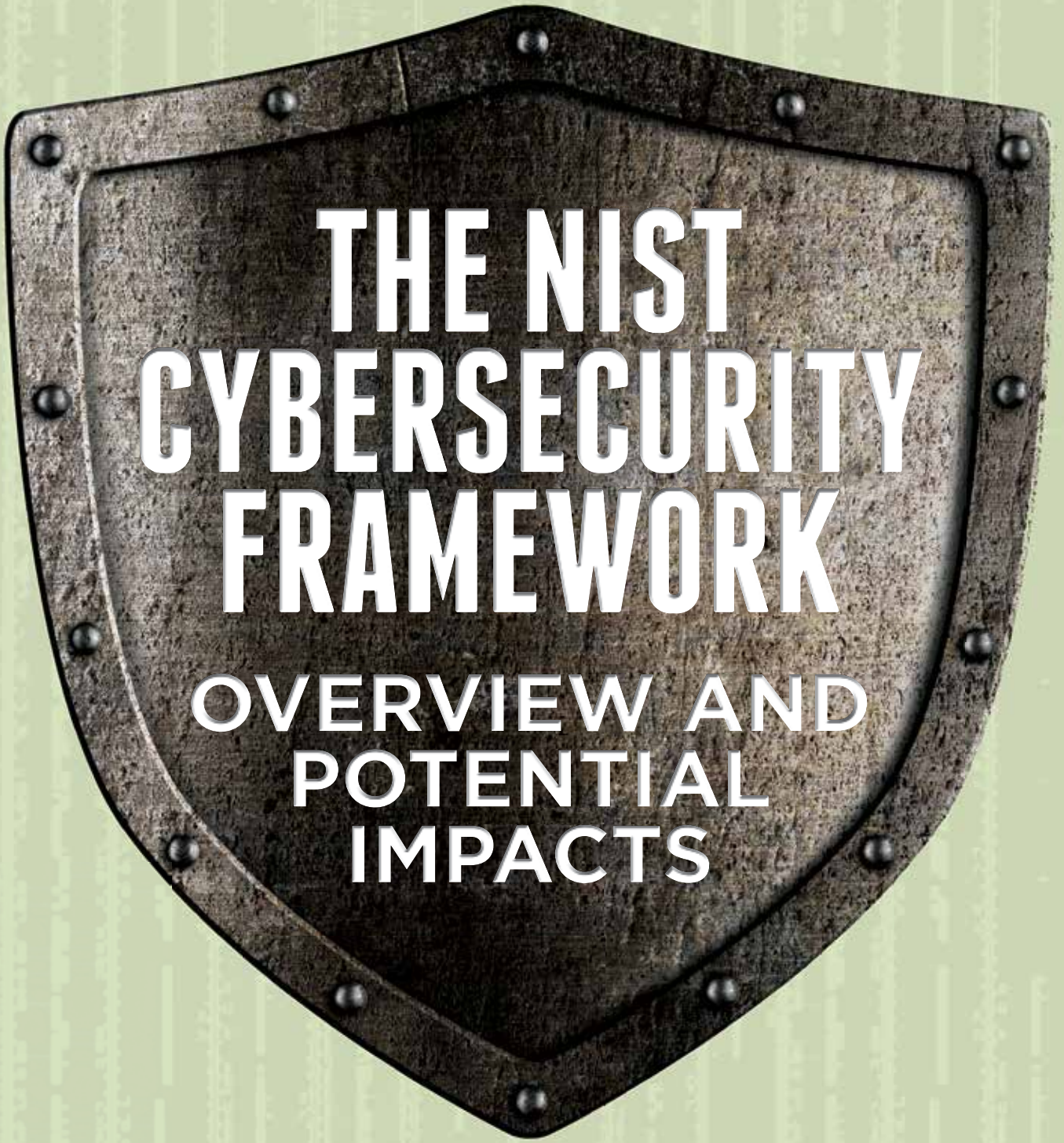

THE NIST CYBERSECURITY FRAMEWORK

OVERVIEW AND POTENTIAL IMPACTS

BY LEI SHEN

With the recent and increasing number of high-profile data breaches, businesses are becoming increasingly concerned about cybersecurity. Such data breaches have cost the affected companies millions of dollars due to liability, lawsuits, reduced earnings, decreased consumer trust, and falling stock prices while putting consumers at risk. Although the recent attacks have targeted consumer data, such attacks may have even greater impact when targeted at the nation's critical infrastructure. The White House acknowledged this when it issued Executive Order 13636,[1] which required the National Institute of Standards and Technology (NIST), a nonregulatory agency of the Department of Commerce, to develop a "cybersecurity framework" to help regulators and industry participants identify and mitigate cyberrisks that could potentially affect national and economic security.

To develop the framework and gain an understanding of the current cybersecurity landscape, NIST consulted hundreds of security professionals in the industry. It held a number of workshops that were attended by many participants from the private sector, and it reviewed numerous comments to the drafts of the proposed framework that it posted for review.[2] More than 3,000 individuals and organizations contributed to the framework.[3]

On February 12, 2014, NIST released its final cybersecurity framework, titled, "Framework for Improving Critical Infrastructure Cybersecurity" (the Framework).[4] Through the collaborative public-private partnership, the resulting Framework adopts industry standards and best practices to provide a set of voluntary, risk-based measures that can be used by organizations to address their cybersecurity risk.

Lei Shen is a senior associate in the Business & Technology Sourcing practice in Mayer Brown's Chicago office. She focuses her practice on privacy and security, technology and business process outsourcing, and information technology transactions.

PHOTO: ISTOCK PHOTO

Although the goal of the Framework is to better protect critical infrastructure,[5] such as banks and utilities, from cyberattacks, the Framework is a flexible and technology-neutral document that can be used by organizations of any size, sophistication level, or degree of cyberrisk. Organizations can use the Framework as a guideline to assess their existing cybersecurity program or to build one from scratch, set goals for cybersecurity that are in sync with their business environment, prioritize opportunities for improvement, or establish a plan for improving or maintaining their cybersecurity.

