MIS Quarterly Executive

Volume 23 | Issue 4 Article 3

December 2024

Adopt Agile Cybersecurity Policymaking to Counter Emerging Digital Risks

Masoud Afshari-Mofrad

Alireza Amrollahi

Babak Abedin

MIS Quarterly Executive

Adopt Agile Cybersecurity Policymaking to Counter Emerging Digital Risks

Policy formulation is a cornerstone in cybersecurity management, and in the ever-evolving cyber landscape, the policymaking process must be agile and adaptable. This crucial imperative introduces fresh challenges to an already intricate governance environment. From in-depth interviews with cybersecurity practitioners, we identify four primary cyber risk areas that underscore the need for agility in policymaking. Based on insights from our interviewees, we provide actionable recommendations for enhancing the agility and adaptability of cybersecurity policymaking processes.[1]

Masoud Afshari-Mofrad
Macquarie Business School (Australia)

Alireza Amrollahi
Macquarie Business School (Australia)

Babak Abedin
Macquarie Business School (Australia)

The Need for Agility and Adaptability in Formulating Cybersecurity Policies

In the constantly evolving cybersecurity landscape, it is crucial to remain vigilant and proactively address both emerging threats and the potential of new technologies to enhance organizational digital defenses. The consequences of not maintaining adequate internal controls can be severe, as SolarWinds (a U.S. information technology firm) discovered after it was targeted in 2019 by a Russian-backed hacking group in one of the worst cyber-espionage incidents in U.S. history. Subsequently, the U.S. Securities and Exchange Commission alleged in a lawsuit that the firm had committed fraud and failed to maintain adequate internal controls for years prior to the hack. SolarWinds had not reformulated its password policy to adapt to new technologies.[2]

Consider, also, the example of a new cybersecurity policy not working as intended, such as the use of passwords for accessing a hospital network, resulting in nurses writing their passwords on a piece of paper and leaving them by their computers, thus compromising

1 Mary Sumner is the accepting senior editor for this article. The authors thank Mary and the members of the review team for their thoughtful feedback and guidance throughout the review process.

2 For more information, see *SEC sues SolarWinds over Massive Cyberattack, Alleging Fraud and Weak Controls*, CNBC, October 31, 2023, available at https://www.cnbc.com/2023/10/31/solarwinds-defrauded-investors-about-cybersecurity-sec-alleges.html.

DOI: 10.17705/2msqe.00102

network security.[3] It is anyone's guess how long it would take policymakers to recognize the inefficacy of such policies and take corrective action.

To address the dynamic shifts in the cybersecurity environment, organizations need to adopt agility and adaptability in policymaking—i.e., swiftly adjusting to newly surfaced threats and emerging technologies to effectively mitigate cyber risks.[4] However, from our review of the literature on cybersecurity management and discussions with industry experts, we found that most firms tend to be static and reactive in response to changes in the cybersecurity environment.[5] They often only reformulate their cybersecurity policies after experiencing an attack or when industry best practices (such as the NIST Cybersecurity Framework or the ISO 27001 international information security standard) update their policies.[6] Meanwhile, the evolving cyber threat landscape doesn't adhere to an annual schedule, and doesn't wait for best practices to prescribe new policies and procedures. Such a reactive approach toward new cybersecurity threats increases the risk of being attacked and gives rise to the question: *In what ways do emerging risks require more agile and adaptive cybersecurity policymaking processes?*

To answer this question, we reviewed how nine Australian organizations are adopting adaptive cybersecurity policymaking by interviewing, in-depth, a cybersecurity expert from each organization. The interviewees included chief information officers (CIOs), chief information security officers (CISOs), chief technology officers (CTOs) and other relevant positions in the field of cybersecurity. Quotes below from the nine interviewees are attributed to Practitioner, 1, Practitioner 2, etc. The organizations represented a range of industries, including technology, finance, communications and consulting. (See the Appendix for more details, which also provides detailed information on our research methodology.)

From the interviews, we identified four pivotal risk areas driving the need for agile and adaptive cybersecurity policymaking: 1) legacy systems, 2) emerging technologies, 3) attacks via third parties, and 4) disruptive external events. Drawing on insights from the interview data, in this article, we explore these risk areas and describe how organizations must adeptly consider them in their cybersecurity policies. Moreover, our findings indicate that despite the common perception of such policies being stable and inflexible, the dynamic nature and inherent risks within both the internal and external cybersecurity landscape demand a more agile approach. Based on our analysis, we provide eight recommendations (two for each risk area) for policymakers to enhance the speed of the cybersecurity policymaking process. Before describing the four risk areas and how policymakers should adeptly consider them, we first provide an overview of the conventional cybersecurity policymaking process.

Conventional Cybersecurity Policymaking Process

Despite the critical significance of cybersecurity policies, researchers have found that many organizations neglect their development.[7] Our interviews with cybersecurity experts generated two key insights into cybersecurity policymaking: 1) the evolution of the policymaking process within organizations over time and 2) the catalysts that expedite this process. These insights provide the context for our discussion on the imperative of agility and adaptability in the policymaking process in response to emerging cybersecurity threats and our recommendations for speeding up the pace of this process.

3 Hedström, K, Karlsson, F. and Kolkowska, E. "Social Action Theory for Understanding Information Security Non-Compliance in Hospitals: The Importance of User Rationale," *Information Management & Computer Security* (21:4), October 2013, pp. 266-287.

4 Janssen, M. and Van der Voort, H. "Agile and Adaptive Governance in Crisis Response: Lessons from the COVID-19 Pandemic." *International Journal of Information Management* (55:1), June 2020, Article 102180.

5 Naseer, A., Naseer, H., Ahmad, A., Maynard, S. B. and Adil, M. S. "Real-Time Analytics, Incident Response Process Agility and Enterprise Cybersecurity Performance: A Contingent Resource-Based Analysis," *International Journal of Information Management* (59:8), August 2021, Article 102334.

