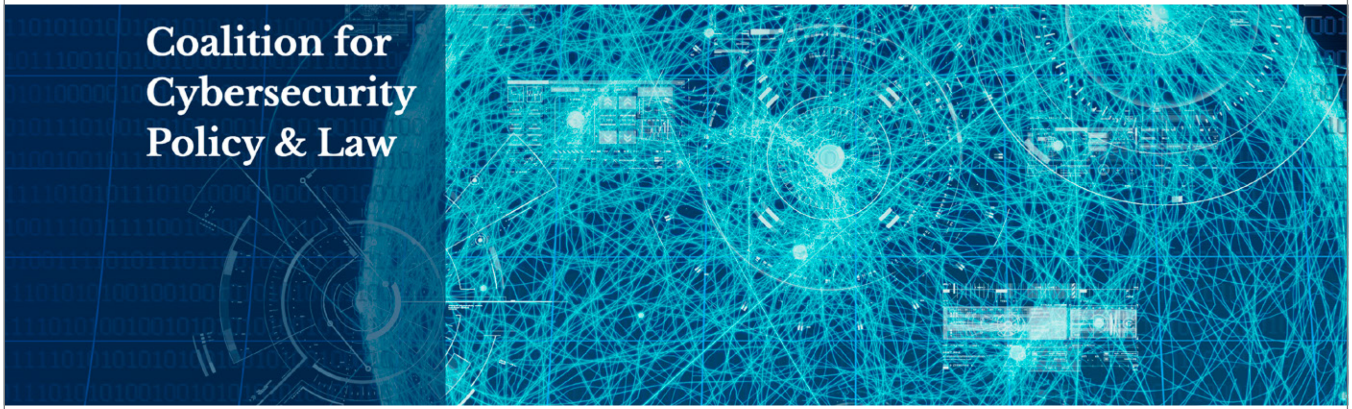
Building a National Cybersecurity Strategy: Voluntary, Flexible Frameworks



Presented by
Coalition for Cybersecurity Policy & Law
10.26.17

CyberNext★DC

I. Executive Summary

This paper begins with an overview of the cyber threat landscape. It is important to understand harmful consequences of cyberattacks as well as how the prevalence of new technologies, including the "Internet of Things," has increased the number of opportunities for cyberattacks. The volume and diversity of cyber threats underscores the importance of developing a framework that is voluntary, flexible, and broadly adopted across organizations of all sizes, and stakeholders at all levels.

Understanding the challenges of effective cyber risk management, it is instructive to consider international models of a national cyber risk management framework to determine which practices have been successful. This paper examines the United States, Italy, the United Kingdom, and Australia as case studies that highlight the most critical components of an effective cybersecurity framework.

As further explained below, an effective cybersecurity risk management framework is one that is: ***(1) prioritized; (2) flexible; (3) repeatable; (4) performance-based;*** and ***(5) cost-effective***. To carry out these five objectives, this paper asserts that organizations must incorporate the following elements into a national cybersecurity risk management framework:

- **DEFINE THE AUDIENCE**
- **ESTABLISH A COMMON LEXICON**
- **PROVIDE IMPLEMENTATION PROCEDURES**
- **INCLUDE AN ORGANIZED AND CATEGORIZED LIST OF ACTIVITIES**
- **ENGAGE IN STANDARDS MAPPING**
- **PROMOTE THE DEVELOPMENT OF INDUSTRY-SPECIFIC PROFILES**
- **INSTITUTE A PROCESS FOR MAINTENANCE**

To ensure broad-based input and stakeholder buy-in, the process of developing a national cybersecurity framework must be one that is the product of public-private collaboration, through an iterative process.

Once the elements of an effective cybersecurity risk management framework have been established, the framework must also be sufficiently customizable to drive organizations towards adoption and implementation. This paper suggests that the development of industry profiles and threat profiles establishes a comprehensive approach to mitigating and addressing risk that can adapt to unique issues, concerns, and practices as they arise in a given industry.

Finally, this paper recognizes that translating a cybersecurity risk management framework should not stop at the industry, sector, or threat level. Instead, this paper encourages the development and deployment of a framework that is flexible enough to be implemented at the organization level.

II. Introduction

The practice of cybersecurity takes effort, investment, coordination, and persistence. Individuals, businesses, industries, and governments must commit resources and work together to design strong and effective cybersecurity measures. To be able to adequately respond to the fast changing nature of the threats and to promote consistency, they must implement these measures guided by a clear framework for managing cyber risk.

