COALITION TO REDUCE CYBER RISK

WHITE PAPER

Cybersecurity Policy for Resilient Economies: A Global, Cross-Sector Approach

membership@crx2.org
www.CRx2.org

Executive Summary

This paper represents the experiences and perspectives of a diverse, cross-sector group of multinational companies that seek to partner with governments as they develop and implement policies to address cybersecurity challenges. Our companies recognize that effectively addressing cybersecurity challenges requires partnerships across sectors and borders, consistent with the inherently interconnected and complex nature of cyberspace. Moreover, we recognize that there is an opportunity for governments and companies from different sectors to collectively address cybersecurity challenges in a way that strengthens security, improves oversight, and promotes economic growth and innovation.

Our starting point is our range of experiences, not only working with governments but also implementing cybersecurity risk management programs across dynamic global infrastructure and operations. We have learned that reliance on globally recognized standards and best practices helps both companies and their customers and assessors manage and evaluate security at scale. Moreover, notwithstanding the value of standards and assessment programs, we have learned that our cybersecurity activities must go beyond compliance and reflect a holistic approach towards cyber resilience. They must incorporate ongoing assessments of cybersecurity risks to our products, services, and enterprises as well as regular cycles of continuous improvement.

This paper builds upon our experiences in implementing cybersecurity risk management programs by describing policy development processes and principles that we consider essential for governments that are working to address cybersecurity challenges. First, it outlines the *processes* that are crucial to developing effective cybersecurity policies and approaches. We encourage government processes to be open, collaborative, and iterative, incorporating the experience and expertise of a range of stakeholders. Second, it describes the *principles* that governments should use to structure and embed into their efforts, establishing as a foundation the cybersecurity lessons that industry has learned and integrated over the last decade.

Finally, the paper articulates economic and security benefits of alignment and/or consistency across global and sectoral approaches to cybersecurity risk management. Whereas policies that fragment across jurisdictions or sectors would risk weakening global cybersecurity and undercutting economic advancement, policies with alignment or consistency support global exchange of information, enable greater visibility into global threats, increase access to best-in-class products and services, and promote economic advancement. As multiple governments initiate a range of efforts intended to address cybersecurity challenges across numerous sectors, we encourage them to consider not only appropriate policy processes and principles but also how their efforts contribute to security across our global, interconnected ecosystem.

Introduction

Organizations around the world are increasingly leveraging the power of information and communications technology (ICT) to connect, innovate, and grow in a dynamic global economy. Small businesses have thrived by using mobile technologies, accessing global investment platforms, and integrating into global supply chains. Larger enterprises have used technology to drive innovation and to help manage scale as they expand global operations. Similarly, governments have used a range of modern technologies, including cloud services, to develop or improve citizen services. Most broadly, consumers have benefited from enhanced products and services, such as safer cars, improved health care, and more flexible financial transactions.

While organizations increasingly leverage ICT, governments are also seeking to ensure that products and services that are important to their citizenry are resilient. As organizations connect more devices to critical systems, cybersecurity challenges increase, and the escalating risk limits economic opportunity and advancement enabled by ICT. In recognition of such challenges, governments have appropriately identified the need for organizations—including companies of diverse sizes and from various sectors—to fully incorporate cybersecurity into their existing enterprise risk management efforts. Moreover, some governments are developing guidance or requirements intended to address cybersecurity threats to critical infrastructure, essential services, and the Internet of Things (IoT). There are dozens of ongoing regional and national initiatives focused on developing or evolving requirements for cybersecurity risk management.[1]

Cybersecurity poses one of the greatest policy and operational challenges facing governments and industries around the world, but it also presents a unique opportunity for governments, companies, and sectors to come together to meet these challenges. Technologies are complex and rapidly changing, and a range of persistent and advanced actors, including nation states and organized crime, develop and constantly evolve threats. Formulating effective public policy in the context of this dynamic environment requires partnership across the public and private sectors. Drafting and implementing guidance or requirements cooperatively will lead to better outcomes on shared goals, including improved security and greater efficiency.

As governments develop and implement policies to address cybersecurity challenges, we seek to be a partner that can inform those processes through our experiences and perspective as a diverse, cross-sector group of multinational companies. To enhance global cybersecurity, these policies must be developed through open, collaborative, and iterative processes; based on principles and best practices for cybersecurity risk management; and aligned with broader international and sectoral efforts. Too often, fragmented and inflexible approaches undermine security goals and misdirect both government and industry resources. By leveraging collaborative processes, recognized principles and best practices, and a global perspective, governments can promote economic opportunity and enhance the security of our interconnected systems.

