©iStockphoto/Ljupco

The NIST Cybersecurity Framework

Data breaches in organizations have rapidly increased in recent years. In 2014, the National Institute of Standards and Technology (NIST) issued a voluntary framework that is fast becoming the de facto standard for organizations to assess their cybersecurity programs.

RICHARD RAYSMAN
PARTNER
HOLLAND & KNIGHT LLP

Richard's practice concentrates on computer law, outsourcing, complex technology transactions and intellectual property. He has significant experience in structuring technology transactions and has represented clients in billions of dollars of outsourcing transactions in addition to litigating reported cases. Richard is a guest contributor to *The Wall Street Journal* on technology issues, and *Chambers* has selected him as a leading technology attorney. Prior to practicing law, Richard was a systems engineer for IBM Corporation.

JOHN ROGERS
CHIEF TECHNOLOGIST
BOOZ ALLEN HAMILTON INC.

John has extensive information security experience in a variety of industries including financial services, retail, healthcare, higher education, insurance, non-profit and technology services. He focuses on improving client cybersecurity programs, assessing these programs against industry standards, designing secure solutions and performing cost/benefit analyses.

Despite major efforts to prevent cyber attacks, no common standard of care exists yet for organizations to assess their cybersecurity programs. While global cybersecurity spending is expected to exceed $50 billion in coming years, the proliferation of high-profile data breaches continues and remains a growing concern in both the US and globally.

To address these concerns, President Obama issued Executive Order 13636, *Improving Critical Infrastructure Cybersecurity* (cybersecurity executive order) on February 12, 2013. The cybersecurity executive order directed the US Department of Commerce's National Institute of Standards and Technology (NIST) to work with stakeholders to develop a voluntary framework for reducing cybersecurity risks to critical infrastructure. As a result, on February 12, 2014, NIST released its *Framework for Improving Critical Infrastructure Cybersecurity* (Framework).

The Framework is a risk-based approach to cybersecurity that provides a methodology to develop a cybersecurity program within an organization but does not provide concrete security recommendations. NIST is a non-regulatory federal agency and the Framework is voluntary. Therefore, the Framework does not form the basis for any formal regulations or regulatory action. However, the cybersecurity executive order directed the federal regulatory agencies to assess their regulations and guidance against the Framework. Accordingly, it is possible that the Framework may become the standard for federal cybersecurity regulations. There is a growing consensus that it is fast becoming the de facto standard for private sector cybersecurity.

By implementing the Framework's approach to developing a cybersecurity program, organizations can:

- Assess and work toward a plan to improve their cybersecurity.
- Potentially avoid the conclusion that they were negligent or inattentive to cybersecurity best practices in the event of an incident.

This article discusses:

- The Framework's development, scope and structure.
- NIST publications and other federal guidance supporting the Framework.
- How organizations can use the Framework to assess and improve their cybersecurity programs, including practical steps to implement the Framework.

THE FRAMEWORK'S DEVELOPMENT AND SCOPE

NIST developed the Framework through a series of workshops held across the US with:

- Input from more than 3,000 individuals and organizations.
- Responses to Requests for Information (RFI) that NIST solicited from industry.

The Framework is a strong step forward for standardizing the process for developing, organizing and managing cybersecurity programs. It features a flexible, logical structure created from the best of existing standards, guidelines and practices.

CYBERSECURITY RISKS AND FEDERAL GOVERNMENT RESPONSE

NIST developed the Framework in response to growing cybersecurity risks and as part of expanded federal efforts to address those risks.

Cybersecurity Risks

Cyber attacks have become increasingly common and have affected virtually every industry, including education, healthcare, energy and finance, as well as the government. State-sponsored hackers that target critical infrastructure present a growing threat, as seen in 2014 by:

- The cyber attack on Sony Motion Pictures believed to have been orchestrated by the North Korean government.
- A series of coordinated attacks on banks believed to have been sponsored by the Russian government.

Methods of cyber attacks evolve rapidly. In the last several years, there has been a consensus growing among security experts that while preventive measures may stop or limit some cyber attacks, it is virtually impossible to eliminate the possibility of a successful cyber attack.

