Westlaw Journal
COMPUTER & INTERNET
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 31, ISSUE 14 / DECEMBER 12, 2013

EXPERT ANALYSIS

The Cybersecurity Framework: Risk Management Process ... And Pathway to Corporate Liability?

By Alexander H. Southwell, Esq., Ryan T. Bergsieker, Esq., and Stephenie Gosnell Handler, Esq.,
Gibson, Dunn & Crutcher

President Barack Obama has focused on cybersecurity as one of the most significant economic and national security challenges facing our nation. To address the complex threat that cybersecurity vulnerabilities pose for public and private entities, the Obama administration has directed the development of cybersecurity standards. While these standards are ostensibly voluntary, their high profile and broad applicability may lead them to be considered baseline standards of care. Therefore, corporations operating in America that fail to meet such standards may be exposed to an increased risk of tort liability and regulatory scrutiny for cybersecurity events. As a result, the standards, which were released in preliminary form in late October and are scheduled for final release in February, are of great importance for corporate America.

INTRODUCTION

In an executive order issued in February, the president reinforced the emphasis he placed on cybersecurity during his 2013 State of the Union address. The executive order called for the development of a voluntary Cybersecurity Framework to establish common standards and guidelines for organizations to manage this risk. The Framework, which is essentially a cybersecurity risk management tool, is intended to shore up a regulatory and legislative gap in this area and encourage organizations — in both the private and public sectors — to develop a more effective approach to managing the serious threats. As such, it establishes a common process that organizations can adopt. While the Framework is aimed specifically at organizations in critical infrastructure sectors, the administration adopted a definition broad enough to encompass the defense industry, financial services, dams, nuclear power plants, museums, office buildings, sports leagues and shopping malls.

WHAT IS THE CYBERSECURITY FRAMEWORK?

At its core, the Framework sets out a risk management approach for addressing cybersecurity threats. It seeks to serve as a common template, drawn from best practices and consensus standards, that a wide variety of organizations can use to identify and respond to these risks and threats. Virtually all companies have processes in place to identify and manage financial, safety and operational risks. The Framework is designed to encourage companies to prioritize and approach cybersecurity threats and challenges in an analogous manner.

Accordingly, the administration intends for the Framework to be a customizable resource[1] for organizations in 16 critical infrastructure sectors.

To address the complex threat that cybersecurity vulnerabilities pose for public and private entities, the Obama administration has directed the development of cybersecurity standards.

In the 2013 executive order, the president directed the Commerce Department's National Institute of Standards and Technology to develop the Framework to standardize organizational approaches to cybersecurity risks and reduce cyberrisks that could pose a threat to national security.[2] Since February, the NIST has been engaged in a collaborative process, which recently produced the preliminary Cybersecurity Framework[3]

THE TARGET AUDIENCE

The voluntary Framework is aimed at organizations that form the nation's critical infrastructure. The term "critical infrastructure" is defined 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."[4]

The 2013 policy directive's 16 critical infrastructure sectors were identified to promote "a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure."[5] These sectors include those that one traditionally thinks of when conjuring threats that would have a debilitating national security impact: the defense industrial base, nuclear reactors and dams. But they also include sectors that one may not necessarily connect with national security, such as commercial facilities, food and agriculture, transportation, and certain manufacturing enterprises.

Though the Framework is intended to be a resource that is used on a voluntary basis, it may have the effect of establishing a minimum standard of care for tort liability in the event of loss due to a cybersecurity breach.

The Department of Homeland Security, which has the task of identifying critical infrastructure, has adopted an expansive view of the organizations that comprise each category.[6] For example, the commercial facilities sector, which includes facilities with open public access, has eight subsectors. The subsectors represent a broad range of facilities, including retail facilities (like shopping malls), places of public assembly (such as stadiums and convention centers) and commercial real estate (such as office buildings and apartment buildings).[7]

The Framework does more than broadly define the critical infrastructure sectors; it also includes language that may further expand the list of organizations that fall under this categorization. More specifically, it states that critical infrastructure includes "other supporting entities that play a role in securing the nation's infrastructure."[8] This means companies should not assume the Framework is inapplicable to them just because they fall outside a sector that is traditionally categorized as critical to national security.