The Framework is also a valuable tool to help executives understand their company's security practices. Executives may use the Framework to see how their company's cybersecurity practices measure up to the Framework's standards, understand where the company's vulnerabilities lie, and determine if they are doing enough.

Although the Framework is voluntary and may be criticized as being little more than a compilation of established industry security practices, the Framework will nevertheless likely become an influential benchmark for assessing an organization's cybersecurity. This article provides an overview of the NIST Framework and an analysis of its potential impact on businesses.

Summary of NIST Cybersecurity Framework

The Framework is made up of three components: the Framework Core, Profiles, and Tiers. Organizations can use these three components together to conduct a comprehensive review of their cybersecurity program.

Framework Core

The main component of the Framework is the Framework Core (the Core). The Core presents a variety of cybersecurity-related activities and outcomes that can be found in a cybersecurity program, such as the performance of vulnerability scans and the detection of malicious code. The activities and outcomes are organized into five main groups or *Functions*—Identify, Protect, Detect, Respond, and Recover. Each Function is divided into *Categories* and *Subcategories* of cybersecurity activities and outcomes. Those Categories and Subcategories then point to specific industry-accepted standards and guidelines (e.g., COBIT 5, ISO 27001) that provide more in-depth instruction on how to achieve each specific activity or outcome.

For example, if an organization is concerned about its incident response plan, it can look within the "Respond" Function. The Respond Function is divided into five Categories—Response Planning, Communications, Analysis, Mitigation, and Improvements. Each of those Categories is broken down into various Subcategories of cybersecurity activities. For example, the "Response Planning" Category has one Subcategory (i.e., "Response plan is executed during or after an event"), while the "Improvements" Category has two Subcategories (i.e., "Response plans incorporate lessons learned" and "Response strategies are updated"). Each of the Subcategories then references related resources, or *Informative References*, that are industry standards and guidelines that provide more detail on how to complete each activity.

An organization that uses the Framework need not include all of the Core activities in its cybersecurity program, but rather can choose only those activities that are applicable to it.

