# PROTIVITI FLASH REPORT

## Cybersecurity Framework: What Happens When the Clock Winds Down?

September 13, 2013

On February 12, 2013, President Barack Obama issued an executive order calling for increased cybersecurity for our nation's critical infrastructure. The term "critical infrastructure" is intended to include any entity with assets whose compromise or degradation could have a significant impact on national security, national economic security, national public health or safety, or any combination of those vital national interests. Thus, this unprecedented cross-sector security order has targeted companies providing a wide range of services, which could include financial, energy and healthcare, as well as many others.

The National Institute of Standards and Technology (NIST) was asked to create a national cybersecurity framework that sets forth voluntary cybersecurity standards and addresses the known shortcomings in the security of critical infrastructure. The president's executive order directs NIST to collaborate with both the public and private sectors in formulating the framework. In approaching this task, NIST published a request for information (RFI); led several public workshop discussions around the country that were composed of cybersecurity professionals and government officials; issued drafts along the way that were available for public comment and review; and pursued other forms of stakeholder engagement (e.g., NIST communicated with several government groups for information and input, including potential incentives for compliance with the voluntary framework). The final framework is expected to be released in February 2014.

### Why Care?

Cybersecurity is a national imperative. While cyber threats have existed for some time, the complexity and evolution of changing technologies over time have made these threats more difficult to manage and control. As new developments (e.g., cloud computing, mobile computing, new platforms and devices, workplace virtualization, increased ease with which large volumes of data are transferred and shared with parties other than the original owner [e.g., transaction processors], among others) present opportunities for companies to create new markets and business models and improve efficiency of operations, they also present fresh venues for cyber attacks and mischief.

Over time, disclosure of security breaches and their sources and consequences have made it clearer to senior executives and boards of directors that cyber threats can be caused by (a) large-scale cybercrime initiatives involving international crime syndicates seeking financial gain; (b) state-sponsored espionage involving governments that seek to steal government documents, intellectual property, blueprints, and other confidential and proprietary documents, or to inflict damage on the country's capacity to function; and (c) the WikiLeaks phenomenon,

driven by ideological grounds to divulge unfiltered sensitive material without consideration of the potential repercussions. Sophisticated intruders seek to infiltrate systems using some form of hacking, network intrusions, malware, physical attacks, social tactics and/or privilege misuse and abuse with the intention of operating undetected within systems for as long as possible to accomplish their aims. These threats extend well beyond the efforts of reclusive hackers seeking to make a vague political statement. The threats come from perpetrators who are playing for keeps.

Many if not all sectors are exposed – from the obvious (e.g., banks, defense contractors, manufacturers, retailers, federal agencies, energy and gas companies, and the telecommunications industry) to transportation companies, the hospitality industry, food services, healthcare and professional services firms. Because it is impossible to ensure 100 percent protection, and difficult to compare best practices in an environment in which there is very little sharing beyond what is already disclosed in public reports, a framework can provide a useful tool for benchmarking purposes. Whether a company or agency applies all or certain parts of the framework, it can improve its existing cybersecurity infrastructure.

## The Three Framework Components

NIST released a preliminary cybersecurity draft framework on August 28, 2013, outlining standards, best practices and guidance expected to be codified in October 2013. The preliminary framework is available at http://nist.gov/itl/upload/discussion-draft_preliminary-cybersecurity-framework-082813.pdf. This draft provided the basis for the fourth and final workshop in Dallas held this week.

Many are asserting that the latest draft is a solid gauge of what the official framework will ultimately look like. Intended as a complement to and not as a replacement for an organization's existing cybersecurity processes, the draft provides guidance to an organization on managing cybersecurity risk, in a manner similar to how it might manage other risks. NIST has insisted that the draft framework is not a one-size-fits-all approach for all critical infrastructure organizations. Each organization and its risks are unique, and are often impacted by the organization's implementation of information and operational technology. Accordingly, NIST is of the view that organizations' implementation of the framework will vary.

The preliminary draft is comprised of three components:

- ***The framework core:*** This component is a compilation of cybersecurity activities and references common across critical infrastructure sectors. The core presents standards and best practices in a manner that allows for communication and risk management across the organization from the senior executive level to the implementation/operations level. It consists of five functions providing a high-level, strategic view of an organization's management of cybersecurity risk – identify, protect, detect, respond and recover. It also identifies underlying key categories and subcategories for each of these functions, and matches them with informative references such as existing standards, guidelines and practices for each subcategory. To illustrate, the "protect" function includes the following categories: data security, access control, awareness and training, and protective technology. The framework drills down from there.
- ***The framework implementation tiers:*** This component demonstrates the implementation of the framework's core functions and categories and indicates how cybersecurity risk is managed. These tiers range from "partial" (Tier 0) to "adaptive" (Tier 3), with each tier building on the previous tier.