This paper argues first that governments should foster the development of appropriate tools for managing cyber risk in the form of a flexible framework. Such a framework should be ***(1) based on a national strategy; (2) developed with wide stakeholder input through voluntary, open, transparent, and participative processes; (3) flexible and adaptable so that it is both capable of being used across sectors but also of being impactful for specific threat profiles and for individual businesses; and (4) aligned with international, voluntary consensus standards.*** Second, the paper then describes the optimal way for governments to consider use of such a framework to pursue effective cyber risk management in a dynamic threat environment without unduly interfering with further technology innovation. Specifically, the paper recommends that wherever feasible, the use of a cyber risk framework should be advanced by governments using market-based incentives. There may be limited situations where regulators determine that the risks are sufficiently great that mandatory regulations may be an appropriate tool. In such circumstances, governments should ensure that any regulations adopted are narrowly targeted at the specific harms to be prevented, process-oriented rather than compliance-oriented, and are built in conformity with how the framework will be used on a voluntary basis in unregulated segments of the economy.

The challenges of mounting a defense against cyberattacks are complex and dynamic. Defense in cyberspace requires integrating a disparate array of people, information sources and technical capabilities to protect assets that can be distributed across many systems and physical locations. Yet careful preparation, a clear strategy, and faithful execution can go a long way. Nations that invest the time, resources, and effort to develop a national cybersecurity framework can reduce the frequency and severity of successful cyberattacks against critical infrastructure, government networks, and private sector assets.

This paper explains the benefits of developing a national, voluntary cybersecurity framework that will provide a roadmap for industry, policymakers, regulators, and other stakeholders. Although this document will lay out common elements associated with successful development of cybersecurity risk management frameworks, it does not espouse the adoption of a specific document, instead focusing on the importance of tailoring the approach to the needs and circumstances of each country.

When shaped and executed as described below, a national cybersecurity framework yields efficient and effective results across all segments of society. A well-crafted framework embraced by the private sector leads to resiliency against evolving threats, which, in turn, means better reliability and availability of business services in the economy. Nations in which cybersecurity planning is ad hoc, nonexistent, or burdened by government overreach face more difficult challenges and more painful outcomes.

III. Building a National Strategy for Cybersecurity Risk Management

The goal of cybersecurity risk management is to move to and maintain a desired, optimal cybersecurity state based on the unique needs, considerations, and best practices of the organization's industry and business model. The goal of a national strategy is to adopt approaches on a country-level that foster more effective and efficient cybersecurity risk management by organizations operating in a given country.

a. Cyber Risks and Vulnerabilities

Events in recent years have made it clear that organizations of all sizes must better manage their cyber risks in order to avoid harmful consequences. Cyber incidents can lead to privacy breaches, identity theft, legal and reputational harm, business disruption, and bankruptcy. When directed against critical infrastructure, cyberattacks can affect the availability of basic public necessities like water and electricity, which can lead to political instability, civil unrest, and the loss of human life.

Rapid technological innovation presents new and unique cyber risk challenges. While connected device technology and the broader "Internet of Things" ("IoT") has already demonstrated great value to the economy and to society, its deployment increases the breadth and depth of cyber risks. With the rapid proliferation of "smart" devices, the available targets for cyberattacks has vastly increased as has the value of the data that new technology is producing. This data creates a powerful incentive for a range of malicious actors, including isolated criminals, organized crime syndicates, and foreign states, to attempt cyberattacks to gain access to rapidly increasing collections of information. Beyond the data, the IoT brings a dramatic increase in the physical consequences of cyberattacks, as thermostats, appliances, automobiles, medical devices, and many other devices found in homes and business everywhere become targets for disruption.

Cyberattacks are increasing in number, sophistication, and rate of success, and their potential for causing financial damage, loss of human capital, and physical destruction continues to climb. The situation demands that leaders and policymakers pursue a thoughtful, deliberate, and holistic approach to cybersecurity that encourages all organizations, entities, and institutions in society to assess their cyber risks and implement changes to mitigate these risks on a continual basis.

b. Develop and Use a Cyber Framework

Addressing these risks must include a national strategy for cybersecurity that can only emerge from a robust understanding of the unique risks facing the nation's cyber infrastructure, data, and digital services. Most countries face the same basic risks to cybersecurity, including cybercrime, cyber espionage, or IP theft. In some circumstances, a single framework that helps mitigate these common risks can have international applicability. However, the relative scale and importance of certain cyber threats can vary greatly from country to country. Ultimately, every nation has a different set of circumstances in this regard. The cybersecurity risk profile is different for Spain and Samoa, for example. As a first step toward building a framework to manage cybersecurity risks, the government and private sector must have a clear understanding of the threats and vulnerabilities they face together and then shape a strategy to confront this reality.