In a recent study conducted by the Ponemon Institute, 50% of respondents that were victims of a data breach said they should have been able to prevent the breach with the technology they currently had in place and 65% of those respondents noted that the attacks evaded their preventative security measures. Even more surprising, 46% of respondents accidentally discovered the breach. (*Ponemon Institute, 2014: A Year of Mega Breaches, January 2015*.)

The Framework is a strong step forward for standardizing the process for developing, organizing and managing cybersecurity programs.

Cyber attacks can have devastating consequences for organizations, including:

- Operational costs associated with asset recovery and system downtime.
- Regulatory investigations or actions.
- Litigation.
- Reputational harm.
- Customer loss.
- A decrease in shareholder value.

Search Cyber Attacks: Prevention and Proactive Responses and Common Gaps in Information Security Compliance Checklist for more on security measures and preventing cyber attacks.

Cybersecurity Executive Order

The cybersecurity executive order called for several action items to strengthen critical infrastructure cybersecurity. In addition to ordering NIST to develop the Framework according to specific guidelines, among other things, the cybersecurity executive order directed:

- Cybersecurity policy coordination across government agencies.
- Cybersecurity information sharing between the government and industry.
- That regulatory agencies:
  - assess their cybersecurity regulations against the Framework once developed; and
  - create a voluntary program to support adoption of the Framework.

The cybersecurity executive order and the concurrently released *Presidential Policy Directive - Critical Infrastructure Security and Resilience* placed responsibility with the Department of Homeland Security (DHS) to coordinate federal regulatory efforts and identify critical infrastructure industries.

Increased Federal Cybersecurity Guidance

In the year between the cybersecurity executive order and the Framework's release, federal agencies increased their activity in the cybersecurity area. Measures taken included:

- The Securities and Exchange Commission issued its *Identity Theft Red Flag Rules*.
- The Office of the Comptroller of the Currency (OCC) issued its *Bulletin 2013-29, Third-Party Relationships: Risk Management Guidance*.
- The Federal Financial Institutions Examination Council issued its *Social Media: Consumer Compliance Risk Management Guidance*.
- The Federal Reserve issued its *Guidance on Managing Outsourcing Risk*.

Underscoring the importance of managing cybersecurity risks, each of these federal agencies in their guidance or regulations assigned cybersecurity responsibilities to senior management and boards of directors. For example, the OCC guidance on third-party relationships vests in the board and senior management responsibility for:

- Overseeing overall risk management processes.
- Reviewing and approving management plans when using third parties for critical activities.
- Developing and implementing the third-party risk management process.

Given the growing emphasis on vesting cybersecurity responsibility with senior management (who may not have technical backgrounds) and the need for information sharing across organizations, the importance of developing a common cybersecurity taxonomy has increased.

THE FRAMEWORK'S SCOPE

The Framework includes recommended practices for organizations within critical infrastructure industries. It is:

- Voluntary.
- Technology neutral.
- Scalable.
- Flexible.

The Framework employs a risk-based approach to cybersecurity and at its highest level operates similarly to a gap analysis. A gap analysis is the comparison of actual performance with potential or desired performance, and:

- Identifies gaps between the current resource level and the optimized state of affairs.
- Identifies areas for improvement.
- Results in documentation and approval of the differences between future business requirements and the organization's current capabilities.

NIST will continue to update the Framework based on feedback and in response to evolving risks.

THE FRAMEWORK'S PURPOSE

The Framework aims to:

- Provide a common, plain-English language for stakeholders to discuss cybersecurity.
- Standardize the approach for addressing cybersecurity concerns.
- Provide organizations with a way to:
  - share best practices and lessons learned, both internally and with other organizations;
  - describe their current and target cybersecurity states;
  - identify and prioritize opportunities for improvement; and
  - assess progress toward cybersecurity goals.

According to NIST, the Framework:

- Does not replace, but complements, an organization's cybersecurity program.
- Can be used as a reference to create a cybersecurity program if one does not already exist.
- Can be used with a broad array of cybersecurity risk management processes, including:
  - International Organization for Standardization's (ISO's), *Risk management - Principles and guidelines*, 31000:2009;

- ISO/International Electrotechnical Commission's *Information technology - Security techniques - Information security risk management*, 27005:2011; and
- NIST's Special Publication 800-39.