Therefore, while the Framework will be voluntary even for organizations clearly defined as critical infrastructure, organizations that may be considered critical infrastructure under the more expansive interpretation should carefully consider using either the Framework or an organizational-specific equivalent. These organizations may find the Framework to be a useful tool that can enhance their cybersecurity risk management approach. Further, any standard of care established by the Framework could be found to apply to such organizations.

DEVELOPMENT OF THE PRELIMINARY FRAMEWORK

The preliminary Framework has been developed via a collaborative process. More than 3,000 critical infrastructure owners and operators, as well as other stakeholders and interested parties in industry, academia and government, have provided input.[9] The collaborative nature of the process stems in part from the objective to include standards, methods, procedures and processes that align current policy, business and technological approaches. The Framework also seeks to incorporate voluntary consensus standards and industry best practices, which are intended to evolve together with technological advances and business requirements.

The engagement process has consisted of a public request for information and a series of public workshops, meetings, webinars and informal sessions. The workshops, in particular, have been used to refine draft versions of the Framework. The final public workshop was held in mid-November at North Carolina State University.[10] In addition, stakeholders had the opportunity to comment on the preliminary Framework during a 45-day public comment period.[11]

PRELIMINARY FRAMEWORK'S OVERVIEW

The preliminary Framework seeks to establish a common language and mechanism that organizations can use to:

- Describe their current cybersecurity posture.
- Describe their target state for cybersecurity.
- Identify and prioritize opportunities for improvement within the context of risk management.
- Assess progress toward the target state.
- Foster communications among internal and external stakeholders.

Although it is a foundation rather than a detailed risk management process, the preliminary Framework incorporates risk management processes that seek to enable organizations to assess and prioritize cybersecurity decisions based on their unique profile. Its risk-based approach comprises three parts: the core, the profile and the implementation tiers.

The Framework core consists of five functions: identify, protect, detect, respond and recover. These functions provide a high-level strategic categorization of cybersecurity risks. Each function is further divided and paired with example references to existing domestic and international standards, guidelines and practices.[12]

The Framework profile seeks to align industry standards and best practices with an organization's unique business requirements, risk tolerance and resources. The profile is intended to highlight opportunities for the organization's improvement and may be used to develop a road map for reducing cybersecurity risks and completing self-assessments.

The final part is the Framework implementation tiers, which are used to categorize an organization's cybersecurity practices into one of four levels. An organization will select which tier is appropriate based on its current risk management practices, the threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints. Tiers range from Partial (Tier 1) to Adaptive (Tier 4), denoting progress from informal, reactive implementations to flexible and risk-informed approaches.

This tripartite design is intended to foster a consistent approach to cybersecurity and to allow organizations to tailor their risk management approach based on factors such as organizational size, sector, threat environment, market and regulatory environment.

POTENTIAL IMPLICATIONS

Because the Framework has been positioned as a voluntary resource, organizations in the critical infrastructure sectors may choose not to use it for their unique organizational needs. However, because legislative and regulatory requirements relating to cybersecurity threats have lagged, the Framework's standards and guidelines will likely establish a minimum baseline cybersecurity risk management approach for all organizations in the 16 critical infrastructure sectors, regardless of whether they choose to officially adopt the Framework.

While these standards are ostensibly voluntary, their high profile and broad applicability may lead them to be considered baseline standards of care.

Therefore, organizations that choose not to comply with the Framework (or have an equivalent risk management approach) could be held liable for losses. It could be argued that before the Framework was developed, there was no consensus reasonable standard of care relating to cybersecurity risk. The Framework presents a more easily identifiable minimum standard of care for managing such risks.

In addition to the possibility of tort liability, organizations may face additional regulatory scrutiny if they do not meet the Framework's standard of care. Thus, the Framework is an integral risk management tool that officers and directors should pay careful attention to as they seek to fulfill their fiduciary duties.

ACTIONS TO CONSIDER

Organizations should conduct a thorough review of the preliminary Framework. In addition to seeking input from technical experts, key leadership and legal counsel should review the Framework from a strategic, organizational risk management perspective that focuses on potential liability. Further, organizations should consider conducting an internal review of their risk assessment mechanisms and corporate governance to determine if they meet the Framework's baseline standards and guidelines and to identify and reduce the risks posed by cybersecurity threats.