Traditionally, cyber risk management relied heavily on the development of periodic reports or "checklists" to measure compliance. Such an approach is static in its controls and objectives and rigid in its implementation. Moreover, given the dynamic nature of the threat environment, such an approach is unlikely to produce results that lead to optimal mitigation of cyber risks, leaving organizations and individuals exposed to attack and often with a false sense of security.

A cybersecurity risk management framework is only as strong as the willingness of stakeholders to use it. This is due in part to the fact that digital technologies bind organizations together through their supply-chains, partnerships, constituents and customers. To build a cybersecurity framework and maximize its adoption, care must be taken to ensure that it incorporates the economic, political, and cultural factors that interact with the cyber realm for organizations of all types. For example, in some cases a national cyber framework will reflect a particular society's general trust in and historic dependence on government regulators to measure or validate private sector adoption of norms and standards, while in other cases the framework may be built on the expectation that adoption will be driven by self-regulatory bodies, independent auditors, or industry associations. Factors such as the different types of corporate entities that are common, as well as the public ownership of utilities or other industries, may also affect the way in which a national framework is constructed.

Regardless of the unique parameters that reflect a framework's tailoring to national priorities, one element should remain present in any national cybersecurity framework—that its adoption is voluntary. Voluntariness is a key concept that allows organizations to buy into the national framework and seek to implement it in a flexible and efficient manner appropriate to their sector or industry, and reflective of the risks that are most relevant to them. Making a framework voluntary rather than mandatory also encourages both stakeholders in cybersecurity policy and the organizations implementing the cyber risk management processes to provide feedback to improve the framework. Similarly, basing the framework on international, voluntary consensus standards insures that the framework is constantly updating as the standards improve. This reassurance helps stakeholders understand how their views will improve—but not necessarily impose new burdens upon—those who engage. The goal is to develop an approach that all organizations across the economy will want to implement. This, in turn, will lead to greater adoption and better outcomes not generally achieved by mandatory compliance.

Moreover, when voluntary adoption is paired with market incentives, the rate of adoption rises substantially. For example, an organization adopting a national cyber framework could be offered certain competitive advantages. Incentives may include insurance premium discounts, tax breaks, or other policy tools. These incentives provide a basis for encouraging full marketplace participation rather than selected sector-based compliance regimes that rely on enforcement.

The voluntary model has worked exceedingly well in fostering innovation while ensuring that interoperability and security are adhered to the extent possible within any given industry. Still there may be situations where mandated regulations are appropriate. In these cases, governments should narrowly target regulations at the specific harms to be prevented and stay away from compliance-oriented checklists and instead focus on risk management and process-oriented controls.

Given the global market focus of Commercial off the Shelf (COTS) technology providers, governments should support alignment with international, consensus-driven standards in risk management frameworks, rather than country-specific requirements aimed at individual market concerns. Utilizing international, consensus-driven standards enables technology companies to focus their resources on enhancing security solutions that can scale for the global market, rather than on making a multitude of adjustments to ensure compliance with a series of static requirements and specifications.

Ultimately, the key to long term and broad success of any standardized framework is how effectively it enables participation by all interested stakeholders, whether at the national or international level. The more inclusive participation is, the more likely the framework will see rapid adoption.

IV. Examples of Voluntary National Frameworks

Several countries have led the way in preparing national cybersecurity frameworks that serve as models for how to develop effective frameworks for widespread adoption. The examples below are illustrative, but not exhaustive. As countries increasingly consider cybersecurity to be a national and economic security issue, strategies and frameworks will be developed and promulgated within many nations.

a. United States

STRONG HISTORY OF VOLUNTARY STANDARDS DEVELOPMENT. The United States has a long history of developing voluntary standards by and for the private sector. In some instances, such standards begin as requirements for the Executive Branch of the US. Government, advanced via Executive Order or developed by the Office of Management and Budget ("OMB") for departments and agencies. In other cases, independent organizations develop recommendations for voluntary standards in a particular area, and over time the standards are adopted by a sector-specific regulator, accepted by consensus, or through mutual agreements in the marketplace. For example, in response to concerns regarding the collection of consumers' web browsing information and use for targeted advertising purposes, the digital advertising industry organized the Digital Advertising Alliance ("DAA") in 2008 and released the Self-Regulatory Principles for Online Behavioral Advertising. While voluntarily developed, the DAA Principles were accompanied by enforcement programs that were designed for industry to hold itself accountable. Since the launch of the DAA Principles, the program has been viewed as a success by regulators and industry alike, and has led to a series of additional standards and applications that have helped the digital advertising ecosystem evolve in a responsible yet flexible fashion.