[1] E.g., across Europe (with implementation of the Network and Information Security Directive) as well as a result of various efforts in Brazil, China, Colombia, Japan, Kenya, Singapore, South Africa, Ukraine, and other regions.

I. Processes for developing effective cybersecurity risk management policies

As governments develop cybersecurity risk management approaches, a crucial first step is to focus on being open, collaborative, and iterative, creating multiple opportunities for partnership with relevant stakeholders and the sharing of perspectives, ideas, and feedback.[2] Through an open and collaborative process, stakeholders can build from diverse sets of expertise and work together to ensure that shared goals are met in practice. The complexity and dynamic nature of cybersecurity threats demands that approaches are fully considered in their practical application by a broad range of stakeholders. In addition, governments should create an iterative process, recognizing that the most effective cybersecurity risk management approaches will be developed and refined over time and with ample opportunity for understanding and incorporating feedback from stakeholders. Ultimately, cybersecurity risk management approaches developed through such open, collaborative, and iterative process can be more easily and effectively implemented.

There are multiple approaches that governments can take to be open, collaborative, and iterative in developing cybersecurity risk management approaches, including public consultations and industry workshops. Through efforts such as public consultations or requests for comments, governments can invite stakeholders to inform, contribute to, or comment on draft policies. In responding to such requests, stakeholders can help inform government efforts in the early stages of policy development, ensuring that an understanding of technology architectures and operations leads to draft policies that are appropriately scoped from the outset. Like public consultations, industry workshops are processes through which governments invite stakeholders to contribute to or comment on draft policies. The benefit of industry workshops is that governments can invite multiple stakeholders to contribute feedback simultaneously, efficiently capturing the interplay between a variety of perspectives and ways that regulation may impact stakeholder communities. That interplay is especially critical to capture as governments create new requirements that will affect various sectors and types of organizations—because cross-sector impacts may be harder for governments to anticipate. However, even after hosting industry workshops, governments will likely find value in publishing draft policies for public comments as well. Industry workshops can provide important opportunities for discussions that help to

Public consultations

In 2017, **China, Singapore, Vietnam, Mexico, and South Africa** publicly shared their draft national cybersecurity laws, seeking public and industry feedback.

In 2016, the **European Network and Information Security Agency (ENISA)** launched open surveys on the Network and Information Security (NIS) Directive requirements, seeking input on current industry processes and capabilities related to cybersecurity risk management and incident notification. Then, taking the survey results into consideration, ENISA developed draft implementation frameworks and shared them with stakeholders, seeking their feedback.

[2] This suggested best practice overlaps with guidance described in *International Cybersecurity, Data and Technology Principles*, http://www.gfma.org/correspondence/item.aspx?id=807. Specifically, the European Banking Federation, Global Financial Markets Association, and International Swaps and Derivatives Association articulated that "[s]tandards, guidelines and regulations should be created in an open and transparent process that encourages consultation and collaboration between developing bodies, those required to adopt the new policies, and other affected stakeholders."

shape early thinking, but they can rarely serve as a full replacement for written comments in response to initial and/or revised draft policies.

We have been encouraged by the trend in countries seeking to take advantage of the private sector's cybersecurity risk management expertise. In 2017 alone, multiple countries, such as China, Indonesia, Mexico, Singapore, South Africa, and Vietnam, shared their draft cybersecurity laws and regulations for stakeholder review and input. However, we remain concerned that industry recommendations, based on experiences implementing cybersecurity risk management programs, are often not incorporated on key issues such as encryption, data protection, and cross-border data flows. By prioritizing local, inflexible approaches above recognized best practices, these policies result in significant economic costs without reducing cybersecurity risk.

II. Best practices and principles for cybersecurity risk management policies

As governments engage in discussions about cybersecurity risk management with stakeholders, ensuring that policies support robust connection and exchange across organizational boundaries and reflect risk-based, outcome-focused, and agile approaches will ensure that these efforts are effective and efficient. These principles and best practices are grounded in industry experience and have proven successful across sectors and around the world. For many years, large enterprises across various sectors have been working to develop, deploy, and better manage ICT products and services, reflecting on cybersecurity lessons learned and integrating those lessons into their security development lifecycles, operational practices, and supply chains. Approaches to cybersecurity risk management that incorporate and reflect these principles and best practices will drive meaningful security improvements, avoid diversion of scarce public or private resources, and enable competition and innovation in the global marketplace.