CRITICAL INFRASTRUCTURE

The cybersecurity executive order broadly defines critical infrastructure as:

> "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

The critical infrastructure community includes public and private owners and operators. DHS has identified the following 16 critical infrastructure sectors:

- Chemical.
- Commercial Facilities.
- Communications.
- Critical Manufacturing.
- Dams.
- Defense Industrial Base.
- Emergency Services.
- Energy.
- Financial Services.
- Food and Agriculture.
- Government Facilities.
- Healthcare and Public Health.
- Information Technology.
- Nuclear Reactors, Materials and Waste.
- Transportation Systems.
- Water and Wastewater.

While power plants, dams and defense facilities obviously evoke critical infrastructure, the commercial facilities category is broad and covers, for example:

- Arenas.
- Casinos.
- Shopping malls.
- Hotels.
- Fairs.
- Campgrounds.
- Motion picture studios.

Given this, the Framework arguably applies, if voluntarily, to virtually every US company.

THE FRAMEWORK'S STRUCTURE

The Framework aims to emphasize the relationship between business drivers and cybersecurity activities. It consists of three parts:

- The Framework Core.
- The Framework Implementation Tiers.
- The Framework Profiles.

THE FRAMEWORK CORE

The Framework Core is a set of cybersecurity activities based on industry standards, guidelines and practices. It also includes desired outcomes that are common across sectors. The Core provides the detailed guidance necessary for organizations to develop their Framework Profiles.

The Core essentially:

- Represents the lifecycle of an organization's cybersecurity risk management.
- Provides a fundamental cornerstone for how an organization should view its cybersecurity practices.

The Core is organized into:

- Functions.
- Categories and Subcategories.
- Informative References.

Each of the above consists of a set of cybersecurity activities, desired results and references that are applied together to form the essential elements of designing and implementing a sound cybersecurity program.

The Framework Core is a set of cybersecurity activities based on industry standards, guidelines and practices. It also includes desired outcomes that are common across sectors.

For an illustration of how Functions, Categories, Subcategories and Informative References may be aligned to create a plan for achieving a desired expected end result for a Function, see *Box, Sample Framework Matrix*.

Functions

The Functions are the highest structural level used to arrange cybersecurity activities. They are designed to assist an organization in defining its cybersecurity risk management by:

Sample Framework Matrix

FUNCTION	CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
Identify	Asset Management	Physical devices and systems within the organization are inventoried.	Inventory of authorized and unauthorized devices (Council on Cybersecurity Critical Security Controls (*CCS CSC 1*)).
Protect	Access Control	Identities and credentials are managed for authorized devices and users.	Account monitoring and control (*CCS CSC 16*).
Detect	Continuous Security Monitoring	The network is monitored to detect potential cybersecurity events.	Maintenance, monitoring and analysis of audit logs (*CCS CSC 14*).
Respond	Response Planning	Response plan is executed during or after an event.	Incident response and management (*CCS CSC 18*).
Recover	Recovery Planning	Recovery plan is executed during or after an event.	Data recovery capability (*CCS CSC 8*).

- Outlining relevant information.
- Assisting in risk management decisions.
- Addressing threats.
- Improving procedures and processes.

The five Functions are:

- **Identify.** This refers to the process of developing an understanding of an organization's systems, assets, business needs and capabilities. Doing so allows the organization to prioritize its cybersecurity efforts and apply the Framework.
- **Protect.** This refers to developing and implementing appropriate cybersecurity safeguards within the organization.
- **Detect.** This refers to developing and implementing processes for detecting a cybersecurity incident.
- **Respond.** This refers to developing and implementing an action plan regarding a cybersecurity incident.
- **Recover.** This refers to developing and implementing a plan to restore normal operations following a cybersecurity event.

There is no hierarchy of Functions, and the Framework does not intend the Functions to operate as a checklist. Rather, organizations must address the Functions concurrently and continuously.