Profiles

The Framework Profiles (the Profiles), which can be used in conjunction with the Core, provide a summary of an organization's cybersecurity program and can be used to align an organization's cybersecurity activities (such as those found within the Framework Core) with its business requirements, risk tolerances, and organizational resources. Organizations can perform a self-assessment to develop a "Current Profile" and a "Target Profile." An organization's "Current Profile" provides a view of the current state of its cybersecurity program (i.e., those elements of the Framework Core that it is currently achieving), while an organization's "Target Profile" identifies a target or goal state (i.e., those elements

of the Framework Core that it desires to achieve). After establishing its Current and Target Profiles, an organization can identify gaps between the two and establish a road map for areas that the organization needs to strengthen in order to progress toward its target state. To allow for flexibility in implementation, the Framework does not provide a template for creating Profiles.

Tiers

The Implementation Tiers (the Tiers), which are separate from the Core, may be used by organizations to self-rank their cybersecurity risk management practices. There are four Tiers available, ranging from Tier 1 (Partial) to Tier 4 (Adaptive). Each Tier refers to an increasing level of rigor and sophistication in an organization's cybersecurity practices.

The lowest Tier is Tier 1 (Partial), which is characterized as an organization not having "formalized" risk management practices and having little awareness of cybersecurity risks. Tier 4 (Adaptive), on the other hand, describes organizations that can adapt "cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities," are generally aware of cybersecurity risks, and have an organization-wide approach to managing such risks.

After organizations have identified where they stand in the four-Tier structure, they can determine whether they should consider investing additional resources to move to a more rigorous Tier. Whereas organizations identified as Tier 1 (Partial) are encouraged to move toward a higher Tier, those organizations that are already higher-Tiered may not need to move to a higher level. NIST cautions that progression to higher Tiers is encouraged when such change is cost-effective and enhances cybersecurity. For example, it may not be cost-effective for a Tier 3 organization to become a Tier 4 organization if the increased protection it receives is relatively small compared to the cost to reach that additional level.

How to Use the Framework

NIST identifies four different ways that organizations can use the Framework.

Basic Review of Cybersecurity Practices

Organizations can use the Framework to compare their current cybersecurity activities with those outlined in the Core to find out which areas they are achieving the outcomes described in the Core and which areas they may want to improve.

Establishing or Improving a Cybersecurity Program

The Framework lists steps that an organization can follow (such as creating a Current Profile and creating a Target Profile) to use the Framework to create a new cybersecurity program or to improve an existing one.

Communicating Cybersecurity Requirements With Stakeholders

Because the Framework establishes a common language to communicate cybersecurity requirements, an organization can use the Framework to communicate the organization's cybersecurity requirements to its various stakeholders (e.g., service providers).

Identifying Opportunities for New or Revised Informative References

Organizations can also use the Framework to identify opportunities to revise or create new standards, guidelines or practices.

Potential Impact of the Framework

Although the Framework is strictly voluntary and NIST has no enforcement authority, companies are encouraged to use the Framework because of its potential to have a significant impact on a company's cybersecurity practices, as described below.

Incentives

Though there are currently no incentives set for using the Framework, the White House has released a list of eight potential incentives that it is proposing to encourage its adoption.[6] Examples of such incentives include risk-based pricing for cybersecurity insurance and liability limitations (such as limited indemnity or lower burdens of proof) for organizations that adopt the Framework. Some incentives, such as limiting liability or providing a safe harbor for companies that adopt the Framework, may require federal legislation, but others, such as the awarding of federal critical infrastructure grants, may make earlier adoption of the Framework very attractive for some companies.

Legislation

Congress and federal regulatory agencies may use the Framework as a basis for new legislation and regulations. Congress may also turn to legislation if it perceives that an insufficient number of organizations are voluntarily adopting the Framework and may make the Framework mandatory for critical infrastructure operators.

