August 13, 2014

Weil

Alert
Cyber Security, Cyber Governance, and Cyber Insurance

Understanding and Implementing the NIST Cybersecurity Framework

By Paul A. Ferrillo and Tom Conkle

Why the Cybersecurity Framework was created and why it is so important

Despite the fact that companies are continuing to increase spending on cybersecurity initiatives, data breaches continue to occur. According to *The Wall Street Journal*, "Global cybersecurity spending by critical infrastructure industries was expected to hit $46 billion in 2013, up 10% from a year earlier according to Allied Business Intelligence Inc.[1]" Despite the boost in security spending, vulnerabilties, threats against these vulnerabilities, data breaches and destruction persist. To combat these issues, the President on February 12, 2013 issued Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity[2]." The EO directed NIST, in cooperation with the private sector, to develop and issue a voluntary, risk-based Cybersecurity Framework that would provide U.S. critical infrastructure organizations with a set of industry standards and best practices to help manage cybersecurity risks.

In February 2014, through a series of workshops held throughout the country and with industry input, NIST released the "Framework for Improving Critical Infrastructure Cybersecurity" ("the Framework")[3]. For the first time, the Framework provides industry with a risk-based approach for developing and improving cybersecurity programs. It also provides a common language regarding cyber security issues to allow for important discussions to take place between an organization's "IT" people, and an organization's "business" people, some of whom may cringe when hearing complicated terms like "APT" (Advanced Persistent Threat). Its common sense, "English language" approach allows an organization and its directors to both identify and improve upon its current cybersecurity procedures. Though the Framework was developed for the 16 critical infrastructure sectors, it is applicable to all companies – albeit at least today – on a voluntary basis.

What is the Cybersecurity Framework

The Framework contains three primary components: The Core, Implementation Tiers, and Framework Profiles.

The Framework Core

The Framework Core ("Core") is a set of cybersecurity activities and applicable references established through five concurrent and continuous

Framework Implementation Tiers Explained

Tier 1 (Partial): Here, the Organization's cyber risk management profiles are not formalized, and are managed on an ad hoc basis. There is a limited awareness of the Organization's cyber security risk at the Organization level, and an Organization-wide approach to managing cyber security risk has not been established.

Tier 2 (Risk Informed): Unlike Tier 1, Tier 2 Organizations establish a cyber risk management policy that is directly approved by senior management (though not yet on an Organization-wide basis). There is some effort by senior management to establish risk management objectives related to cybersecurity, to understand the Organization's threat environment, and to implement cyber security procedures with adequate resources.

Tier 3 (Repeatable): Here, the Organization is running with formal cyber security procedures, which are regularly updated based upon changes in risk management processes, business requirements, and a changing threat and technology landscape. Cyber-related personnel are well-trained and can adequately perform their duties. The Organization also understands its dependencies and business partners, and receives information from them which allows for collaboration and risk-based management decisions.

Tier 4 (Adaptive): Here, the Organization adapts its cybersecurity practices "in real time" based upon lessons learned and predicative indicators derived from previous and current cyber security activities. Through a process of continuous improvement incorporating advanced cyber security technologies, real time collaboration with partners, and "continuous monitoring" of activities on their systems, the Organization's cyber security practices can rapidly respond to sophisticated threats.

functions – Identify, Protect, Detect, Respond and Recover – that provide a strategic view of the lifecycle of an organization's management of cybersecurity risk. Each of the Core Functions is further divided into Categories tied to programmatic needs and particular activities. The outcomes of activities point to informative references, which are specific sections of standards, guidelines, and practices that illustrate a method to achieve the outcomes associated with each subcategory. The Core principles can be thought of as the Framework's fundamental "cornerstone" for how an organization should be viewing its cybersecurity practices: (1) identifying its most critical intellectual property and assets; (2) developing and implementing procedures to protect them; (3) having resources in place to timely identify a cybersecurity breach; and (4) having procedures in place to both respond to and (5) recover from a breach, if and when one occurs.