Similarly, the U.S. Consumer Product Safety Commission ("CPSC") encourages manufacturers to engage with voluntary standards organizations to develop safety standards for a variety of consumer products. These standards are developed by private organizations that bring together industry groups, government agencies, and consumer groups to agree on the best consumer product safety practices. Some of the standard development organizations include those focused on home appliances, outdoor power, automotive standards, window coverings, and pyrotechnics. Standards have been developed for a many products, ranging from mattresses to generators to smoke alarms.[1] These standards ultimately are codified in the Code of Federal Regulations and carry the force of law. They are viewed by regulators as a "floor," and not a "ceiling," which is to say that manufacturers are encouraged to think of additional ways to protect consumers and not to view the standards as a strict maximum compliance protocol.

Another example of industry self-regulation is the Payment Card Industry (PCI) Standards Development Council. This group of credit card and financial companies voluntarily developed the Digital Security Standard (DSS) for organizations to adhere to when accepting credit card transactions as part of their business. They update using consensus as new technologies and threats emerge.

It is important to recognize that public-private collaboration is essential for voluntary standards. For over one hundred years, the U.S. government has turned to its non-partisan scientific agency, the National Institute for Standards and Technology

[1] See Memorandum From Patricia Edwards, Voluntary Standards Coordinator, to CPSC Commissioners (Nov. 16, 2016), https://www.cpsc.gov/s3fs-public/VoluntaryStandardsActivitiesFY2016AnnualReport.pdf.

("NIST") to develop and promote technical and scientific standards needed in areas intersecting public policy matters. For the private sector, NIST helps produce standards that are voluntary and developed in conjunction with—and reflecting the consensus of—industries that will be leveraging the standards for application.

DEVELOPMENT OF THE CYBERSECURITY FRAMEWORK. In the area of cybersecurity, NIST provides standards and guidance for government entities to adopt, focusing on privacy and data security concerns and risk management processes. In February 2013, President Obama issued an Executive Order calling for the development of a voluntary risk-based cybersecurity framework comprised of a set of industry standards and best practices to help organizations manage cybersecurity risks.[2] The ensuing process took a year and involved the coordination of hundreds of public and private sector organizations, resulted in the development of the NIST Cybersecurity Framework for Critical Infrastructure. Since its release, the NIST Cybersecurity Framework has been successfully adopted in a wide range of contexts in the U.S. government and private sector marketplace, including those that fall outside the critical infrastructure designation.

The NIST Framework consists of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across sectors, which provide detailed guidance for developing individual organizational Profiles. Through use of the Profiles, the Framework aims to help organizations align their cybersecurity activities with business requirements, risk tolerances, and resources. The Framework Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk.

b. Italy

In 2016, a consortium of Italian cybersecurity academic and scientific entities led by the CINI Cyber Security National Lab released a "National Cyber Security Framework" for Italy.[3] The President of the Council of Ministers of the Italian government participated in the preparation of the national framework.

The Italian National Framework is modeled after the NIST Framework, with tailoring for Italian production context and a focus on small and medium enterprises.[4] Importantly, the process used to develop the Italian National Framework leverages a similar multi-stakeholder development model to the NIST Framework. This yields a compatible approach to NIST's but allows for customization to better fit the Italian market. The Italian National Framework builds off of the basic elements from the NIST Framework – Framework Core, Profile and Implementation Tiers. However, the Italian Framework adds priority and maturity levels to the Framework Core. It also introduces the notion of Framework contextualization, namely that a company that would like to use the Framework should first identify a "contextualization" or current state, according to which it can evaluate its actual risk profile.

Flexibility is a key component of the Italian Cybersecurity Framework. The document emphasizes that the framework is "not a security standard, but a common reference to identify existing and future sector standards and regulations."[5] This means that the task of defining standards is expressly contemplated as being committed to national and international standardization bodies and institutions, in conjunction with industry regulators. In accordance with this collaborative and international approach, Framework use is described as voluntary.[6]

[2] Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" (Feb. 12, 2013)

[3] ROBERTO BALDONI, LUCA MONTABARI, CYBER INTELLIGENCE AND INFORMATION SECURITY CENTER, CYBER SECURITY NATIONAL LABORATORY, ITALIAN CYBER SECURITY REPORT (2016), http://www.cybersecurityframework.it/sites/default/files/CSR2015_ENG.pdf

[4] *Id.* at X.

[5] *Id.* at 10.

[6] *Id.* at 14.