Contractors

As critical infrastructure companies begin adopting the Framework standards, they will likely start requiring their suppliers to use and abide by it as well. Likewise, those suppliers will in turn require their own providers to abide by the Framework. This domino effect could dramatically increase usage in many industries and result in industries where adoption of the Framework is required by default in order to land a

contract. For example, the Department of Defense has published a report that recommends the government "institute baseline cybersecurity requirements as a condition of contract award for appropriate acquisitions."[7]

Insurance

The Framework's standards may shape how insurance carriers view data breaches. Insurance carriers may begin using the Framework as a baseline standard or benchmark in insurance contracts and may start tying a company's cybersecurity Profile to its insurance rates.

Litigation

Without cybersecurity legislation in place, the Framework could effectively become the de facto standard for an organization's cybersecurity efforts. Litigants, such as class action plaintiffs and even shareholders, may start using the Framework's standards as a reasonableness measure in cybersecurity litigation, and may assert that the Framework establishes a standard of care that companies are obligated to follow. In light of the US Security and Exchange Commission's increasing emphasis on the appropriate disclosure of cyberrisks, plaintiffs may bring securities class action litigation alleging material omissions or misrepresentations of a company's cyberrisks based on the Framework. Enforcement actions by state attorneys general and regulators (like the SEC and the Federal Trade Commission) may rely on a similar argument. In *FTC v. Wyndham Worldwide Corporation*, for example, counsel for Wyndham have already cited the Framework as a potential guide as to what constitutes reasonable data security.

On the other hand, organizations at risk for cyberattacks may use their compliance with the Framework as a defense against litigation related to a data breach or other cyberincidents. In addition, proper attention to cybersecurity risk-factor disclosures may decrease the likelihood of a company facing securities class action litigation.

Although the Framework was not intended to be used as a prescriptive standard, organizations should be aware that the Framework may very well end up being used as such.

Future of the Framework

The Framework is likely to evolve as cybersecurity threats and standards evolve. NIST has said that the Framework is not intended to be a static document but rather a "living document." It named the recently released Framework as "version 1.0" and issued a supplementary road map for future developments and recommendations. Such updates will help the Framework keep pace with changes in technology and threats, incorporate lessons learned from its use, and ensure that the standards address the needs of various sectors in a dynamic and challenging environment.

Conclusion

The Framework is not intended to replace a company's existing cybersecurity practices or to establish prescriptive standards. Rather, the Framework provides a tool for organizations to use to assess themselves and to use as a baseline to measure their cybersecurity programs. It is a reference point for objective evaluations of an organization's cybersecurity programs and for identifying potential gaps in those programs.

In view of the recent high-profile data breaches and the pervasiveness of cybersecurity incidents in general, companies should pay close attention to the NIST Framework. Although the Framework will not be a panacea for security issues, it has the potential to have a significant impact in many industries, not just those industries that are related to critical infrastructure. ◆

Endnotes

1. Exec. Order No. 13636, *Improving Critical Infrastructure Cybersecurity* (Feb. 19, 2013), http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

2. Prior drafts of the NIST Cybersecurity Framework are available at http://www.nist.gov/cyberframework/cybersecurity-framework-archived-documents.cfm.

3. *NIST Releases Preliminary Cybersecurity Framework, Will Seek Comments*, NIST.gov (Oct. 22, 2013), http://www.nist.gov/itl/cybersecurity-102213.cfm. ("Through a request for information and a series of workshops held throughout 2013, NIST engaged with more than 3,000 individuals and organizations on standards, best practices and guidelines that can provide businesses, their suppliers, their customers and government agencies with a shared set of expected protections for critical information and IT infrastructure.")

4. NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, NIST.gov (Feb. 12, 2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

5. The Executive Order 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 the security, national economic security, national public health or safety, or any combination of those matters."

6. Michael Daniel, *Incentives to Support Adoption of the Cybersecurity Framework*, The White House Blog (Aug. 6, 2013), http://www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework.

7. Department of Defense and General Services Administration, *Improving Cybersecurity and Resilience through Acquisition*, Department of Defense (Nov. 2013), http://www.defense.gov/news/Improving-Cybersecurity-and-Resilience-Through-Acquisition.pdf.