The Framework Implementation Tiers

The Framework Implementation Tiers ("Tiers") describe the level of sophistication and rigor an organization employs in applying its cybersecurity practices, and provide a context for applying the core functions. Consisting of four levels from "Partial" (Tier 1) to "Adaptive" (Tier 4), the tiers describe approaches to cybersecurity risk management that range from "informal, reactive responses to agile and risk-informed."

The Framework Profile

The Framework Profile ("Profile") is a tool that provides organizations a method for storing information regarding their cybersecurity program. A profile allows organizations to clearly articulate the goals of their cybersecurity program. The Framework is risk-based; therefore the controls and the process for their implementation change as the organization's risk changes. Building upon the Core and the Tiers, a comparision of the Profiles (i.e. Current Profile versus Target Profile), allows for the identification of desired cybersecurity outcomes, and gaps in existing cybersecurity procedures.

Why Directors should care about the Framework

Tom Wheeler, Chariman of the Federal Communications Council (FCC), stated that an industry-driven cybersecurity model is preferred over prescriptive regulatory approaches from the federal government.[4] Nonetheless, it continues to see successful attacks on critical infrastructure organizations.

At some point, if critical infrastructure organizations do not demonstrate that a voluntary program can provide cybersecurity standards that are the same as, if not better than, federal regulations, regulators will likely step in with new laws. In fact, according to SEC Commissioner Luis Aguilar, the Framework has already been suggested as a potential "baseline for best practices by companies, including in assessing legal or regulatory exposure to these issues or for insurance purposes. At a minimum, boards should work with management to assess their corporate policies to ensure how they match-up to the Framework's guidelines — and whether more may be needed."[5] If SEC or other proposed federal regulation of cybersecurity becomes a reality, implementing the Framework could be a mandatory exercise. By choosing to act now, organizations have the benefit of more flexibility in how they implement the Framework.

In addition to staying ahead of federal and state regulators and potential Congressional legislation, the Framework provides organizations with a number of other benefits, all of which support a stronger cybersecurity posture for the organization. These benefits include a common language, collaboration opportunities, the ability to verifiably demonstrate due care by adopting the Framework, ease in maintaining compliance, the ability to secure the supply chain, and improved cost efficiency in cybersecurity spending. Though it would be Herculean to accurately summarize all benefits of the Framework and how to implement them, we pull out its key points below.

Common Language

The Framework, for the first time, provides a common language to standardize the approach for addressing cybersecurity concerns. As we have noted in other articles, including in June 2014 and July 2014, many cyber security principles are not intuitive. They are not based upon well-established principles that Directors (especially audit committee members) are used to hearing, like "revenue recognition." The Framework allows for cybersecurity programs to be established and shared within an organization and to organizational partners using a common language. For example, the Framework allows for the creation of several types of Profiles: Profiles that provide strategic enterprise views of a cybersecurity program, Profiles that are focused on a specific business unit and its security, or Profiles that describe technologies and processes used to protect a particular system. Despite the number of Profiles that may exist for an organization, directors can quickly and easily understand how corporate guidance is implemented in each Profile since they have a standard language and format for describing an organization's cybersecurity programs.

Collaboration

NIST and participants from industry that assisted in the Framework development envision the Framework Profiles as a way for organizations to share best practices and lessons learned. By leveraging the common language and increased community awareness established through the Framework, organizations can collaborate with others through programs such as the Cybersecurity Forum (CForum)[6]. CForum provides an online forum for organizations to share lessons learned, post questions regarding their cybersecurity challenges, and maintain the conversation to continually improve cybersecurity capabilities and standards.

Demonstrating Due Care

By choosing to implement the Framework (or some part of it) sooner rather than later, organizations can potentially avoid the inevitable conclusion (or parallel accusation by a plaintiff's attorney) that they were "negligent" or "inattentive" to cybersecurity best practices following disclosure of a cyber breach. Organizations using the Framework should be more easily able to demonstrate their due care in the event of a cyber attack by providing key stakeholders with information regarding their cybersecurity program via their Framework profile. At the same time,

Directors can point to their request that the organization implement the Framework in defense of any claim that they breached their fiduciary duties by failing to oversee the cyber security risk inherent in their Organization.

