Financial Fraud Law Report

AN A.S. PRATT & SONS PUBLICATION JANUARY 2014

The FINANCIAL FRAUD LAW REPORT is published 10 times per year by Matthew Bender & Company, Inc. For subscription information and customer service, call 1-800-833-9844. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., PO Box 7080, Miller Place, NY 11764, smeyerow@optonline.net, 631.331.3908 (phone) / 631.331.3664 (fax). Material for publication is welcomed — articles, decisions, or other items of interest.
POSTMASTER: Send address changes to the *Financial Fraud Law Report*, LexisNexis Matthew Bender, 121 Chanlon Road, North Building, New Providence, NJ 07974. Direct inquiries for editorial department to catherine.dillon@lexisnexis.com. *ISBN: 978-0-76987-816-4*

Dissecting the NIST Preliminary Cybersecurity Framework

MARY ELLEN CALLAHAN, DANIEL E. CHUDD, MICHAEL T. BORGIA,
SABRINA N. GUENTHER, AND ANNE C. PERRY

The authors explore the preliminary cybersecurity framework released by the National Institute of Standards and Technology, discussing what it means, what's next, and what companies should consider before adopting it.

The National Institute of Standards and Technology ("NIST") has released the Preliminary Cybersecurity Framework (the "Framework"),[1] which it was directed to develop under Executive Order 13636, "Improving Critical Infrastructure Cybersecurity" (the "Executive Order"). The Framework was intended to "reduce cyber risk and help owners and operators of critical infrastructure identify, assess, and manage that risk." Specifically, the Executive Order required the Framework to provide a "prioritized, flexible, repeatable, performance-based, and cost-effective approach" to managing cybersecurity risk. Although the Framework, and the Executive Order itself, specifically are directed toward "critical infrastructure" and more specifically at federal agencies, the Framework is designed to be utilized by all types of organizations in any industry and, once in place, may eventually be legislatively adopted to cover a larger set of industries.

This article summarizes the Framework, describes what the Framework is (and what it is not), and provides insight into the considerations organizations should take into account in determining whether, how, and to what

The authors, attorneys with Jenner & Block LLP, can be reached at mecallahan@jenner.com, dchudd@jenner.com, mborgia@jenner.com, sguenther@jenner.com, and aperry@jenner.com, respectively.

Published by Matthew Bender & Company, Inc. in the January 2014 issue of *Financial Fraud Law Report*.

extent they will want to adopt the Framework once it is finalized in February 2014.

OVERVIEW OF THE PRELIMINARY FRAMEWORK

The primary objective of the president's February 12, 2013 Executive Order, and thus of the Framework, is to secure critical infrastructure in the United States from the threats of cyber attacks or intrusions. Pursuant to the Executive Order, the Framework is designed for federal departments and agencies under the Executive Order (for which the Framework will be mandatory). In reality, however, the Framework was written with private sector owners and operators of critical infrastructure in mind, and private companies can "voluntarily" adopt the Cybersecurity Framework. In fact, the Departments of Homeland Security, Commerce, and the Treasury have suggested various incentives to encourage critical infrastructure to adopt. The final incentives have not yet been determined, but some of the incentives under consideration include cybersecurity insurance, prioritizing government grants and technical assistance for participating organizations, limiting liability for adopters, streamlining regulatory compliance burdens on adopters, offering public recognition for adopters, allowing rate recovery for utilities' (and other price-regulated industries') cybersecurity investments, and encouraging development of commercial solutions for cybersecurity challenges.

The Framework guides companies through an assessment of their cybersecurity procedures, identifies best practices, and establishes a rubric through which companies can enhance and implement their cybersecurity. The Framework contains a "Core" that sets forth proven cybersecurity activities organized by function; "Implementation Tiers," which allow organizations to prioritize their goals with respect to implementation of cybersecurity activities tailored to the organization's specific cybersecurity risks; and "Profiles," which companies can develop on an overall or threat-specific basis to document both their current cybersecurity profile and their "target" or goal profile.