According to the Italian Framework, one of the key advantages for having a national framework integrated with international standards and norms is the ability to generate public-private-national research, through integrated technology programs, joint research centers, and other initiatives. This allows for the identification of common technology reference points for defense and crisis management operations. This national, voluntary approach is calibrated to yield a more robust and effective cybersecurity services industry, having gained the benefit of collaboration with the government, academia, and other centers of cybersecurity expertise. The result is to foster a marketplace where the bar has been raised high enough to push the cyber services sector further and harder than otherwise.

c. United Kingdom

The Government of the UK has been actively engaged in developing a national, voluntary cybersecurity framework for several years. In 2012, multiple entities in the UK Government—the CESG (the Information Security Arm of the GCHQ), the Cabinet Office of Cyber Security & Information Assurance, the Centre for the Protection of National Infrastructure, and the Department for Business Innovation & Skills—together released a practical guidance document entitled “10 Steps to Cyber Security.” The steps were not intended to be an exhaustive guide to confronting potential cyber threats or mitigations, but nonetheless covered a range of cyber issues, including malware protection, monitoring, secure configuration, and incident management.

Since its first issuance in 2012, the 10 Steps document has been updated several times and is now provided by the Government in a streamlined website and accompanied by a number of related materials designed for specialized advice for particular audiences.[7] For example, there is an accompanying paper entitled “10 Steps: A Board Level Responsibility,” as well as 10 Step technical documents for practitioners and specialists. The materials are provided now by a newly created government entity, the National Cyber Security Centre (“NCSC”), which was launched in October 2016 to replace and consolidate several cyber security functions in the UK Government.

In 2014, the Government released a “Cyber Essential Scheme”, which complements the 10 Steps documents that the Government provided as part of its national approach to cybersecurity, and was intended to fulfill two functions.[8] First, it provided a clear statement of the basic controls that all UK organizations were encouraged to implement to mitigate the risk from common Internet based threats, within the context of the 10 Steps. The five technical controls it sets forth to protect against “commodity threats” include access controls, boundary firewalls and Internet gateways, malware protection, patch management, and secure configuration, and were designed to address the vast majority of cyberattacks that use relatively simple methods to exploit basic vulnerabilities.

Second, Cyber Essentials is designed to be used alongside an “Assurance Framework” in order to offer a mechanism for organizations to demonstrate to customers, investors, insurers, and others that they have taken these precautions.[9] Organizations that obtain this assurance—i.e., get certified by an accredited body as having implemented the Cyber Essentials—results in a number of other benefits, including the ability to bid for Government contracts, which otherwise is not available to organizations that are not certified to the Cyber Essentials.[10] In this sense, the UK’s voluntary framework applied to the private sector has the added benefit of improving and securing the Government’s supply chain.

[7] *See* National Cyber Security Centre, 10 Steps to Cyber Security (2016), https://www.ncsc.gov.uk/guidance/10-steps-cyber-security.

[8] *See* HM GOVERNMENT, CYBER ESSENTIALS SCHEME SUMMARY (2014), https://www.cyberaware.gov.uk/cyberessentials/files/scheme-summary.pdf.

[9] *See* HM GOVERNMENT, CYBER ESSENTIALS SCHEME ASSURANCE FRAMEWORK (2015), https://www.cyberaware.gov.uk/cyberessentials/files/assurance-framework.pdf.

[10] *See* Procurement Policy Note 09/14: Cyber Essentials scheme certification (Sept. 26, 2014), https://www.gov.uk/government/publications/procurement-policy-note-0914-cyber-essentials-scheme-certification

These successful initiatives and efforts by the UK Government grew out of a National Cybersecurity Strategy that was first published by the Government in 2011.[11] In that strategy document, the Government committed to raising awareness and educating the public and firms on cybersecurity protection and prevention, on the basis that "80% or more of currently successful attacks exploit weakness that can be avoided by following simple best practice."[12] Specifically, the Government stated that it would "provide clear cyber security advice for use by anyone using the internet so that people can decide how they want to use cyberspace, informed of the risks."[13] The voluntary initiatives noted above derived from this 2011 commitment, and were updated and expanded in the UK's National Cybersecurity Strategy of 2016, which set forth a five-year vision for making the UK secure and resilient to cyber threats and economically competitive in the cyber economy.[14]

d. Australia

In 2016, the Australian Prime Minister's Office released "Australia's Cyber Security Strategy," a document that set forth a comprehensive set of principles, objectives, and initiatives for addressing and mitigating cyber risks and threats.[15] At the outset, the Strategy noted that while the Australian Government would take a lead role in promoting action to protect online security, much of the country's digital infrastructure is owned by the private sector. Therefore, efforts to secure Australia's cyberspace must be a shared responsibility…and it will be important that businesses…work with governments and other stakeholders to improve [Australia's] cyber defenses and create solutions to shared problems."[16] The Strategy recognizes as a fundamental principle that "cyber security cannot be left to the Government alone to solve…organizations and individuals play an essential role in effectively reducing cyber security risk."[17]