- ***The framework profile:*** This component conveys how an organization manages cybersecurity risk in each of the framework's core functions and categories by identifying the subcategories that are implemented or planned for implementation. Profiles are used to identify the appropriate goals for an organization or for a critical infrastructure sector and to assess progress against meeting those goals.

The three framework components are designed to (1) provide industry and government with common cybersecurity taxonomy, (2) establish goals and targets, (3) identify and prioritize opportunities for improvement, (4) assess progress, and (5) improve communications between stakeholders. Each component is discussed further below.

## The Framework Core

As noted above, the core is broken down into five functions:

- ***Identify*** what must be protected and establish priorities and processes for reaching risk management goals. This function is all about learning and understanding the organization or infrastructure to be protected. Management must keep accurate priorities of the high-value targets and manage the risks that are desirable to manage given the potential threats.
- ***Protect*** by implementing safeguards to ensure preservation of high-value targets and critical infrastructure services. The objective is to execute the necessary activities which will allow the business to continue, despite the reality of ongoing cyber attacks.
- ***Detect*** by establishing methods for identifying malicious activities. Effective detection requires monitoring or assessing cyber events and incidents on an ongoing basis and determining the degree of urgency of events and incidents effectively and efficiently.
- ***Respond*** by developing and implementing priorities and activities for taking action after an event or incident. Risk management and incident response decisions and actions must be designed to stop incidents in a timely manner.
- ***Recover*** using established tools for restoring impaired capabilities after malicious activity. The purpose of this function is to return to a normal state of affairs after an event or incident has occurred.

As noted earlier, each function has categories as well as subcategories, with many of the subcategories containing supporting resources. The supporting references will include current security standards or models, such as ISO 27001. The idea behind the informative references is to provide quick access to the specific sections of standards and practices common among critical infrastructure sectors and illustrate a method to accomplish the activities within each subcategory.

While each of the functions can be implemented independently, some will likely complement each other; therefore, it may make sense to review and consider multiple functions when implementing improvements. A good example of this integration might be that "detect" could necessitate that a business has "identified" the high-value targets it should be monitoring.

## The Framework Implementation Tiers

The framework's implementation tiers provide guidance on how an organization implements the various framework core functions and categories as well as how it manages its risk. The progressive tiers range from zero, or partially participating in the framework's guidelines, to three, or adaptive, which involves ongoing updates that enable agile cybersecurity and risk management. The tiers provide a maturity continuum of sorts.

To illustrate, the descriptions of the tiers[1] are provided below:

- ***Tier 0: Partial*** – The organization has not yet implemented a formal, threat-aware risk management process to determine a prioritized list of cybersecurity activities. The organization may implement some portions of the framework on an irregular, case-by-case basis due to varied experience or information gained from outside sources. An organization at Tier 0 might not have the processes in place to share cybersecurity information internally among its organizational layers, or to participate in coordination or collaboration with other entities.
- ***Tier 1: Risk-Informed*** – The organization uses a formal, threat-aware risk management process to develop a profile of the framework. In addition, risk-informed, management-approved processes and procedures are defined and implemented and staff has adequate resources to perform their cybersecurity duties. The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally.
- ***Tier 2: Repeatable*** – The organization updates its profile based on regular application of its risk management process to respond to a changing cybersecurity landscape. Risk-informed policies, processes and procedures are defined, implemented as intended, and validated. The organization will also have consistent methods in place to provide updates when a risk change occurs. Personnel have adequate knowledge and skills to perform defined roles and responsibilities. The organization understands its dependencies and partners, and can consume information from these partners to help prevent and improve its reaction to events.
- ***Tier 3: Adaptive*** – The organization updates its profile based on predictive indicators derived from previous and anticipated cybersecurity activities. These updates to the profile enable the organization to adapt actively to a changing cybersecurity landscape and to emerging/evolving threats. Risk-informed policies, processes and procedures are part of the organizational culture and evolve from previous activities (and from information shared by other sources) to predict and address potential cybersecurity events. The organization manages risk and actively shares information with partners to ensure accurate, current information is being distributed and consumed to improve cybersecurity before an event occurs.

The framework provides that organizations determine the desired tiers at the category level, ensuring the selected levels meet organizational goals, reduce cybersecurity risk to critical infrastructure, and are feasible to implement. In doing so, the framework implementer selects the appropriate categories and target tiers through the use of the framework profile. Each company must decide the appropriate tier and functions that make business sense after considering all the risks.