Clear and Consistent: Improving a company's cybersecurity requires clear and consistent communication among security practitioners, managers, executives, and government partners. A common language and set of reference points (i.e., internationally recognized standards) enable effective collaboration and robust exchanges, helping to link strategic and tactical activities. For instance, executives may better understand the strategic value of resourcing practitioners to meet their goals, address gaps, or change tactics. Government partners may better understand discrete cybersecurity activities within a broader risk management context. In this way, materials that are understandable and meaningful to practitioners, executives, and government partners can help all stakeholders understand,

The **Cybersecurity Framework**, developed by the National Institute of Standards and Technology (NIST) in collaboration with the industry and civil society stakeholders it convened, is a leading global best practice in cybersecurity risk management, in particular because the structure of the Framework's Core facilitates *clear* communication across organizational boundaries. Risk management guidance is organized across Functions, Categories, Subcategories, and Informative References, which provide varying levels of detail, enabling executives, security practitioners, and government partners to discuss risk management maturity and investments in a coordinated and consistent way.

The Cybersecurity Framework also uses a risk-based approach, driving security outcomes in a flexible manner. Many organizations have highlighted the value of the Framework for their operational risk management, and the Australian, Canadian, Italian, and Japanese governments have translated and utilized it.

measure, and advance cybersecurity risk management practices. Similarly, between or across multiple organizations, such as technology providers and users, clear language with common reference points can facilitate communication around shared security learnings or act as a mechanism for suppliers to share information about their risk management practices.[3]

Risk-based: Cybersecurity risk is like many other types of enterprise risk: it cannot be eliminated; rather, it must be assessed and mitigated to ensure operational security and resiliency. As such, cybersecurity risk management must be considered within a broader context of risk. Efforts to treat cybersecurity risk management apart and separate from other types of risk are inefficient and potentially counterproductive. Visibility and integration into enterprise-wide risk assessments, including those reviewed by corporate boards, will help to promote appropriate investments in people, processes, and technologies that will drive advancements and maturity in cybersecurity.

In 2015, Japan's **Ministry of External Trade and Industries (METI)** published "Cybersecurity Management Guidelines," clearly stating that corporate management should consider cybersecurity *risk* as a part of company-wide risk. Likewise, in 2016, Japan's **National Center of Incident Readiness and Strategy for Cybersecurity (NISC)** stated that cyber security should be considered as an element of business risk.

Moreover, a risk-based approach allows for a company to prioritize its cybersecurity efforts on the basis of its particular context. By conducting a risk assessment, companies can prioritize their resources and better communicate with stakeholders about their efforts. As no organization has unlimited security resources, a risk-based approach allows for consideration of the likelihood of an event and its expected consequences. In this way, companies can adapt to changes in a strategic way as business, technology, or threat factors evolve over time.[4]

Outcome-focused: Outcome-focused approaches provide organizations with sufficient flexibility to manage cybersecurity risk in a way that is consistent with constantly changing threats and technology developments. Specifically, outcome-focused cybersecurity risk management approaches are described in terms of desired security objectives rather than in terms of prescriptive requirements that dictate how those objectives should be achieved. For example, some regulatory approaches highlight the importance of tactical activities like conducting risk assessments, implementing access controls, and developing incident response plans. In doing so, they must appropriately scope the requirements, including considering relevant risk, and allow companies the flexibility to use new or alternative security techniques or capabilities. Rather than limiting an organization's ability to manage risk in a dynamic threat environment, outcome-focused approaches enable organizations to adopt new, more effective tactics that are most appropriate for their architectures and operating environments.

By focusing on desired security outcomes, governments can ensure that requirements work across organizations and over time. To complement those efforts, sector-specific organizations may also develop implementation or capabilities-focused guidance, which should constantly be revised to reflect

[3] On private sector use of the Cybersecurity Framework, see, e.g., https://www.nist.gov/cyberframework/additional-information/rfis (with responses from various U.S. and global companies); Report 429: Cyber Resilience: Health Check, Australian Securities & Investments Commission (2015), http://download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf; Fundamentals of Cyber Security for Canada's CI Community, Public Safety Canada (2016), http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-fndmntls-cybr-scrty-cmmnty/2016-fndmntls-cybr-Scrty-cmmnty-en.pdf; Framework Nazionale per la Cyber Security (2016), http://www.cybersecurityframework.it/; Japanese Translation of the NIST Cybersecurity Framework, https://www.ipa.go.jp/files/000038957.pdf.

[4] There are numerous existing resources to support organizations in implementing risk assessments, including International Standardization Organization (ISO) 31000.

organizational and industry learnings, the evolution of threat models, and the development of innovative security techniques or capabilities. Governments may also reference existing and updated sector-specific guidance in their more static cybersecurity requirements.