As a practical matter, the Strategy describes this approach as providing for a "National Cyber Partnership," in which the Australian Government and business leaders will set the strategic agenda through annual Cyber Security meetings hosted by the Prime Minister.[18] At the organizational level, the Strategy states that "Governments, businesses and the research community will co-design ***national voluntary cyber security guidelines*** to promote good practice" for use by all organizations.[19] The Strategy announced that these guidelines "will be based on world class strategies developed by the Australian Signals Directorate and aligned with international standards where possible." Also planned are "voluntary cyber security governance health checks" that are intended to help organizations understand their cyber security strengths and gaps. Although the guidelines are voluntary, the Strategy contemplates a self-regulation mechanism for encouraging its use.[20]

A critical component of the Australian Cyber Security Strategy is its clear orientation toward boosting cyber security innovation and the expansion of the nation's cyber services sector into new markets. The approach focuses on research, development, and diversification that is responsive to the needs of industry and government, both domestic and overseas. The goal is to generate investment and jobs to make Australia a more attractive destination for businesses to invest and grow. The Strategy cross-references other agendas and strategies tied to science and innovation initiatives elsewhere in the Government. Thus, Australia is positioned to defend against cyber risks but also take advantage of the opportunities that the growth of cyber marketplace offers.

[11] *See* UK CABINET OFFICE, THE UK CYBER SECURITY STRATEGY: PROTECTING AND PROMOTING THE UK IN A DIGITAL WORLD (2011), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf.

[12] *Id.* at 26.

[13] *Id.* at 31.

[14] *See* UK CABINET OFFICE, NATIONAL CYBER SECURITY STRATEGY 2016-2021 (2016), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

[15] *See* AUSTRALIAN GOVERNMENT, AUSTRALIA'S CYBER SECURITY STRATEGY (2016), https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf.

[16] *Id.* at 5.

[17] *Id.* at 20.

[18] *See id.* at 21-26.

[19] *See id.* at 7 (emphasis added).

[20] *Id.* at 35.

The National Cyber Security Strategy set forth priorities that were captured in the Australian Government Information Security Manual ("ISM"), issued by the Australian Signals Directorate.[21] The ISM exists to assist Australian government agencies in applying a risk-based approach to protecting their information and systems. A similar document exists for risk management of outsourced ICT arrangements when Australian Government information is involved.[22]

V. Features of a Voluntary Cybersecurity Framework

a. Risk Management Best Practices

It is critical to note that a national cybersecurity framework, while intended for widespread applicability and uniformity in addressing the seriousness of the problem, should not be drafted at such a high level as to encourage a generic, "one-size-fits-all" approach to cybersecurity risk management. The objective in drafting a national framework is to be flexible but also have a sufficient level of granularity that it can be used to develop specific "industry profiles". The goal should be to aim for a balance between a comprehensive and evolving set of standards and an organization's understanding and management of its specific risk, both independently, and in conjunction with its sector and partners.

The hallmark of an effective cybersecurity risk management framework is one that leads to prioritized, flexible, repeatable, performance-based and cost-effective measures designed to manage cyber risks identified in a risk assessment.

PRIORITIZATION. Prioritized risk management means a program that is able to determine and rank the severity of cyber risks to promote the successful operation of the organization. This requires an effort to identify cyber assets, classify their value to the organization, identify potential vulnerabilities, and determine the probability of attack, among other steps. While organizations are often able to identify cyber assets and classify their value to the organization on their own, they often need help from third parties to identify potential vulnerabilities and determine the probability of attack. Organizations benefit from relying on the expertise of coordinated efforts including Information Sharing and Analysis Centers (ISACs) and Computer Emergency Readiness Teams (CERTs), as well as cybersecurity companies to appropriately asses the probability of attack and relative risks. Collaborating with these third parties helps organizations identify a hierarchy of risks to manage, a step that is critical for optimizing the process of and results obtained from risk management.

FLEXIBILITY. A cybersecurity risk management framework must be usable to the wide variety of organizations it seeks to cover. Flexible risk management means a program that can be adapted and adjusted to meet the needs of a variety of organizations and meet these needs over time as the organization changes. For example, a single framework should be able to address cybersecurity issues across industry sectors, and be used by different audiences within an organization, from executives down to operations. It is also important that a framework be technology neutral, to avoid creating bias towards any vendor or solution.

Other factors may affect a single organization that changes over time, such as the size, scope of activity, structure, organization, partnerships, industry sector, technology, and focus. These factors are able to be incorporated and reflected in a flexible program for risk management. In the cyber context, flexibility is key given the rapid nature of technological development.

[21] *See* AUSTRALIAN GOVERNMENT, INFORMATION SECURITY MANUAL (2016), https://www.asd.gov.au/infosec/ism/index.htm.