## The Framework Profile

A framework profile enables organizations to establish a road map for reducing cybersecurity risk that (a) is closely aligned with organization and sector goals, (b) considers legal and regulatory requirements, and (c) reflects risk management priorities. A framework profile can be used to describe both the current state and the desired (or target) state of specific cybersecurity activities, thereby revealing gaps that should be addressed to meet cybersecurity risk management objectives.

[1] *Discussion Draft of the Preliminary Cybersecurity Framework*, provided by the National Institute of Standards and Technology (NIST) in advance of the Fourth Cybersecurity Framework workshop, Sept.11-13, 2013, page 6.

Used to identify an organization's cybersecurity goals and assess progress toward those goals, the profile summarizes an organization's standing in terms of its management of cyber risks. It is used to select the functions, categories and subcategories aligned with the organization's business requirements, risk tolerance and available resources and financial wherewithal. The target profile should support business and mission requirements and aid in the communication of risk within and between organizations. The gaps between the current profile and the target profile drive the creation of the road map that organizations should implement to reduce cybersecurity risk to an acceptable level. The profile is based on the use of the framework's core functions, which include categories and subcategories, and how much of the guidance is being implemented or planned for implementation.

## Key Concerns and Potential Issues

Many questions remain regarding the voluntary framework and what it means for various organizations. Some are excited about the uniformity of the measure, while others worry about repercussions for not following through with the framework due to current requirements, standards and constraints. Some common considerations include:

- Will our customers demand that this framework be implemented, either in its entirety or specific components, during the bidding process?
- Will the framework become a new legal standard for expected levels of reasonableness for similar organizations that are relevant in contractual provisions or tortious suits?
- Might the framework components eventually be turned into a regulatory requirement, overseen by a new regulatory entity or adopted by existing regulators?
- How do we map these key functions to our current standards?

The last question may already have a partial answer. Since some subcomponents will map to industry references, many of the framework components and functions should be easy to adopt where organizations have already performed mapping to other technology security principles or standards. However, organizations that have not mapped to the specific references used by the framework may have to complete additional mapping to standards.

## Where We Go From Here

Developments on the cybersecurity framework are moving forward aggressively. This week, the NIST director, Patrick Gallagher, indicated that the process for writing cybersecurity standards is approaching a "real shift in focus" to implementation. In opening the Dallas workshop, Mr. Gallagher noted the framework "is now becoming real," adding that NIST's standard-writing process is entering the "beginning of the end" as the agency prepares for the October release.

Despite the level of effort, there are still many questions that need to be answered. However, there are some key takeaways organizations can use to begin their preparations based on where the framework is heading. The good news is the security paradigm is not changing. Yes, some new terminology, methods and functions may soon enter the market. And yes, there will be functions already performed by organizations that may take on yet another name, and some functions that may be added to augment existing practices and ensure thorough coverage of the risks. However, the basic approach makes sense, and the compilation of informative references composed of existing standards, practices and guidelines to reduce cyber risks to critical infrastructure industries should prove helpful.

As noted earlier, the final draft framework will be available for comment beginning next month. Entities defined as “critical infrastructure” but that have not been involved in the process will have an opportunity to comment on the final draft. Although the focus is on convergence and moving forward to implementation, NIST officials have said they are expecting feedback before February 2014 from industries and other groups already trying out the emerging standards. As a result, now is a good time for organizations to plan on identifying those components and functions of the framework that are best-suited to their needs.

## Summary

According to NIST, by relying on practices developed, managed and updated by industry, the framework will evolve with technological advances and remain aligned with business needs over time. NIST also notes that unique missions, threats, vulnerabilities and risk tolerances may require different risk management strategies. As one organization’s decisions on how to manage cybersecurity risk may differ from another’s, the framework is intended to help each organization manage its cybersecurity risks while maintaining flexibility and the ability to meet varied business requirements.

Organizations with high-value targets should stay abreast of developments and formulate plans on applying the new framework once it is released in 2014. Both large and small organizations should find the framework useful in reducing cyber risks to critical infrastructure as they align and integrate cybersecurity-related policies and plans, functions and investments into their overall risk management processes. This is an important attribute of any voluntary framework intended to improve cybersecurity in the nation’s critical infrastructure.

## About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit. Through our network of more than 70 offices in over 20 countries, we have served more than 35 percent of FORTUNE 1000® and FORTUNE Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.



protiviti®
Risk & Business Consulting.
Internal Audit.