Agile: By emphasizing agility, effective cybersecurity risk management approaches allow companies to meet the challenges of today and tomorrow. There is no one-size-fits-all approach to cybersecurity; rather, businesses should have the agility to build from foundational best practices, customizing approaches so that they are most appropriate for their particular technology decisions, risk profile, and threat posture. Approaches that emphasize agility are grounded in an organization's own technology architectures, business structures, and priorities and allow for continuous improvement. While external compliance requirements may provide helpful artifacts, it is essential that those requirements are articulated in a way that embeds flexibility, enabling organizations to continue developing and integrating improved capabilities rather than requiring them to continue demonstrating a status quo capability that is not responsive to the risk environment. Further, such agility allows an organization to iterate and incorporate new learnings over time as threats and vulnerabilities evolve. This approach also enables government partners to engage in a robust, continuous dialogue about industry efforts rather than merely focusing on minimal compliance. As governments transition toward focusing on desired security outcomes and allowing companies sufficient agility in meeting those outcomes, their improved understanding of technology decisions and tradeoffs will inform and advance their risk management efforts.

The **International Organization for Standardization (ISO)** has published "Information technology — Security techniques — Cybersecurity and ISO and IEC Standards" (ISO 27103). This document promotes an outcome-focused and agile approach. It is outcome-focused because it includes a range of desired cybersecurity risk management outcomes as well as references to ISO and IEC standards that may be used to support implementation across different sectors and unique organizations. This approach enables ISO 27103 to be agile, adaptable to different organizations and sectors that seek to achieve common outcomes as the technology and threat landscape change over time.

Additional information is available online:
https://www.iso.org/standard/72437.html
https://webstore.iec.ch/publication/62742

III. The value of alignment in government approaches to effective cybersecurity risk management

As governments develop effective approaches to cybersecurity risk management, we encourage them to track activity across the broader ecosystem. In 2017, the Financial Stability Board reported that: "Seventy-two percent of jurisdictions report plans to issue new regulations, guidance or supervisory practices that address cybersecurity for the financial sector within the next year,"[5] and we anticipate similar developments in other sectors over the next few years. Governments can leverage, build from, and improve existing best practices and standards with demonstrated positive impacts rather than developing one-off and potentially fragmented, untested, and burdensome requirements. Moreover, public-private cooperation is critical to promoting alignment across government approaches to cybersecurity risk

[5] http://www.fsb.org/2017/10/fsb-publishes-stocktake-on-cybersecurity-regulatory-and-supervisory-practices/

management to the greatest extent possible, recognizing that different cultural norms or government priorities will make absolute harmonization unlikely. However, aligning the *approach* and *substance* of cybersecurity risk management policies and ensuring compatibility provides tremendous value to all stakeholders.

In leveraging recognized best practices and promoting alignment across jurisdictions, governments will advance both security and economic opportunities. By utilizing approaches that have already been vetted, implemented, and proven to support improved risk management outcomes, governments and companies alike can reduce costs and increase effectiveness. In addition, such an approach removes barriers to development and adoption, as governments can adopt proven models and companies can focus their efforts on security rather than developing new compliance processes. Greater alignment across jurisdictions also creates opportunity for dialogue and shared learnings and improvements among industry and government organizations that are implementing and iterating on existing best practices.

Such alignment also produces economic benefits for domestic industry. Whereas fragmented approaches present challenges for private sector organizations that operate across multiple jurisdictions, participate in global supply chains, or access global solutions, increasing compliance costs and impeding innovation, aligned approaches reduce costs and promote an open flow of resources and market opportunities. Situated in jurisdictions in which governments are pursuing aligned approaches, domestic companies are able to develop products, services, and solutions that can compete in the global market. Alternatively, companies situated in jurisdictions that develop country-specific requirements may only be able to sell their products, services, and solutions locally. In addition, many local companies develop new products and services by leveraging emerging innovations and ideas that are brought to the global market. To the extent that companies must focus on complying with one-off, untested government requirements, domestic industry may not be able to leverage those new products and services to expand, improve, or secure their offerings. By allowing flexibility and reducing the cost of complying with jurisdiction-specific compliance routines, companies can invest in security innovation and increase collaboration with government partners to address shared challenges.

Conclusion

The guiding principles discussed above can benefit all stakeholders and create lasting approaches that can address both current and future cybersecurity risk and evolving threats. Effective cybersecurity risk management approaches advance security, improve oversight, and promote economic opportunities. Working collaboratively with industry, governments can leverage effective practices and improve outcomes, enabling impacted organizations to focus resources on security, promoting economic opportunity, and ensuring that policies are significantly aligned across sectors and geographies to support an interconnected ecosystem.