- *Core*: To provide guidance useful to companies of various sizes across industries, rather than defining a checklist of specific behaviors or procedures, the Framework's Core comprises five Functions — Identify,

Protect, Detect, Respond, and Recover — that group cybersecurity risks at the highest level of generality. More narrowly defined Categories within the Function, such as "Data Security" and "Access Control," and "Subcategories" offer specific actions organizations can take to enhance their cybersecurity. To facilitate implementation of these concepts, the Framework Core also provides "Informative References" — examples of existing best practices companies can adopt and leverage to achieve the goals of the functions. Through the use of these Informative References, the Framework specifically contemplates that organizations will use pre-existing tools and standards when designing their cybersecurity programs. More generally, the Framework Core contemplates that organizations will survey their existing cybersecurity programs and determine how they are already meeting the various Functions, Categories and Subcategories. For organizations that already have sophisticated cybersecurity programs, adopting the Framework will be more a matter of translating the components of their existing programs into the language of the Framework.

- *Implementation Tiers*: The Framework's "Implementation Tiers" categorize the degree to which a company addresses cybersecurity risk and integrates the Framework into its business. These range from Tier 1, which describes sporadic implementation of the Framework, to Tier 4, the highest level of implementation, which involves organization-wide management of and appreciation for cybersecurity risk, including assimilating information from within and without the organization to adapt to evolving threats.
- *Profiles*: The "Profile" component of the Framework provides organizations a mechanism to document their Current and Goal implementation profiles, by Function or by Category. Because each organization may have different needs and priorities, the Profile component contemplates that each organization will tailor its cybersecurity management activities to its own particular risks. The preparation of Current and Goal Profiles facilitates the identification of gaps in an organization's cybersecurity risk management program and prioritization of cybersecurity enhancements.

WHAT THE PRELIMINARY FRAMEWORK IS (AND WHAT IT ISN'T)

Before determining how to respond to the Framework, an organization must first understand what the Framework is and what it is intended to accomplish. Several definitional points have emerged from the process NIST took in developing the Framework, as well as from the Framework itself:

The Framework Is High-Level and Designed To Be Adaptable

Crucially, the Framework is **not** a checklist of discrete tasks that every organization must complete to be considered "in compliance." Such an approach would have two fatal flaws. First, articulating a "one-size-fits-all" list of cybersecurity tasks would thwart the Framework's main goal — to articulate a robust approach to cybersecurity that can be extrapolated to every critical infrastructure sector, and every public or private organization working in that sector. Second, as NIST has stressed throughout the Framework development process, thinking of cybersecurity simply as a matter of completing a standard set of tasks (for example, setting up a firewall, encrypting sensitive data, etc.) results in poor cybersecurity. The perpetrators of cyber attacks are constantly looking for ways to defeat new preventative measures, and thus effective cybersecurity must, in turn, take a varied, flexible approach to respond to evolving challenges and threats.

A more appropriate way to think of the Framework is as both a process for building an effective cybersecurity program and a common language for speaking about cybersecurity across organizations, industries, and job roles. As a process, the Framework is intended to encourage organizations to think methodically about their cybersecurity risks and how to address them. As a common language, the Framework is intended to help different organizations and industries, which currently may think and speak about cybersecurity in significantly different ways and at differing levels of sophistication, more easily share and compare their cybersecurity programs.

Furthermore, by linking together different levels of abstraction through the Functions, Categories, Subcategories and Informative References, the Framework is also intended to bridge the linguistic and conceptual gaps between technical staff, who may focus more on the nuts and bolts of information and system security, and management, who may concentrate on high-level risk management and operational issues.

The Framework Applies to Critical Infrastructure, and Potentially Others

Owners and operators of critical infrastructure should begin considering whether to formally adopt the Framework. Adoption of the Framework is voluntary, although certain sectors are concerned that the Framework will become a *de facto* security standard.

As noted above, the Framework and Executive Order define "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 cybersecurity, national economic security, national public health or safety, or any combination of those matters.[2]

This definition is susceptible, however, to some expansive interpretation because many organizations that do not otherwise qualify as critical infrastructure — for example, certain subcontractors, vendors, insurers and law firms — interact with those who unquestionably do. While the Framework considers only critical infrastructure, those organizations that work closely with critical infrastructure also may benefit from adopting some or all of the Framework's components.

