea of a CRO … who is more focused on the broad security of the organisation*." Additionally, delegation of some policymaking endeavours to lower layers of the organisation and evading from sending all decisions to be made at the board level can be helpful in improving the speed of policymaking. Expert 1 asserted that "*without delegating your policy making down to the right levels, there will be an inability to adapt to changes effectively*."

By addressing these antecedents, organisations can enhance their agility in cybersecurity policymaking and improve their ability to respond to evolving threats effectively.

5 Discussion and Concluding Remarks

A key factor for organisations' success in hypercompetitive environments is organisational agility, which pertains to the organisation's ability to sense relevant change and respond readily to market opportunities. One vital aspect of organisational agility is being agile in cybersecurity matters (Zaini et al., 2020). Therefore, it is crucial to be agile in the face of new, unknown, or unexpected attacks in the cybersecurity context to effectively mitigate risks. Agility enables the organisation to continuously enhance and redefine its ability to detect and respond to these new, unknown, or unexpected attacks (Siregar & Chang, 2019). However, the question arises as to how organisations should react or proact to their internal and external cyberthreat environment, and what prerequisites are required?

To address these questions, we conducted an empirical study by interviewing cybersecurity experts. The main contribution of the current study is that there is a need for a systematic approach to continuously analyse changes in the cyberthreat landscape. This involves prioritising internal and external cybersecurity risks based on their nature, the organisation's critical assets (aligned with business needs) and identifying critical vulnerabilities. These prioritised threats should then be integrated into the policymaking process, allowing for agile decision-making.

The required data for agile policymaking might come from external sources (such as vendors, consultants, or even start-up firms that are forming in the cybersecurity ecosystem) or internal intelligence gathering. Building internal capabilities or outsourcing parts of the cybersecurity services to vendors depends on the size, cybersecurity maturity, and budget of the organisation (Keramati et al., 2016). The synthesised data and information should then be analysed against the risk appetite of the organisation, and the prioritised cyber risks would provide a good foundation for reformulating the policies. This is in line with the findings of Naseer et al. (2021) and Keramati et al. (2012) who emphasise on the importance of threat intelligence and analysing it especially in the context of broader business.

We argue that in some cases, policy changes may not be necessary, but rather adjustments to tools and standards. These changes must be implemented in the organisation's processes, requiring training and awareness affairs. Bélangera et al. (2017) have also emphasised the cruciality of the awareness in cybersecurity policy endeavours. In the dynamic cybersecurity policy-cycle, evaluation of policies could occur at each stage or after implementation of policies, so that the learning from the parts that might not work properly can help policymakers to make changes accordingly. Our analysis revealed that the ultimate objective of CSPM agility is to achieve business resilience. This finding is consistent with those of Loonam et al. (2020) who argue that cyber-resiliency is an important aim for leaders across the organisation.

To be able to be agile in CSPM, there are antecedents. These antecedents encompass several key factors. Firstly, having an informed board and decision-makers with a strategic mindset is crucial for effective policymaking. Secondly, implementing asset management practices allows organisations to prioritise and protect their critical assets. The importance of asset management in cybersecurity endeavours is highlighted in cybersecurity frameworks such as NIST, and has been considered as an important capabilities in cybersecurity domain (Malatji et al., 2022). Thirdly, change management processes, including effective communication, help foster a collaborative and risk-aware organisational culture. This finding is consistent with those of Uchendu et al. (2021) who found that change management is one of the most important factors to build a cybersecurity culture. Fourthly, vulnerability management ensures the identification and mitigation of vulnerabilities in an organisation's IT infrastructure. The finding continues the findings of Syed (2020) concerning the gathering of intelligence from various sources to identify the cybersecurity vulnerabilities of the organisation. Fifthly, continuous risk management and integration with enterprise risk management frameworks enable the proactive management of cybersecurity risks. Additionally, policy awareness and training programs are essential for ensuring employees are well-informed and compliant with policies. This is in line with the findings of Wong et al. (2022) who argue that improved policy awareness of employees can increase their policy compliance. Finally, establishing a suitable corporate structure with a risk committee and a Chief Risk Officer enhances the organisation's overall security posture and decision-making capabilities.

These findings have both theoretical and practical implications. The paper contributes to the IS theory by delving deeper into the concept of cybersecurity policymaking agility and introducing the cybersecurity policy helix. It also explains the agile process of policymaking in organisations and highlights the necessary changes that need to be made in the policymaking process.

Additionally, the paper utilises empirical data to identify the antecedents of CSPM agility. Our investigation into the antecedents of cybersecurity policymaking agility opens the door to reimagining and enhancing the conventional policy cycle. The factors we have identified as crucial elements for agile cybersecurity policymaking are not only pertinent for organisational resilience but can also serve as foundational principles for a dynamic policy cycle. By incorporating these key elements into the existing policy cycle model, we have the potential to create a more responsive and adaptable framework. This revised model would offer decision-makers the tools they need to continuously evaluate and prioritise cybersecurity threats, seamlessly integrating them into the policymaking process. Such a model not only aligns policy formulation with the ever-evolving cybersecurity landscape but also fosters a culture of proactive risk management within organisations.