[22] *See* AUSTRALIAN GOVERNMENT, ATTORNEY-GENERAL'S DEPARTMENT, PROTECTIVE SECURITY POLICY FRAMEWORK (2015), https://www.protectivesecurity.gov.au/informationsecurity/Pages/RiskManagementOfOutsourcedICTArrangements-IncludingCloud.aspx.

REPEATABLE. A cybersecurity risk management framework must be constructed to ensure that risk assessment, prioritization, and mitigation are routine, ongoing processes. Cybersecurity is a dynamic discipline that requires constant vigilance. Integrating the cybersecurity risk management process into routine organizational operations is key to ensuring that cyber risks are identified and addressed quickly and effectively.

PERFORMANCE-BASED. Because the framework is expected to be usable by a diverse set of organizations, it is important that it focus on outcomes, rather than highly granular, or overly-prescriptive control recommendations. The performance outcomes should be measurable in ways that allow for organizations or sectors to develop innovative means to meet the intent of the control. A focus on performance also ensures that measures will remain viable for longer periods of time, as technology continues to advance.

COST-EFFECTIVE. Implementing security comes with unavoidable costs. However, a flexible and adaptable framework will allow for stakeholders to implement controls that will address actual risks, helping to keep costs at manageable levels. Organizations that are guided by a flexible approach to risk management are less susceptible to the unnecessary costs that accompany prescriptive requirements, which often place pressure on organizations to adopt the latest trend. Inflexible approaches, such as those that rely on checklists or prescriptive standards, create costs through the implementation of controls that may be of little to no value in a particular circumstance.

b. Elements of a Framework

The strategic goal of encouraging all organizations to improve their cybersecurity risk management on an ongoing basis can be advanced by incorporating the following elements when constructing a national cybersecurity risk management framework:

- **AUDIENCE:** The framework should specify and delineate its scope by clearly identifying the intended audience. The audience could include regulators, publicly-owned entities or institutions, the private sector, critical infrastructure, etc.

- **COMMON LEXICON:** The framework should establish a common language and set of definitions that describe cybersecurity risks, actions, practices, and responses, from which all organizations, public and private, small and large, can draw in order to design and apply the risk management framework for their specific circumstances. A common lexicon that uses clear language makes cybersecurity risk management accessible not only to all organizations, but also to all actors within these organizations, from management to field operations.

- **IMPLEMENTATION:** The framework should provide an explanation of how to use and apply it to conduct cyber risk management, including a description of maturity levels or other means to help organizations set reasonable baselines and voluntarily measure progress.

- **ACTIVITIES:** The framework should present an organized and categorized list of cyber activities and desired outcomes to represent the cybersecurity risk management universe for industries and organizations to examine when designing an individualized risk management program. An example of a list of cyber activities and outcomes is the “Framework Core” in the NIST Framework. Such a list could reference existing standards, controls, and other frameworks that already exist in other contexts or that would supplement the list.

- **STANDARDS MAPPING:** The drafters of the framework should identify other cybersecurity and related standards used in the government and private sector and map these standards to the framework's list of activities and outcomes. The exercise of mapping the various existing sets of standards to a single set of activities and outcomes in a national framework will ease the burden of information security professionals that in most context are applying varying—and at times conflicting—sets of standards.

- **PROFILE DEVELOPMENT:** The framework should be oriented to promote the development of industry-specific profiles that are necessary to drive adoption of the framework at the organizational level. Profiles that are based on the framework and tailored to specific industries and threats help organizations identify opportunities for improving their cybersecurity posture by comparing their "current state" with a "target state."

- **MAINTENANCE:** The framework should include a description of the process and expectations for soliciting and incorporating updates and the consensus-based profiles developed based on the framework. This element is necessary to ensure that over time, the framework is updated to reflect changes in technology or new ways of understanding and mitigating risk.

c. Process of Development

The process of developing a national cybersecurity framework should be geared toward public-private collaboration to ensure broad-based input and stakeholder buy-in. In particular, the government should view its role as both a coordinator and a stakeholder, as well as in some cases, an author of the framework. Ideally, the public agency or coalition that is leading the process of developing a framework should convene workshops with stakeholders for soliciting ideas and for educating about the elements of the framework that are being considered. The process of drafting the framework should be iterative, allowing for evolution of the framework's substance and methodology.

VI. Customization

a. General

Customization allows for the alignment of standards, guidelines, and practices in the framework to one or more implementation scenario. The NIST Cybersecurity Framework refers to this as "profiles." A successful cybersecurity framework is one that provides a clear path for developing industry-specific profiles that drive member organizations to adopt and implement cybersecurity risk management programs and practices that are optimized for the set of issues that are unique to the industry. In addition to developing industry profiles, stakeholders and adopters also can use a cybersecurity framework to develop specific threat profiles that can be applied by individual organizations that have identified the threat as a unique concern. In both cases—industry and threat profiles—the elements are drawn from the framework and given more contour and detail for customization to the target state.