Cybersecurity Should Be Part of Organization-Wide Risk Management

Accompanying the Framework is a "Message to Senior Executives" that characterizes cybersecurity as an organization-wide issue of risk management, much like issues of reputational, financial, and supplier risks. The Framework itself is designed to function as a high-level risk-management tool, encouraging organizations to identify their significant cybersecurity risks and then determine how to address those risks in a cost-effective and operationally feasible manner.

Thinking of cybersecurity as a matter of organizational risk management has several advantages. First, as many organizations already have sophisticated risk management systems, the Framework encourages those organizations

to leverage their preexisting tools and methods when building an appropriate cybersecurity program. Second, thinking of cybersecurity in that way encourages organizations to address cybersecurity like any other significant risk management issue — as one that must be evaluated and addressed at all operational levels. Third, as is evidenced by the "Message to Senior Executives," characterizing cybersecurity as a matter of risk management provides a useful way of selling the importance of cybersecurity to senior management and the board of directors. By emphasizing the high-level organizational risks that cyber threats can pose, rather than simply presenting cybersecurity as a question of which technical tools and procedures to adopt, the Framework speaks about cybersecurity in a language that is already familiar to senior executives.

The Appropriate Level of Implementation Is (Mostly) Defined by Each Organization

As a process and language, the Framework aims to improve and standardize the way organizations think about and implement cybersecurity programs. But the Framework explicitly does not dictate what a successful cybersecurity program should look like at any given organization, nor does it require that organizations adopt every available cybersecurity tool or address every potential cybersecurity risk. Rather, the Framework envisions that each organization, after a thorough evaluation of its needs and risks, will design its own cybersecurity program that is both cost-effective and calculated to provide the organization with an adequate level of protection. Throughout the Framework consultation process, private sector companies were leery of an overly compliance-based Framework to the detriment of effective risk management, and therefore NIST attempted to avoid such pitfalls.

Because the Framework is drafted not as a checklist, or even as a strict set of "best cybersecurity practices," it imposes almost no requirements on adopting organizations. In other words, adopting the Framework will not necessarily be a matter of achieving specific cybersecurity requirements. Rather, it will be a matter of being able to articulate that an organization's cybersecurity program is the product of thorough analysis and designed to adequately serve the organization's needs in a cost-effective manner.

The only apparent exception to this is a provision in Section 3.1, Basic Overview of Cybersecurity Practices. There, the Framework provides:

> Organizations can examine what capabilities they have implemented in the five high-level Functions identified in the Framework Core: Identify, Protect, Detect, Respond, and Recover. *Organizations should have at least basic capabilities implemented in each of these areas*, and can begin to review what particular categories and subcategories they currently use to help achieve those outcomes.[3]

The highlighted sentence, added after the previous Framework draft was published in August 2013, is the only reference to "basic capabilities," and the Framework does not expand on its meaning. At the most recent NIST draft conference, however, several stakeholders expressed confusion regarding why the first implementation tier (then Tier 0, now Tier 1) was set at partial implementation. Thus, NIST may have added this provision to fill the perceived gap, and clarify that critical infrastructure organizations should establish basic cybersecurity capabilities for each Function to minimally comply with the Framework. Although this addition might be considered a conceptual shift from earlier Framework drafts—NIST has emphasized throughout the process that the Framework does not require that an organization take any particular action—the addition is probably better viewed as a clarification that a viable cybersecurity program, by definition, involves at least some activity on each of the five Functions. Indeed, it would be hard to argue that an organization was complying with the Framework, or adopting a cybersecurity program generally, where it took absolutely no action to Identify, Protect, Detect, Respond, or Recover. Thus, despite this additional language, it remains the case that the Framework does not require an organization to adopt any specific tool or policy.