6 Afshari-Mofrad, M., Abedin, B. and Amrollahi, A. "Developing Dynamic Capabilities to Increase Cybersecurity Policymaking Agility and Resilience," *Proceedings of the 28th Pacific Asia Conference on Information Systems*, AIS Electronic Library (AISeL), July 2024, pp. 1-9.

7 See. For example, Paananen, H., Lapke, M. and Siponen M. "State of the Art in Information Security Policy Development," *Computers & Security* (88), September 2019, Article 101608.

Evolution of the Policymaking Process

A review of the literature and practical forums reveals that numerous strategies and methods exist for the development of cybersecurity policies. These approaches and methods have become increasingly intricate over time, mirroring advancements in systems and organizations.[8] One approach is the information security policy architecture (ISPA), which requires policies to be initially formulated at the highest organizational level. Subsequently, these strategic-level policies can be elaborated upon or distributed to the tactical and operational levels in the form of more detailed policies.[9]

Each approach proposes a distinct method to outline the process of cybersecurity policy development. One prevalent strategy involves integrating the policy development process into a broader lifecycle model, a perspective widely acknowledged and detailed in numerous textbooks that provide guidance on personnel, tasks and outcomes.[10] Despite the existence of various models, including the *garbage can model, multiple streams* and the *advocacy coalition framework*, among others, the most enduring conceptual framework is the *policy cycle*.[11] This framework encompasses sequential, cyclical phases or stages of organizational problem solving, and has evolved to become the ubiquitous "cycle" construct with five main stages: 1) agenda-setting, 2) policy formulation, 3) decision-making, 4) implementation, 5) and evaluation. Though this model provides a comprehensive understanding of the cybersecurity policymaking process, it has faced criticism for its static nature and a lack of timely updates.[12]

Catalysts Expediting the Policymaking Process

The results of the interviews revealed that there are a few catalysts that trigger changes in static policies within organizations, albeit rarely and sporadically. One of the most prominent is the occurrence of cyber incidents. Many organizations do not initiate the revision or adaptation of their cybersecurity policies until they experience a direct threat or breach. This reactive approach underscores the need for more proactive measures. In addition to incidents, changes in laws and regulations also act as significant catalysts. Organizations often rely on the fear of enforcement or compliance requirements to spur action, rather than make policy changes proactively.

Such catalysts highlight the importance of shifting from a reactive to a more anticipatory approach in cybersecurity policymaking. For state-of-the-art cybersecurity policy development, researchers and policymakers should focus more on customized and organization-specific cybersecurity needs and try to incorporate contextual factors of each industry or organization into policies.[13] Different types of policy are needed by organizations operating in static or volatile environments; the former might be able to use rule-based static policies, while the latter may need to adopt a dynamic approach that allows adaptable decisions based on the new situations.[14] This dynamic approach requires an agile, iterative policymaking process that detects and takes account of continuous changes in cybersecurity threats and opportunities, swiftly makes policy decisions and seamlessly integrates these decisions into organizational processes while continually evaluating and refining the policies with speed and flexibility.[15] A "one-size-fits-all" policy might not be suitable, and determining the architecture and scope of the policies for each organization needs further investigation in future research. We strive to shed light on this topic in this study by emphasizing

8 Klaić, A. "Overview of the State and Trends in the Contemporary Information Security Policy and Information Security Management Methodologies," *Proceedings of the 33rd International Convention MIPRO*, IEEE, June 2010.

9 Von Solms, R., Thomson, K-L. and Maninjwa, P. M. "Information Security Governance Control through Comprehensive Policy Architectures," *Proceedings of 2011 Information Security for South Africa*, IEEE, 2011.

10 Afshari-Mofrad, M., Abedin, B. and Amrollahi, A., op. cit., July 2024.

11 Howlett, M., McConnell, A, and Perl, A. "Moving Policy Theory Forward: Connecting Multiple Stream and Advocacy Coalition Frameworks to Policy Cycle Models of Analysis," *Australian Journal of Public Administration* (76:1), March 2017, pp. 65-79.

12 Afshari-Mofrad, M., Abedin, B. and Amrollahi, A. "Policy Helix and Antecedents of Cybersecurity Policymaking Agility," *Proceedings of the 34th Australasian Conference on Information Systems*, AIS Electronic Library (AISeL), December 2023, pp. 1-12.

13 Afshari-Mofrad, M., Abedin, B. and Amrollahi, A., op. cit., July 2024.

14 Ibid.

15 Afshari-Mofrad, M., Abedin, B. and Amrollahi, A. "Old Keys May Not Open New Doors: The Necessity of Agility in Cybersecurity Policymaking," *Proceedings of the 33rd Australasian Conference on Information Systems: The Changing Face of IS*, AIS Electronic Library (AISeL), December 2022, pp. 1-11.

the need for agility and adaptability in the policymaking process.

Key Cyber Risk Areas Driving the Need for Agile Policymaking

While there has been increased awareness of the importance of agility in cybersecurity management in recent years, our findings reveal that the policymaking process often remains inert and bureaucratic and requires a more dynamic and adaptive framework to effectively tackle evolving cybersecurity threats. Our interviewees consistently emphasized a range of risks that demand adaptive policy initiatives, and we categorized these risks into four key areas: 1) legacy systems, 2) emerging technologies, 3) attacks via third parties, and 4) disruptive external events. The first risk area is internal and the other three involve external factors. Each risk area requires a more agile and adaptable approach to cybersecurity policymaking.

Cyber Risk Area 1: Legacy Systems

Organizations' legacy systems emerged as a significant internal cyber risk, posing intricate challenges that demand careful consideration. Legacy systems are often remnants of earlier technological eras, and it may be difficult to align them seamlessly with contemporary best-practice cybersecurity policies. The evolving landscape of cybersecurity standards, exemplified by frameworks like NIST and ISO 27001, has progressively raised the bar for safeguarding digital assets and sensitive information. However, the continuing use of legacy systems, designed with outdated security measures, introduces a potential misalignment that can give rise to cyber risks.