Although all organization can and should seek to customize their risk management program to their specific circumstances, some organizations, particularly small business and individuals, often require additional guidance due to resource constraints. In the United States, NIST has published a guide for small business and the UK has the NSCS. These guidelines are consistent with the broader and more complex risk management approaches, but are streamlined and prioritized in the way that help resource constrained organizations to make significant security improvements.

Regardless of whether a profile is developed with, or independent of, government regulators or other actors, the industry profile should reflect consensus among its most prominent members and organizations.

b. Industry Profile

An industry profile is intended to help industries develop cyber risk management plans that align with sector goals, best practices, risk tolerances, and resources. The goal is for industries to follow the same process for adopting the framework but arrive at a different "Profile" for each separate industry based on unique issues, concerns, and practices of that industry.

For example, in the United States, the telecommunications sector, through the Communications Security, Reliability and Interoperability Council ("CSRIC"), prepared in 2015 a report on cybersecurity risk management and best practices for telecommunications entities to use when adopting and implementing cybersecurity risk management programs.[23] The CSRIC working group began preparing the report—which constitutes the sector's framework profile—after completion of the NIST Cybersecurity Framework and with the aim of incorporating the Framework's methodology. According to the document, the working group was given the task of developing voluntary mechanisms that give the Federal Communications Commission and the public assurance that communication providers are taking the necessary measures to manage cybersecurity risks across the enterprise.[24] Critical to the success of the CSRIC effort was the fact that all of the major telecommunications providers participated in the preparation of the report and supported its release. This leadership by the foundational members of an industry help drive adoption across the entire industry ecosystem.

Another example of an industry profile is the NIST Framework Profile created for the manufacturing sector.[25] This document was created to represent a "Target Profile" that focuses on the desired cybersecurity outcomes and provides a roadmap to the ideal end-state state of cybersecurity posture of the manufacturing system. According to the document, an individual manufacturer could use the manufacturing profile in a number of ways, including to express cybersecurity risk management requirements to an external service provider, and to express its cybersecurity state through a Current Profile to report results relative to the Target Profile, or to compare with acquisition requirements.

As explained below, individual organizations can use profiles to develop more specific and tailored profiles that more clearly describe risk management priorities for the organization, but built and developed from the industry profile.

[23] CSRIC WG4, https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf.
[24] *Id.* at 4.
[25] http://csrc.nist.gov/cyberframework/documents/csf-manufacturing-profile-draft.pdf

c. Threat Profile

In addition to developing industry profiles, a framework can be used to create threat mitigation profiles for cross-industry threats that require a comprehensive approach to mitigate and address risk. Such a “Threat Profile” would allow organizations to address a specific threat based on experience, intelligence, or evolution of their practices and services where a sector-specific Profile is not specific enough.

For example, cybersecurity stakeholders could use the framework to develop specific profiles for important cross-industry threats, such as DDOS attacks, insider threats, malware, and others. These threat profiles should be used to provide guidance in addition to the industry or organization specific profiles.

d. Adaptation and Implementation at Organizational Level

The development and deployment of framework profiles by stakeholders allows for the customized and efficient implementation of cybersecurity risk management at the organizational level. However, for organizations looking to implement one of these profiles, the translation of the framework’s principles need not stop at the industry, sector or threat level, but rather can continue to be adapted to reflect the specific risks and priorities of the organization.

FLEXIBILITY. Profiles should be regarded as flexible enough to accommodate organizational adaptation, and organizations should be encouraged to adapt framework profiles to specific organizational features, practices, activities, and plans. One avenue of adaptation could come from an organization’s broader enterprise risk management program. The process of implementing the cybersecurity framework profile for the industry could be adapted to complement—not replace—the organization’s existing cyber and risk management programs, which would entail modifications in some of the cyber activities set forth in the profile.

IMPLEMENTATION. At the organizational level, implementation of a profile is a multi-step process. First, the organization must measure its current cybersecurity posture. Then, using the results of this risk assessment and drawing from the industry profile, the organization must describe its target state, as modified to reflect organizational parameters and priorities. The target state is then compared with the current state, and the comparison yields information about gaps that represent cyber risks requiring a determination on remediation. Finally, after a plan for prioritized and cost-effective risk mitigation is implemented, the organization must measure its progress toward the target state.

Coalition for
Cybersecurity
Policy & Law

cybersecuritycoalition.org