Categories and Subcategories

The Functions are further subdivided into:

- **Categories.** Categories are the groups of cybersecurity anticipated end results tied to the organization's needs and particular activities for a given Function. For example:
  - "access control" is a Category under the Protect Function;
  - "continuous security monitoring" is a Category under the Detect Function; and
  - "mitigation" is a Category under the Respond Function.
- **Subcategories.** Subcategories further divide a given Category into specific activities that support the desired achievement in each Category. For example:
  - "cataloguing external information systems" is a Subcategory of access control;
  - "malicious code is detected" is a Subcategory of continuous security monitoring; and
  - "incidents are contained" is a Subcategory of mitigation.

The Framework sets out specific Categories and Subcategories mapped to the corresponding Function in its Appendix A. However, the Framework's Categories and Subcategories are not exclusive and organizations may develop their own.

Informative References

Informative References are the security standards, guidelines and practices that show a methodology to achieve the outcomes associated with each Subcategory. The Framework includes a non-exhaustive compendium of Informative References assembled during the process of developing the Framework. Examples of Informative References included in the compendium are:

- COBIT 5.
- ISO/IEC 27001:2013.
- NIST Special Publication 800-53 Rev. 4.

Organizations may identify additional Informative References.

THE FRAMEWORK IMPLEMENTATION TIERS

The Framework Implementation Tiers are an assessment of how extensively an organization manages its cybersecurity risks. The Tiers describe the level of sophistication and rigor an organization employs in its cybersecurity practices and provide a context for applying the core Functions.

The tiers range from Partial to Adaptive. Tier assignments are based on the strength of the cybersecurity program. From lowest to highest, the four Tiers are:

- **Partial.** An assignment within the Partial Tier recognizes that prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment or business requirements.
- **Risk Informed.** An assignment within the Risk Informed Tier acknowledges that risk management processes may be approved by management, but may not be established as organization-wide policies.
- **Repeatable.** An assignment within the Repeatable Tier suggests that organizational cybersecurity practices are regularly updated based on the application of risk management processes.
- **Adaptive.** An assignment within the Adaptive Tier means the organization adapts its cybersecurity practices based on lessons learned and predictive risk indicators derived from previous and current activities.

THE FRAMEWORK PROFILES

The first step an organization must take in implementing the Framework is to assess its Current and Target Profiles. The Current Profile reflects the organization's current cybersecurity processes, practices and results, while the Target Profile reflects the organization's future goals to improve and strengthen its cybersecurity program. The Framework does not include profile templates.

According to the Framework, by creating a profile, an organization can:

- Identify cybersecurity gaps it needs to address.
- Identify the resources it needs to achieve its cybersecurity goals.
- Create a plan for reducing cybersecurity risk that:
  - is aligned with organizational goals;
  - considers legal and regulatory requirements;
  - incorporates industry best practices; and
  - reflects risk management priorities.

Once the organization has assigned its Current and Target Profiles, it designs a plan to get from one to the other. The process anticipates, and successful compliance requires, discussions between an organization's information technology people and its business people.

NIST PUBLICATIONS AND OTHER FEDERAL GUIDANCE

The federal government has supported the Framework by developing resources, including:

- NIST publications and other materials.
- DHS's Critical Infrastructure Cyber Community C^3 (pronounced "C Cubed") Voluntary Program.

In December 2014, Congress passed legislation formalizing the Framework process.

NIST GUIDANCE

NIST published its *Roadmap for Improving Critical Infrastructure Cybersecurity* (Roadmap) concurrently with the Framework. The Roadmap discusses NIST's plans for moving forward with the Framework and identifies key areas for development, including plans for developing a standard for privacy protections. NIST published a summary of its April 2014 workshop to further its development of the privacy standards (*NIST, Summary of the Privacy Engineering Workshop, April 9-10, 2014*).

NIST also has developed the *Cybersecurity Framework Reference Tool*. The tool consists of a database that allows a user to search and browse the Framework Core by reference to its various components, such as Functions, Categories, Subcategories and Informative References.

On December 5, 2014, NIST published an *Update on the Cybersecurity Framework* (Update) reflecting input from stakeholders on the use and progress of the Framework. The Update also addresses how NIST intends to support the future use of the Framework.