The misfit between legacy systems and current cybersecurity policies comes sharply into focus when organizations face heightened vulnerability. The reluctance or inability to upgrade these systems to meet modern security standards or tailor the cybersecurity policies based on the status of the legacy systems can create a cybersecurity gap, leaving organizations susceptible to exploitation by malicious actors.

One of our interviewees (Practitioner 4) shared insights gained from steering two banks in London and Melbourne toward internet banking. She emphasized the imperative for agility and adaptability in cybersecurity policies, particularly in understanding the trajectory of the business and being well-versed in key digital transformation initiatives and strategies. The banks wanted to deliver their services online while ensuring the security of their customers' assets. This required a collaborative effort between cybersecurity and business personnel to discern essential non-negotiable patterns and policies to embed into business solutions. The banks also needed to consider the policies and procedures that would allow some flexibility or incorporate compensating measures. The primary challenge they faced was their legacy systems, which operated on outdated technologies, as Practitioner 4 explained:

> *"You can look at what best practice is around on patching and updating those legacy environments, but you cannot necessarily enforce those policies on day one … because [the legacy systems] cannot handle the updates and patching that is required. So, this is where agility becomes crucial, requiring the introduction of compensating measures and policies. … Then over time, you should start to replace that legacy environment with more contemporary solutions, be it cloud-based or other cutting-edge alternatives, to start to reduce those risks and exposures, acknowledging that, from day one, the legacy systems may not conform to these new policies."*

In the scenario described by Practitioner 4, rather than suggesting policies and procedures that may not function optimally on legacy systems, the cybersecurity team should embrace an agile approach, offering viable solutions that can effectively meet both security and business requirements. This requires the cybersecurity team to adopt an agile and adaptive mindset, enabling it to align its security solutions and policies seamlessly with the evolving needs of the business.

Cyber Risk Area 2: Emerging Technologies

Emerging technologies such as artificial intelligence or quantum computing have given

rise to new cyber threats such as impersonation through deepfakes or voice assimilation.[16] Hackers exploit these tactics to portray themselves as legitimate users, thus deceiving employees and gaining access to an organization's critical digital assets. This escalating threat landscape requires proactive measures and decision agility to safeguard the integrity, confidentiality and availability of essential information systems and data.[17] An important aspect of agility in this context is policymaking agility, as outlined by Practitioner 6:

> *"Recently, hackers [have been] using AI to imitate voice and [to create] deepfakes for phishing and social engineering [these so-] called multi-modal attacks … can be fuel on the fire. For instance, they can imitate the voice of a manager and call the employee to get the password. So, organizations should devise proper policies and procedures for these new threats."*

Integrating artificial intelligence in multi-modal attacks, such as voice imitation and deepfakes, introduces a new layer of complexity to phishing and social engineering. Practitioner 6 underscored the importance of policymaking agility in response to these evolving threats, emphasizing the need for organizations to devise and implement updated policies and procedures tailored specifically for combating these innovative techniques.

Prior cybersecurity policies might need to be updated in light of the risks arising from the deployment of a new technology, or there might be a need to formulate and introduce a new set of policies, as highlighted by Practitioner 8:

> *"If someone is calling you as an employee and even though [it] sounds legit, if they are asking you to do something, you shouldn't do that on the phone; there should be policies and steps in place to verify what you are being asked to do before you do that. If someone is calling you to transfer a certain amount of money or provide user name and password, there should be official policies."*

However, as pointed out by Practitioner 7, most organizations have a reactive approach toward updating their policies, while the dynamics of the cybersecurity environment demand a proactive approach. He stated that:

> *"Some of the reactions to the new threats really depend on having a massive data breach leveraging that specific technique to get into [the] environment, whether it's deepfake or somebody changes their voice or mimics your voice. And the moment that happens, then companies start thinking that we should have a policy, or we should implement that control to make sure that we are protecting ourselves."*

This quote emphasizes the inherent risks associated with a reactive stance, where policy adjustments and control implementations primarily occur in response to a security incident. Waiting until after an event has occurred may expose organizations to unnecessary risks and prolonged periods of vulnerability. By adopting a proactive stance, organizations can stay ahead of emerging threats, fortifying their defenses before malicious actors exploit vulnerabilities. This proactive approach is being adopted by some financial institutions in preparation for deploying AI, as highlighted by Practitioner 2: "The banking industry is currently thinking about what policy considerations [they should] have if the banking sector starts to take up AI and generative AI at scale."

Cyber Risk Area 3: Attacks Via Third Parties

An increasingly prevalent and sophisticated tactic employed by malicious actors involves infiltrating organizations not through direct attacks but rather by exploiting vulnerabilities within their supply chain partners. The intricate web of interconnected relationships common in modern business operations provides hackers with a strategic route to compromise the integrity and security of their targets. This method, often termed a "supply chain attack,"

16 Dash, B. and Sharma, P. "Are ChatGPT and Deepfake Algorithms Endangering the Cybersecurity Industry? A Review," *International Journal of Engineering and Applied Sciences* (10:1), January 2023.

17 Gurpreet, D., Smith, K. and Dissanayaka, I. "Information Systems Security Research Agenda: Exploring the Gap between Research and Practice," *The Journal of Strategic Information Systems* (30:4), December 2021, Article 101693.

places organizations at heightened risk, because hackers strategically compromise trusted partners and suppliers to stealthily gain access.[18] The implications of such breaches extend beyond individual organizations, creating cascading effects across interconnected networks. An example is the 2013 breach of American retailer Target's systems, which was due to its vendors' poor cybersecurity.[19] To counter the emerging "supply chain attack" threat, there is an urgent need for cybersecurity policymaking agility.

Another example of the significance of supply chain cyber risk is the "Latitude hack," where cybercriminals successfully exploited vulnerabilities in a third-party vendor offering back-end infrastructure provider services to the company. (Latitude Financial Services is an Australian financial services company.) The hacker ultimately gained access to the login credentials of a Latitude employee, leading to the theft of personal information.