As our study has highlighted the key antecedents necessary for agile cybersecurity policymaking, it naturally raises questions about their integration into established policy models. The dynamic policy cycle that we propose is underpinned by the notion that an agile mindset of decision-makers, robust asset management, effective risk management, and vulnerability management are essential components. This concept challenges traditional static policy frameworks by advocating for a more responsive, continuously adaptive approach. By acknowledging these theoretical implications, we embark on a path to reshape not only how organisations navigate the complex cybersecurity landscape but also how policy cycles are conceived and applied.

From a practical perspective, the novel notion of agility in cybersecurity policies draws the attention of practitioners to the necessity of reformulating policy objectives or tools according to the changes in their internal and external environment. Moreover, introducing the antecedents of agile CSPM can assist decision-makers in taking into account factors such as the intersection of asset management and vulnerability management, helping them prioritise the organisation's assets and vulnerabilities that should be managed to keep those assets safe.

Further research is still needed to identify the capabilities that organisations need to be agile in their cybersecurity policy endeavours and to demonstrate how CSPM agility can improve the cyber resilience of firms.

6 References

Afshari-Mofrad, M., Abedin, B., & Amrollahi, A. (2022). Old Keys May Not Open New Doors: The Necessity of Agility in Cybersecurity Policymaking. Australasian Conference on Information Systems, Melbourne, Australia.

Bélangera, F., Collignon, S., Enget, K., & Negangard, E. (2017). Determinants of early conformance with information security policies. *Information & Management*, *54*, 887–901. https://doi.org/10.1016/j.im.2017.01.003

Boh, W., Constantinides, P., Padmanabhan, B., & Viswanthan, S. (2023). Building digital resilience against major shocks. *MIS Quarterly*, *47*, 343-360.

Brewer, G. D. (1974). The policy sciences emerge: to nurture and structure a discipline. *Policy Sciences* *5*, 239-244.

Dhillon, G., Smith, K., & Dissanayaka, I. (2021). Information systems security research agenda: Exploring the gap between research and practice. *The Journal of Strategic Information Systems*, *30*(4), 101693. https://doi.org/10.1016/j.jsis.2021.101693

Gioia, D. A., Corley, K. G., & Hamilton, A. L. (2013). Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. *Organizational research methods*, *16*(1), 15-31.

Grover, V. (2022). Digital agility: responding to digital opportunities. *European Journal of Information Systems*, *31*(6), 709-715.

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/10.1111/1467-8500.12191

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

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.

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.

Loonam, J., Zwiegelaar, J., Kumar, V., & Booth, C. (2020). Cyber-resiliency for digital enterprises: a strategic leadership perspective. *IEEE Transactions on Engineering Management*, *69*(6), 3757-3770.

Malatji, M., Marnewick, A. L., & Von Solms, S. (2022). Cybersecurity capabilities for critical infrastructure resilience. *Information & Computer Security*, *30*(2), 255-279.

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/10.1016/j.ijinfomgt.2021.102334

Naseer, H., Desouza, K., Maynard, S. B., & Ahmad, A. (2023). Enabling cybersecurity incident response agility through dynamic capabilities: the role of real-time analytics. *European Journal of Information Systems*, 1-21.

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

Park, Y., El Sawy, O. A., & Fiss, P. (2017). The role of business intelligence and communication technologies in organizational agility: A configurational approach. *Journal of the Association for Information Systems*, *18*(9), 1.

Pinsonneault, A., & Choi, I. (2022). Digital-enabled strategic agility: it's time we examine the sensing of weak signals. *European Journal of Information Systems*, *31*(6), 653-661. https://doi.org/10.1080/0960085X.2022.2027824

Queiroz, M., Tallon, P. P., Sharma, R., & Coltman, T. (2018). The role of IT application orchestration capability in improving agility and performance. *The Journal of Strategic Information Systems*, *27*(1), 4-21.

Silverman, D. (2019). Interpreting qualitative data. *Interpreting Qualitative Data*, 1-568.

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/10.1016/j.giq.2021.101590

Siregar, S., & Chang, K. (2019). *Cybersecurity Agility: Antecedents and Effects on Security Incident Management Effectiveness* Pacific Asia Conference on Information Systems (PACIS), https://aisel.aisnet.org/pacis2019/175

Syed, R. (2020). Cybersecurity vulnerability management: A conceptual ontology and cyber intelligence alert system. *Information & Management*, *57*(6), 103334. https://doi.org/10.1016/j.im.2020.103334

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/10.1016/j.cose.2021.102385

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

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/10.1016/j.giq.2020.101509

Wong, L.-W., Lee, V.-H., Tan, G. W.-H., Ooi, K.-B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management*, *66*, 102520. https://doi.org/10.1016/j.ijinfomgt.2022.102520

Zaini, M. K., Masrek, M. N., & Abdullah Sani, M. K. J. (2020). The impact of information security management practices on organisational agility. *Information & Computer Security*, *28*(5), 681-700.

Copyright