NOTES

[1] Obama has specifically directed that the Framework provide a "prioritized, flexible, repeatable, performance-based and cost-effective approach" to assist organizations in their management of cybersecurity risks. Exec. Order No. 13636, 78 Fed. Reg. 11,739 (Feb. 19, 2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

[2] Language in Sen. Jay Rockefeller's proposed Cybersecurity Act of 2013 stipulates that the NIST would "on an ongoing basis, facilitate and support the development of a voluntary, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to reduce cyber risks to critical infrastructure." S. 1353, 113th Cong. § 101(a)(2) (2013). In addition to providing for an "ongoing, voluntary public-private partnership to improve cybersecurity," the bill proposes to "strengthen cybersecurity research and development, workforce development and education, and public awareness and preparedness." S. 1353, 113th Cong. (2013).

[3] Nat'l Inst. of Standards & Tech., Preliminary Cybersecurity Framework (Oct. 22, 2013), *available at* http://nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf.

[4] USA Patriot Act of 2001, § 1016(e), 42 U.S.C. § 5195c(e) (2001). This definition of critical infrastructure is adopted in Executive Order No. 13636, as well as Presidential Policy Directive-21 (Feb. 12, 2013).

[5] Presidential Policy Directive-21 identifies the 16 critical infrastructure sectors as: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials and waste; transportation systems; and water and wastewater systems. Presidential Policy Directive-21 (Feb. 12, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

[6] The Department of Homeland Security list of critical infrastructure sectors, subsectors and examples of entities comprising the subsectors is *available at* http://www.dhs.gov/critical-infrastructure-sectors.

[7] A complete list of the subsectors of the commercial facilities sector is *available at* http://www.dhs.gov/commercial-facilities-sector.

[8] Preliminary Cybersecurity Framework, *supra* note 3, at 1.

[9] Press Release, Nat'l Inst. of Standards & Tech., NIST Releases Preliminary Cybersecurity Framework, Will Seek Comments (Oct. 22, 2013), *available at* http://www.nist.gov/itl/cybersecurity-102213.cfm.

[10] More information on the Nov. 14-15 workshop, including webcasts and the agenda, is available at http://www.nist.gov/itl/csd/5th-cybersecurity-framework-workshop-november-14-15-2013.cfm.

[11] Request for Comments on the Preliminary Cybersecurity Framework, 78 Fed. Reg. 64478 (Oct. 29, 2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-10-29/pdf/2013-25566.pdf.

[12] For example, the "protect" function includes the following categories: data security, access control, awareness and training, and protective technology. One of the subcategories of data security is "data during transportation/transmission is protected to achieve confidentiality, integrity and availability goals." One of the information references to support this subcategory is "ISO/IEC 27001 Control A.10.8.3" (referring to the International Organizations for Standardization/International Electrotechnical Commission standard). Preliminary Cybersecurity Framework, *supra* note 3, at 16-22.



Alexander H. Southwell (L) is a partner with **Gibson, Dunn & Crutcher** in New York, where he co-chairs the firm's information technology and data privacy practice group. Southwell works with clients on issues relating to privacy, information technology, data breach, theft of trade secrets and intellectual property, computer fraud, national security, and network and data security. He is an adjunct professor of law at Fordham University School of Law, where he teaches a cybercrimes course, and is a former cybercrimes federal prosecutor. He can be reached at ASouthwell@gibsondunn.com. **Ryan T. Bergsieker** (C) is of counsel in the firm's Denver office. A former federal computer crimes prosecutor, his practice includes cyber-related internal investigations, government enforcement defense, litigation and counseling. He can be reached at RBergsieker@gibsondunn.com. **Stephenie Gosnell Handler** (R) is an associate in the firm's New York office, where she practices in the corporate transactions department. A former active duty officer in the U.S. Marine Corps, she holds a J.D. from Stanford Law School and a master's degree in national security studies from Georgetown University. She can be reached at SHandler@gibsondunn.com.