Practitioner 1 recounted how an attack on one of his company's suppliers compelled it to update policies and standards for working with other organizations in its network:

> *"We were using a password manager application for our product, and [the supplier] had a massive data breach. ... [However], they were not communicating with their customers about what was happening. After they revealed more about the data breach, we [found] that we lost all our code base with all the keys in it. ... We had to make a very quick decision and roll them off. ... But why did this happen? Because we started working with [that supplier] before we established our vendor assurance policy. We didn't have any evidence of them complying with any standards like ISO 27001. Before we could migrate [to a new supplier], we had to make sure that [the] vendor had all of those ... security assurance things. So, we made sure we did a review of two ... other vendors. And we updated our security policy in terms of working with third parties and setting higher standards."*

This experience illustrates the importance of cyber risks arising from supply chain partners and service providers. It also shows the consequences that a breach in a third party can unleash upon an organization. Beyond the immediate impacts of losing sensitive data, the recounted incident spotlights the systemic risks and vulnerabilities inherent in supplier relationships. It also serves as a reminder that the effectiveness of an organization's cybersecurity defenses is intricately tied to the security practices of its suppliers.

Given the interconnected nature of the digital ecosystems, there is a need for stringent security measures not only within the organization but throughout the entire supply chain. Thus, the updated security policy should not only establish higher standards for third-party engagement but also incorporate a continuous monitoring framework, as illustrated by the experience recounted by Practitioner 5:

> *"Our [telecoms] company decided to delegate certain customer services to individuals in foreign countries and thus we had to reassess our policy framework in response to the change in risk landscape, as well as the shifting legal and regulatory requirements in those countries."*

By adopting a flexible and responsive approach to cybersecurity policy development and enforcement, organizations can rapidly adjust their security frameworks to address vulnerabilities exposed through their associations with external vendors and service providers. These agile policies provide organizations with a tool for creating consistent and comprehensive security over the whole network and updating providers about any changes.

Cyber Risk Area 4: External Disruptive Events

Another source of external cyber risks involves unforeseen events such as natural disasters, social unrest and geopolitical tensions. Predicting all future disruptive events is impractical, highlighting the imperative for agility and adaptability in cybersecurity policymaking.

18 Jay, S. and Omar, A. "Cybersecurity Investments in the Supply Chain: Coordination and a Strategic Attacker," *European Journal of Operational Research* (282:1), April 2020, pp. 161-171.
19 Travis, F. and Schwartz, M. "Using Contracts to Curb Cyber-risks," *Risk Management* (64:5), May 2017, p. 16.

Practitioner 2 cited the Russia-Ukraine tension, which has given rise to the challenge of a "hybrid war," involving simultaneous physical and cyber warfare. In his view, responding to this challenge requires agile decision-making in adapting cybersecurity policies to address the evolving landscape of cyber threats and ensuring the resilience of organizational defenses.

Another example of an external disruption was during the COVID-19 pandemic, when working from home became commonplace, which heightened cybersecurity concerns and posed unprecedented challenges. Cybercriminals capitalized on the unpreparedness of organizations, particularly software vendors, by intensifying their attacks.[20] As a consequence, formulating or updating cybersecurity policies became imperative, as emphasized by Practitioner 8:

> *"After COVID-19, organizations decided to use work from home as a solution, but they needed a policy change regarding using organization-issued devices, which have proper security controls such as EDR [endpoint detection and response], antivirus or other mitigation security controls. But what happened was many employees were using their own devices, like their home laptop. It was causing some problems because using their own devices on the organization's VPN could increase the likelihood of a cyberattack. So, many organizations started updating their policies and banned using personal devices, denying the personal devices to be connected to the organization's network."*

Another external factor is government regulations, which may result in fines if organizational cybersecurity policies do not align with them. Policymakers must therefore constantly monitor regulations and initiate the revision of existing policies or the formulation of new ones to ensure compliance. This proactive approach is already underway in some organizations, as recounted by Practitioner 9:

> *"In our organization, there is a constant [monthly] cycle of [information security] policy update to align with overall government policies and regulations, and this is being done [by a] steering committee that has representatives from the different departments."*

In summary, organizations should not only react to specific external events but also proactively anticipate potential challenges. The interconnectedness of geopolitical tensions, global events like pandemics and regulatory frameworks underscores the need for continual agility and adaptation in cybersecurity policies. Agility will ensure that organizations remain resilient and responsive to the evolving cybersecurity landscape, mitigating risks effectively and maintaining the integrity of their digital infrastructure. However, being proactive and agile does not imply that organizations must address every possible risk; rather, their response depends on the risk appetite of each organization, as implied by the recommended actions for cybersecurity policymakers set out below.

Recommendations and Actions for Enhancing Agility in Cybersecurity Policymaking

From the insights gathered from the interviews, it is evident that organizations need to take several actions to enhance the agility of their cybersecurity policymaking processes. Though we acknowledge that an organization's size and maturity may influence the specific needs and requirements of these actions, they represent common themes extracted from practitioners across various industries and organizational sizes. Our overarching recommendation for each risk area is shown in Table 1, along with a summary of our recommended actions for achieving the requirements of the recommendations.

Recommendation 1. Update Cybersecurity Policies to Address Legacy System Cyber Risks

There are two requirements for updating cybersecurity policies to address risks arising from legacy systems: adopting a digital asset

20 Lallie, H. S., Shepherd, L. A., Nurse, J. R. C, Erola, A., Epiphaniou, G., Maple, C. and Bellekens, X. "Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic," *Computers & Security* (105), June 2021, Article 102248.