C^3 VOLUNTARY PROGRAM

In conjunction with NIST's release of the final Framework, DHS launched the C^3 Voluntary Program to encourage use of the Framework. The C^3 Voluntary Program's primary activities are:

- Supporting use of the Framework.
- Increasing awareness and use of the Framework.
- Collecting feedback on the Framework.

The C^3 Voluntary Program is developing guidance on how to implement the Framework in combination with the Sector-Specific Agencies (SSAs), which are those federal agencies that have authority over the various critical infrastructure sectors and other industry stakeholders.

CYBERSECURITY ENHANCEMENT ACT OF 2014

In December 2014, Congress passed The Cybersecurity Enhancement Act of 2014 (*Pub. L. 113-274, 128 Stat. 2971*) (Cybersecurity Act). The Cybersecurity Act authorizes NIST to continue its practice of supporting the development of voluntary industry standards and best practices to reduce cybersecurity risks to critical infrastructure. The Cybersecurity Act also codifies the Framework development and support process.

USING THE FRAMEWORK

The Framework provides a good starting point for small to mid-sized organizations that do not yet have strong cybersecurity programs. At its most detailed level, the Framework consists of roughly 100 procedures that NIST believes make for a strong

cybersecurity program. While these procedures are stated at a relatively high level, for example, "[p]rotections against data leaks are implemented," they still offer insight to organizations with immature programs. NIST's intent is that organizations will implement these procedures within the context of their unique cybersecurity risks.

Organizations can use the Framework to create an end-to-end risk management approach to cybersecurity that helps:

- Identify gaps in their existing programs.
- Provide a construct for organizing future improvements.

Private industry seems prepared to implement the Framework. For example:

- Many financial institutions are showing interest in reorganizing their programs around the Framework.
- In some cases, security teams are reorganizing executive dashboard reports according to the Framework's Functions, highlighting where financial investment in one Function may be at the expense of another.
- Many companies are conducting gap analysis assessments against the Framework's procedures to ensure that important coverage areas are not overlooked.

Some companies also are creating analytical approaches to measuring adherence to the procedures, assigning maturity scores for each and weighing the value of each procedure against business risk. This quantitative approach allows an organization to:

- Measure the maturity of the overall program.
- Eliminate much of the subjectivity in determining prioritization of future investment.

This approach also aides in defining the organization's Target Profile.

BENEFITS OF IMPLEMENTING THE FRAMEWORK APPROACH

Regardless of an organization's size, structure or sophistication, it may benefit from implementing a Framework approach. For instance, the Framework provides a:

- Straightforward matrix for:
  - assessing an existing cybersecurity program;
  - developing a new cybersecurity program;
  - identifying gaps in compliance; and
  - designing a plan to remediate any gaps and improve cybersecurity.
- Common and understandable taxonomy that stakeholders can use to communicate both within an organization and with outsiders, including regulators.

In the event of a cybersecurity incident, an organization that has implemented the Framework can also:

- Have concrete documentation that it implemented a recognized industry standard in assessing, designing and improving its cybersecurity program.
- Argue that it followed NIST's recommendations, perhaps avoiding a determination by regulators or courts that it was negligent in its cybersecurity efforts in the event of a breach or an investigation.

However, the Framework's reception has been mixed. For a discussion of some of the criticisms, see *Box, Criticisms of the Framework*.

Criticisms of the Framework

Despite its positive attributes, the Framework does have some challenges to overcome. Some organizations find it difficult to implement because it lacks demonstrative examples of adherence to specific components and guidance on how to best understand the cybersecurity risks of business environments.

The Framework also does not provide any guidance about the relative importance of available controls. For example, whether protective controls are more important than strong procedures for responding to events.

Other criticisms of the Framework include that it:

- Is too complicated for management and board members to understand.
- May lead senior management to focus on actuarial risk rather than capabilities of potential hackers because it is more oriented towards process and response than prevention.
- Is too focused on compliance and not focused enough on real security because of the nature of its high-level process orientation.
- Places greater emphasis on detecting and responding to security incidents than preventing them.
- Merely provides a baseline of what is reasonable should an incident occur and does not provide any real improvements on the existing standards and processes.
- Does not take into account specific legal or regulatory requirements.
- As applied to large organizations, the time it may take to map detailed actions to the Framework can be cost- and time-prohibitive given their extensive data assets.