KEY CONSIDERATIONS FOR ADOPTING THE FRAMEWORK (OR IMPROVING AN ORGANIZATION'S CYBERSECURITY GENERALLY)

Because economic incentives (and non-adoption impacts) remain unclear, critical infrastructure organizations may find it too early to decide whether to adopt all or portions of the Framework. Nonetheless, those organizations should monitor these developments to determine whether these

incentives are sufficient for the companies to expressly adopt the Framework, or whether, given any business impacts from full adoption, such companies are better served by incorporating certain elements of the Framework into their already existing cybersecurity response plans without expressly adopting the Framework.

Regardless of whether an organization chooses to formally adopt the Framework, several considerations are key to adopting good cybersecurity practices and overcoming common obstacles:

Identifying (or Hiring) the Right Personnel

Finding personnel with the right knowledge is perhaps the most vexing problem that organizations face when trying to develop their cybersecurity programs. This problem arises largely from the fact that cybersecurity is an interdisciplinary subject — it requires expertise with information and operational systems, an understanding of the organization's business and workflows; and knowledge about the varied and evolving forms of cyber attacks and their goals. When building a cybersecurity team, organizations must make sure that each of these areas of expertise is represented.

Obtaining Executive Buy-In

Demonstrating the importance of cybersecurity to senior executives is crucial to the development of an adequate and viable cybersecurity program. The organization's senior management should be briefed regularly on cyber threats and vulnerabilities, and preventative measures and policies should be considered in accordance with the organization's existing risk management framework. If an organization has a CTO, CIO or CISO, that officer should ensure that the organization's cybersecurity program is designed with appropriate input from both technical and operational staff.

Leveraging Existing Standards

As discussed above, the Framework contemplates that adopting organizations will continue to use existing cybersecurity standards and tools. Regardless of whether an organization formally adopts the Framework, however, one

of the first things any organization should do when evaluating its cybersecurity program is understand how it is already successfully addressing cyber risks. Some sectors, such as the energy sector, have already adopted many best practices, and organizations in those sectors may have robust cybersecurity programs. Likewise, many organizations may have already adopted robust data security practices to comply with existing state and federal privacy and data security laws. It is important, therefore, to recognize that many of those existing practices will already address at least a portion of an organization's most critical cybersecurity needs.

That said, organizations must not assume that simply because they employ good data security practices they are already adequately addressing cybersecurity. Data security generally focuses on the protection of personal or otherwise sensitive customer (or sometimes employee) data. Although that is one key consideration of any cybersecurity program, it does not account for other major cyber threats, such as those intended to shut down critical systems or to steal sensitive intellectual property or trade secrets.

NEXT STEPS FOR THE FRAMEWORK

The NIST opened a comment period on the draft Framework. The NIST Framework Web site includes an Excel spreadsheet template for providing comments. The Web site also notes that all comments will be posted online, "without change or redaction, so commenters should not include information they do not wish to be posted (*e.g.*, personal or business information)."

The final Framework will be published in February 2014, in accordance with the Executive Order. Notably, although the Framework published in February 2014 will be labeled "final," NIST has emphasized repeatedly that it sees the final draft only as the beginning of an ongoing process to evaluate adoption and improve the Framework. NIST intends to revisit the Framework in the future and revise it based on industry feedback.

As they review the Framework and consider the submission of comments, businesses should consider the following questions, among others: How easy or difficult would incorporation of the Framework be into your existing cybersecurity response plans? Would changes to the Framework make incorporation more efficient? Does the Framework cover all the areas that

it needs to cover or are there gaps you are covering in your cybersecurity program that you think all critical infrastructure should be covering? In addition, with the "final" Framework set to be submitted in just four months, businesses, especially those in critical infrastructure sectors, should begin to consider now whether full incorporation of the Framework is appropriate, how such incorporation would be accomplished, and whether they have the right people in the right positions to guide the company through any such incorporation.

NOTES

[1] The Preliminary Framework is available on the NIST Web site at: http://www.nist.gov/itl/upload/preliminarycybersecurity-framework.pdf.

[2] *Id.* at 42, Appendix E.

[3] *See id.* at 11, Section 3.1 (emphasis added).