Table 1: Summary of Recommendations and Actions for Enhancing Agility in Cybersecurity Policymaking

Recommendation for Risk Area:	Requirements	Recommended Actions
1. Update Cybersecurity Policies to Address Legacy System Cyber Risks	Digital Asset Management	**Action 1.1:** Adopt an agile approach to continually identify, prioritize and oversee digital systems crucial to operations, adapting cybersecurity measures promptly to address evolving threats and risks arising from legacy systems
	Vulnerability Management	**Action 1.2:** Update cybersecurity policies concurrently with the gradual migration from vulnerable legacy systems to the latest technologies
2. Adapt Cybersecurity Policies for Emerging Technologies	Technology Scouting	**Action 2.1:** Enhance technology scouting capabilities to dynamically monitor and swiftly adapt cybersecurity policies in response to emerging threats and defense opportunities associated with new technologies
	Cyber Risk Management	**Action 2.2:** Establish a resilient cyber risk management framework for conducting technology-specific risk assessments, ensuring ongoing alignment with emerging threats, and enabling prompt adjustments to cybersecurity policies as necessary
3. Strengthen Policies for Third-Party Cyber Risks	Vendor Risk Assessment	**Action 3.1:** Strengthen vendor risk management by conducting agile assessments of vulnerabilities, availability and compliance, enabling prompt policy adjustments in response to emerging cyber threats in the business ecosystem
	Contractual Security Controls	**Action 3.2:** Review and update cybersecurity policies and contracts periodically, ensuring they align with emerging risks, standards and industry best practices
4. Build Flexible Cybersecurity Policies for Disruptive External Events	Training and Awareness	**Action 4.1:** Enable prompt adjustments to policies during disruptive events by providing ongoing training to all employees (including board members)
	Business Continuity Plans	**Action 4.2:** Periodically test and update business continuity and disaster recovery plans, incorporating insights from disruptive events and fostering a flexible policymaking approach that allows for innovative solutions while safeguarding vital information systems

management system and including vulnerability management. Our recommended actions for addressing these requirements are described below.

Action 1.1: Adopt an Agile Approach to Digital Asset Management. Digital asset management requires a methodical process to identify, organize and oversee various assets within an organization's information technology infrastructure. It assists organizations in recognizing and prioritizing critical assets and data, commonly referred to as the "crown jewels." Practitioner 7 emphasized the importance of having an asset management system, stating: "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." This underscores the need for a structured asset management approach as one of the foundations of an effective cybersecurity policymaking process. Practitioner 7 continued by emphasizing the need to have an asset management program in place as one of the required steps for agile and adaptive policymaking: "We would want to know our crown jewels, we would want to know what are [the] important critical assets for the organization that we need to worry about. … And we want to know what data we hold. … [But knowing] what critical data is important for the organization is only part of the game." He went on to say that information about the crown jewels and their related risks should find its way to the policymaking process, facilitating the security and protection of critical data in a timely manner.

Additionally, Practitioner 2 emphasized the significance of understanding the most attractive digital assets to hackers: "Knowing what the hackers will target allows you to narrow down your crown jewels and then that's where you can have targeted programs in keeping those assets safe and away from the hands of the threat actors."

These insights highlight the importance of asset management as one of the main pillars in agile and adaptive cybersecurity policymaking. Though our interviewees highlighted the significance of asset management, they see it as a necessary but not sufficient step because the intelligence gathering should find its way to the policy decision-making process. This underscores the importance of decision agility in cybersecurity policymaking, where emerging risks to an organization's digital crown jewels require swift adaptation in policies, procedures and standards.

Asset management is particularly crucial for legacy systems, as they may hinder the organization from adopting best-practice policies, potentially becoming a source of threat. Implementing an asset management program is the initial step for organizations to identify and prioritize their assets, especially legacy systems, and assess the associated cyber risks and necessary policy updates.

In summary, our recommended action for addressing the digital asset management requirement in the context of legacy systems is to adopt an agile approach to continually identify, prioritize, and oversee digital systems that are crucial to operations, adapting cybersecurity measures promptly to address evolving threats and risks arising from legacy systems.

Action 1.2: Include Vulnerability Management in Cybersecurity Policymaking. Vulnerability management requires a structured and systematic approach to identifying, assessing, prioritizing and mitigating vulnerabilities within an organization's IT infrastructure. Implementing such an approach is crucial because vulnerabilities persist indefinitely, new systems are continually introduced and legacy systems remain in place within the organization, as emphasized by Practitioner 3: "A vulnerability management program is a great idea to implement in the organization in light of the fact that vulnerabilities are never ending; we always put new systems in the organization, and we always have legacy systems in the organization."

Practitioner 8 mentioned the practical IT aspect of vulnerability management: "When you look at vulnerability in a strictly kind of IT sense, that's about running vulnerability scans across your organization, getting that data back and then effectively prioritizing how you're going to mitigate those vulnerabilities to prevent them from becoming risks." This insight reveals the importance of an ongoing scanning and prioritization program for the effective management of vulnerabilities.

Practitioner 6 underscored the broader significance of vulnerability management: "Organizations need to [have] a level of threat intelligence, … [they should] hunt [down and] understand where their biggest vulnerabilities are." This quote emphasizes that in addition to regular scanning, organizations must engage in proactive threat intelligence. This will help them to identify and prioritize their most critical vulnerabilities. However, as Practitioner 4 highlighted, knowing and prioritizing vulnerabilities, and updating cybersecurity policies accordingly is of great importance. She said: "When you look at the cybercriminals and hacktivists and so forth, they don't necessarily take advantage of every single vulnerability. So, there are some trends that you can get to really understand where the biggest vectors of

compromise are that have been used in the past to compromise a particular organization."

Identifying and prioritizing vulnerabilities in legacy systems and adapting policies based on these vulnerabilities can also help the organization reduce the cyber risks associated with these systems. Moreover, implementing a vulnerability management program together with an asset management program will provide crucial data and information to create an "asset-vulnerability matrix." This matrix will enable the organization to quantify its risk appetite, allowing it to analyze the vulnerabilities associated with each legacy system. Moreover, the asset-vulnerability matrix will aid policymakers in formulating appropriate cybersecurity policies in a timely manner.

A vulnerability management program can also be instrumental in prioritizing systems requiring upgrades, paving the way for an incremental upgrade program. In this scenario, the organization can concentrate on integrating security patches and updates compatible with the existing infrastructure, while developing a phased migration plan to transition from legacy systems to more modern, secure solutions. As these upgrades take place, policymakers can gradually update the cybersecurity policy as legacy systems are phased out.