DEVELOPING A CYBERSECURITY PROGRAM

An organization can use the Framework as a basic outline of the steps to develop a sound cybersecurity program, such as:

- Performing a basic review of existing cybersecurity practices.
- Creating or improving a cybersecurity program by:
  - defining scope and priorities;
  - identifying the organization's current practices;
  - conducting a risk assessment;
  - identifying the organization's goal for its cybersecurity program;
  - determining, analyzing and prioritizing gaps; and
  - designing and implementing an action plan.
- Communicating cybersecurity requirements:
  - with stakeholders; and
  - among interdependent stakeholders for delivery of essential critical infrastructure services.

With the inclusion of Informative Resources, the Framework also provides a guide to specific industry standards and controls relevant to particular cybersecurity tasks (the Subcategories in the Framework taxonomy).

PRACTICAL STEPS TO IMPLEMENT THE FRAMEWORK

Many organizations should find implementing the Framework approach relatively straightforward. Larger organizations with well-organized cybersecurity programs can easily allocate their existing program procedures into the respective Framework Function (for example, awareness and training activities already in place would be grouped into the Protect Function). Smaller organizations can use the Framework Functions as a means of identifying areas in which their programs may be lacking.

Regardless of an organization's size, the following are key steps to implementing the Framework:

- Identify a key executive responsible for cybersecurity.
- Conduct a threat and risk workshop.
- Conduct a cybersecurity program assessment.
- Create a future state roadmap.
- Create a Framework scoring model.
- Perform a peer benchmark assessment.
- Continuously collaborate and communicate.

Key Executive Responsible for Cybersecurity

Identifying a key executive responsible for cybersecurity may seem obvious in light of some of the most recent destructive cyber attacks and with many organizations already having a chief information officer, chief information security officer (CISO), chief compliance officer and chief privacy officer. However, the CISO must be given sufficient authority within the organization to make the necessary improvements to the cybersecurity program.

Threat and Risk Workshop

The first step in implementing the Framework is understanding the organization's particular cybersecurity risks. Organizations should conduct a strategic, business-focused threat and risk workshop to provide appropriate context for future security initiatives.

The purpose of the workshop is to understand the business impacts associated with a variety of threat scenarios. Understanding these impacts allows prioritization of future spending based on risk. The workshop should include C-level executives such as the chief information officer, the CISO, the chief compliance officer and the chief privacy officer.

Cybersecurity Program Assessment

Once the organization understands the impacts of its cybersecurity risks, it must then determine whether it is vulnerable to those risks. Conducting an assessment of the existing cybersecurity program against the Framework can:

- Identify areas where focus is needed.
- Produce a baseline on which improvements can be made.

This baseline then becomes the Current Profile under the Framework.

Future State Roadmap

After conducting an assessment, taking into consideration the threats identified in the workshop, the organization should create a future state roadmap to highlight the ways in which the cybersecurity program should improve to appropriately address risk. This analysis results in the Target Profile.

Framework Scoring Model

The organization should develop a maturity scoring model that measures adherence of the cybersecurity program against the roughly 100 Framework procedures. This scoring model, while not a requirement of the Framework, assists in measuring program maturity improvements over time. It creates a means by which improvements can be measured quantitatively rather than subjectively, permitting senior leadership to ascertain progress using a standard lens.

Peer Benchmark Assessment

Following the development of a future state roadmap, an organization should work to understand how its program's security capabilities measure up against those of industry peers. A benchmark assessment provides valuable insights into an organization's security strengths, as well as areas of weakness that may create systemic risks for the industry.

It will most likely be necessary to retain a third-party technology research organization to get aggregated industry data to perform the benchmark activities, although industry peer sharing groups, such as the Financial Services Information Sharing and Analysis Center (FS-ISAC), may also be a resource.

Collaboration and Communication

One of the primary responsibilities of the CISO or other responsible executive should be to continue to foster a dialogue among the various stakeholders within the organization to ensure that everyone is informed of possible vulnerabilities.