In summary, our recommended action for addressing the vulnerability management requirement in the context of legacy systems is to update cybersecurity policies concurrently with the gradual migration from vulnerable legacy systems to the latest technologies.

Recommendation 2. Adapt Cybersecurity Policies for Emerging Technologies

The two requirements for adapting cybersecurity policies for emerging technologies are technology scouting and establishing a cyber risk management framework. Our recommended actions for addressing these requirements are described below.

Action 2.1: Enhance Technology Scouting Capabilities. Emerging technologies can present both new threats and opportunities for organizations. To mitigate the negative impacts of emerging technologies, firms should implement a robust cyber threat intelligence monitoring system. This involves staying informed about emerging cyber threats associated with new technologies either through using vendor services or building internal capabilities to gather intelligence from various sources, such as social media or hacker forums. Practitioner 4 stated:

> *"The only way that [we] can successfully understand the threat landscape and obtain some threat intelligence data to apply internally is through augmented resourcing and augmented capability. However, when you can buy those capabilities from trusted vendors, consultants, third-party or providers, it might be a more viable option for most firms."*

Though emerging technologies introduce new cyber threats, new developments like AI, cybersecurity services outsourcing, cloud access security brokers and computational-intelligence-enabled technologies also provide opportunities for firms to improve their defenses against cyber threats. Proactively searching for and systematically incorporating emerging technologies into the cybersecurity policy agenda allows organizations to prioritize specific technologies and leverage them for better preparation against new threats.

To enhance the effectiveness of technology scouting in agile cybersecurity policymaking, we recommend that organizations establish dedicated teams or collaborate with external experts specializing in technology trends and cybersecurity. Regularly monitoring industry reports, attending conferences and participating in technology forums can provide valuable insights into emerging threats and potential defenses. Additionally, fostering partnerships with research institutions or technology startups can facilitate access to cutting-edge solutions aligning with the organization's cybersecurity goals.

By incorporating technology scouting into agile cybersecurity policymaking, organizations can strategically leverage emerging technologies to enhance their cyber defenses, stay ahead of evolving threats and maintain a resilient security posture.

In summary, our recommended action for enhancing technology scouting is to dynamically monitor and swiftly adapt cybersecurity policies

in response to emerging threats and defense opportunities associated with new technologies.

Action 2.2: Establish a Resilient Cyber Risk Management Framework. The second critical requirement for cybersecurity policy related to emerging technologies is to actively manage cyber risks rather than solely focusing on identifying them. We recommend that organizations empower teams to promptly report cybersecurity risks and establish a framework for facilitating the proper qualification and escalation of these risks to the relevant level. Depending on the nature of the risk, it may be accepted avoided, transferred or mitigated. As highlighted by Practitioner 9, "There should be a well-defined mechanism within the cybersecurity domain to effectively manage these risks through a framework, ensuring seamless integration with enterprise risk management."

In addition to actively managing cyber risks, organizations should conduct comprehensive assessments of the risks that emerging technologies may pose before widely adopting them. This proactive approach will not only empower teams to promptly report cybersecurity risks but can also provide the opportunity to tailor cybersecurity policies based on the unique risks posed by each new technology. Establishing a well-defined mechanism within the cybersecurity domain, as highlighted by Practitioner 9, ensures seamless integration with enterprise risk management and reinforces the organization's resilience against evolving threats.

Organizations can also enhance agility in cybersecurity policymaking by establishing a risk committee and appointing a chief risk officer (CRO), as Practitioner 8's company has done: "For me, [cybersecurity policy is] 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." Practitioner 9 emphasized the importance of integrating a CRO position into the organizational structure, stating: "In terms of what's needed, the idea of a CRO … who is more focused on the broad security of the organization [can be helpful]."

Delegating some policymaking responsibilities to lower levels of the organization and avoiding the need to escalate all decisions to the board level can further enhance the speed of policymaking. Practitioner 1 asserted: "Without delegating your policymaking down to the right levels, there will be an inability to adapt to changes effectively."

In summary, our recommended action for cyber risk management for emerging technologies is to establish a resilient cyber risk management framework for conducting technology-specific risk assessments, ensuring ongoing alignment with emerging threats and enabling prompt adjustments to cybersecurity policies as necessary.

Recommendation 3. Strengthen Policies for Third-Party Cyber Risks

The two cybersecurity policy requirements for cyberattacks via third parties are strengthening vendor risk management and reviewing and updating contractual security controls. Our recommended actions for addressing these requirements are set out below.

Action 3.1: Strengthen Vendor Risk Management. There are considerable challenges in sustaining an organization's business ecosystem arising from uncertainties and risks tied to factors such as the scope of cybersecurity requirements, adherence to industry best practices and the continual upkeep of their relevance and sufficiency. The competitive and proprietary nature of deploying new technologies further complicates matters, posing challenges in reaching a consensus about the extent of necessary cybersecurity measures. To address these issues, we recommend that organizations establish a process for continuously assessing vendors' cybersecurity. This involves formulating policies to ensure that less-secure vendors do not act as a conduit for letting hackers into the organization's systems.

Another supply chain risk relates to the continuing availability of third parties in the event of a cyberattack, as emphasized by Practitioner 4:

> *"A lot of organizations, whether mature or just beginning their journey in third-party risk management, are currently looking across their supply chains. They evaluate them from the perspectives of availability, confidentiality and integrity. The focus lies on identifying critical services*

> *from third- or fourth-party providers that are providing critical services for their business operations and resilience. Understanding the potential impact on operational success if specific systems or applications are offline for a period of time is crucial. This evaluation, particularly from an availability perspective, is a vital aspect. Another aspect is to understand the locations of these critical services to ensure ongoing operational resilience from a different perspective."*

We therefore recommend that organizations assess the availability and significance of their vendors and formulate policies to ensure that in the event of a cyber incident affecting them, the organization can sustain its essential functions.

To stay abreast of the risk profile of third parties, assess their adherence to mandated cybersecurity policies and monitor their controls, organizations should establish continuous monitoring mechanisms for tracking the cybersecurity posture of their ecosystem parties. Automated tools like CyberGRX can be used to identify anomalies and potential security breaches and thus mitigate the risk of cyberattacks via third parties.

In summary, our recommended action for addressing the vendor risk assessment requirement is to strengthen vendor risk management by conducting agile assessments of vulnerabilities, availability and compliance, enabling prompt policy adjustments in response to emerging cyber threats in the business ecosystem.

Action 3.2: Review and Update Cybersecurity Policies and Contracts Periodically. To enhance the security of working with third parties, we recommend that organizations incorporate specific cybersecurity requirements into contracts with them. Organizations should start by developing their own policies for collaborating with third parties, ensuring they include the necessary cybersecurity standards and procedures. Subsequently, contracts with vendors should clearly define the expectations if a cyber incident occurs related to data protection, incident response notice or cooperation and compliance.[21] Importantly, there should be flexible processes for updating policies and contracts to accommodate emerging risks and enforce new standards.

As mentioned earlier, Practitioner 1 stated that after the data breach in one of his company's vendors, it had to set stricter policies and standards and migrate to another vendor. He further elaborated: "We looked at the white papers saying how they [i.e. third parties] were secure and then made the decision who we were going to go with, then migrated off the previous vendor to the new vendor. We updated our policies and standards and [incorporated] them into our new contract." In another case, Practitioner 7 stated: "We've got lots of suppliers … and we need to decide what to share with each supplier. We've got a methodology [and policy] for it and we assess those suppliers, their posture, their maturity and the level of information we share with them. … [Information] security of our partners is one of the important aspects of our contracts."

In summary, our recommended action for meeting the contractual security controls requirement of third-party cyberattacks is to review and update cybersecurity policies and contracts periodically, ensuring they align with emerging risks, standards and industry best practices.

Recommendation 4. Build Flexible Cybersecurity Policies for Disruptive External Events

The two requirements for building flexible policies for disruptive external events are providing training and awareness and having and testing business continuity plans. Our recommended actions for addressing these requirements are set out below.

Action 4.1: Provide Continuous Training and Awareness. Enhancing cybersecurity policy awareness through security education, training and awareness programs is integral to every cybersecurity initiative. Training and awareness become particularly crucial during disruptive events when the need may arise for policy and practice adjustments to adapt to the evolving environment. In this context, specialized training for both board members and employees is especially important.

21 Travis, F. and Schwartz, M., op. cit., May 2017.

For board members, "tabletop" cyber threat simulation services can prove invaluable, as noted by Practitioner 7. "We provide a service called Tabletop exercise. We take a professional consultant who is experienced in sovereign incidents, and we put our executives into a closed room, and we give them a scenario of an incident. We can then assess their reactions … and they can learn and … update their policies [for disruptive events] if necessary."

For employees, it is important to make sure that they are aware of the current policies and procedures, changes in the policies and the need for changes in dynamic environments. As Practitioner 4 highlighted: "In some cases, it is not about policy formulation or implementation, but about awareness. Especially when we are talking about changes in policies, employees need to be aware of the changes and the reason for change." However, some researchers have reported that resistance to change by employees is one of the main challenges of agile organizations,[22] and it is essential to increase employees' awareness of the need for change and to increase their skills through training, so they can adapt to the change. Practitioner 6 asserted that "If there is no connection between the individual's personal motivation and the organizational objectives or policies, they are unlikely to comply. This is a crucial aspect that is currently lacking: establishing a meaningful connection between the 'individual's why' and the 'organization's why.'"

In summary, our recommended action for cybersecurity training and awareness is to enable prompt adjustments to policies during disruptive events by providing ongoing training to all employees (including board members).

Action 4.2: Periodically Test and Update Business Continuity Plans. Establishing robust business continuity and disaster recovery (BCDR) plans is a significant part of cybersecurity in many organizations. However, these plans and cybersecurity policies need to be periodically tested and updated to make sure they are consistent with the latest threats found in the cyber landscape. Practitioner 2 revealed that many organizations fail to update their BCDR plans, which could be a source of threat in times of disruptive events:

> *"A good example is: I get a lot of questions about … when did you last update your business continuity policy and when did you last test it? And we respond, well, we do it every year and here's the change log. Here's the fact that we reviewed it. … But [those] same organizations that ask us that question, they have not done it themselves."*

The BCDR plan should encompass the organization's response to various disruptive events, including pandemics. Responses to the COVID-19 pandemic are a valuable source of insights for policy preparation—for example, work-from-home policies. Moreover, the policymaking process should exhibit flexibility during disruptive events, enabling the implementation of innovative solutions without compromising the security of vital information systems.

In summary, our recommended action for addressing the business continuity plans requirement is to periodically test and update BCDR plans, incorporating insights from disruptive events and fostering a flexible policymaking approach that allows for innovative solutions while safeguarding vital information systems.

Concluding Comments

Though the ISO 27001 international standard and the NIST framework recognize the importance of identifying opportunities for improving cybersecurity policies, our recommendations delve deeper and offer a more dynamic approach specifically targeted at adapting policies in response to evolving threats. Building on the software development lifecycle (SDLC) framework, NIST recognizes the importance of identifying opportunities for improving cybersecurity policies, emphasizes the significance of developing appropriate responses, including updating policies, to changing supply chain risks, and highlights the need to review and update policies. ISO 27001 also uses a structured approach to secure information security management systems. While ISO is

22 Storme, M., Suleyman, O., Gotlib, M. and Lubart, T. "Who is Agile? An Investigation of the Psychological Antecedents of Workforce Agility," *Global Business and Organizational Excellence* (39:4), July 2020, pp. 28-38.

thorough, it is often a high-level document that requires organizations to interpret and apply the guidelines according to their specific needs and context.

Acknowledging that ISO 27001 and the NIST framework provide the initial steps, our findings show that these frameworks do not provide sufficient recommendations specific to adapting policies in response to new threats, especially in the turbulent cyber environment. For example, the NIST framework excludes the requirements for policy adaptation and the need for agile decision-making. Additionally, it discusses the need for organizational risk management at the strategic level, though the experts we interviewed believe that policy making agility should flow from the results of risk management efforts, which should be used to proactively update policies, procedures and processes.

Our findings also delve deeper into the importance of managing supply chain risks (mentioned in the NIST framework) and propose the need for contracts that incorporate the need to update cybersecurity policies over the entire business ecosystem. We also found that technology scouting can be a good source of insights for cybersecurity policymakers on adopting emerging defensive technologies—a proactive approach to policy improvement that is not part of ISO 27001 or the NIST framework.

In summary, though ISO 27001 and NIST provide valuable foundations for cybersecurity, to effectively address the rapidly changing landscape of cyber threats, they should be complemented with the more granular, agile and technology-focused recommendations set out in this article.

Appendix: Research Methodology

The primary goal of our study was to examine the practical application of agility and adaptability in cybersecurity policymaking through real-world cases. Our aim was to explore how practitioners have employed these concepts and identify the essential requirements for achieving agility in cybersecurity policymaking. We chose to conduct interviews with cybersecurity experts because this method ensured that our research was grounded in current practices, offering a thorough and detailed understanding of the imperative for agility in cybersecurity policymaking processes.

We employed an inductive and exploratory method to unveil novel and unforeseen findings. Consistent with the exploratory nature of the study, we conducted nine semi-structured interviews (eight online and one face-to-face) in May and June 2023 with cybersecurity experts from Australian companies. The eligibility criteria for participants included a minimum of three years' experience in roles such as CIO, CISO, CTO or other relevant positions within the cybersecurity field. To ensure the inclusiveness and broad applicability of our findings, we selected interviewees from diverse industries, including technology, telecoms, consulting, finance and the public sector (see table below). The interview durations varied between 45 and 60 minutes, with an average of 52 minutes.

Each semi-structured interview began with four primary questions about the interviewee's understanding of cybersecurity policymaking adaptability, how the interviewee's organization tries to stay up to date about threats in the cybersecurity landscape, how the organization learns from past policymaking experiences, and examples of using agile and adaptive policymaking. We transcribed all the interviews, and the transcripts were carefully reviewed, corrected and analyzed by the interviewers.

We used the NVIVO 12 software to apply inductive coding to the transcripts and employed thematic content analysis to scrutinize the data. Despite the linear presentation of our findings in this article, it's crucial to highlight that our entire data analysis process was iterative, focusing on enhancing insights and improving the generalizability of our findings. In essence, we conducted constant comparative analyses, iteratively analyzing data after each interview, leading to the refinement of our understanding and interview questions. After the first three interviews, this approach uncovered an additional theme relating to risk management in cybersecurity. As a result, we added another question to our primary set of questions in subsequent interviews that asked about the way new risks affect policymaking processes. It's noteworthy that during the interviews, the first

Interviewee Profiles

Interviewee	Experience (Years)	Roles	Sector	Company Size
Practitioner 1	12	COO, cybersecurity architect and advisor	Cybersecurity solutions	Small (1-19 staff)
Practitioner 2	18	Chief security officer, former CISO	Technology	Large (more than 200 staff)
Practitioner 3	4	Cybersecurity manager	Cybersecurity solutions	Small
Practitioner 4	22	Consultant, former CISO	Health, financial and professional services	Large
Practitioner 5	11	Cyber specialist (data analyst), cybersecurity solution architect	Telecoms	Large
Practitioner 6	15	Senior vice president of cyber security strategy and architecture	Financial services	Medium (20-200 staff)
Practitioner 7	18	Cybersecurity specialist, consultant	Cybersecurity solutions	Medium
Practitioner 8	15	Principal security consultant	Technology	Medium
Practitioner 9	20	Cybersecurity manager, former senior security auditor and IT architecture manager	Public sector	Large

author executed the three stages of the Gioia[23] process, which were subsequently confirmed by the other co-authors in weekly meetings.

We used a structured approach to organize and review our data to make sure the final concepts were consistent with the original data. We used the existing literature on cybersecurity policymaking and our knowledge of organizational agility and adaptability to identify the themes and concepts emerging from the interview data. This process helped us create a clear connection between the raw data, the concepts that emerged from our analysis and the broader themes we identified. By considering the viewpoints of both the interviewed experts and the researchers, we were able to develop a precise and thorough discussion of the concepts that were firmly based on the data.

23 Gioia, D. A., Corley, K. and Hamilton, A. "Seeking Qualitative Rigor in Inductive Research," *Organizational Research Methods* (16:1), January 2013, pp. 15-31.

About the Authors

Masoud Afshari-Mofrad

Masoud Afshari-Mofrad (Masoud.Afsharimofrad@hdr.mq.edu.au) is a researcher at Macquarie Business School, Macquarie University, Sydney, Australia. He is currently working as a postdoctoral research fellow at the Australian National University.

Alireza Amrollahi

Dr. Alireza Amrollahi (Ali.Amrollahi@ mq.edu.au) is a lecturer of business information systems at Macquarie Business School, Macquarie University, Sydney Australia. His research is published in top-tier journals with a focus on the social and organizational impacts of information systems, including digital work, technology governance, digital innovation, the strategic impact of emerging technologies, digital strategy, openness and digital strategizing. His work is also highlighted in the media and implemented in various organizations globally. Ali serves as a section editor for *Australasian Journal of*

Information Systems and has held leadership roles at the Australasian Conference on Information Systems (ACIS) over multiple years.

Babak Abedin

Babak Abedin (Babak.Abedin@mq.edu.au) is a professor of business analytics, head of the Department of Actuarial Studies and Business Analytics, and an executive member of Macquarie Business School, Macquarie University, Sydney Australia. His research has been published in top-tier journals such as *Decision Support Systems*, *Information & Management* and *Journal of the Association for Information Science and Technology*.