Maintaining Compliance

Many critical infrastructure organizations are required to meet multiple regulations with overlapping and conflicting requirements. In order to avoid fines and additional fees from regulatory bodies, many operators are forced to maintain multiple compliance documents describing how the organization is complying with each requirement. The standard developed by the Framework enables auditors to evaluate cybersecurity programs and controls in one standard format eliminating the need for mulitple security compliance documents.

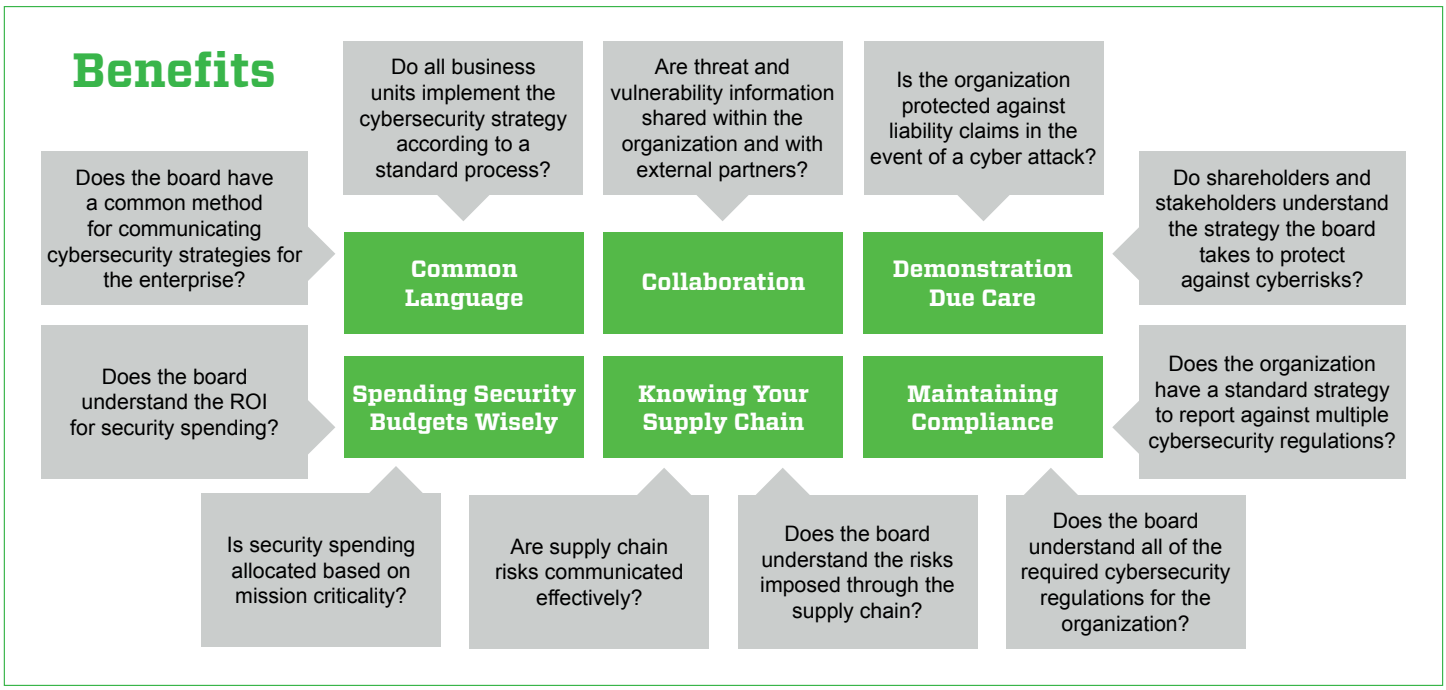
Knowing your Supply Chain

The Framework also provides an opportunity for organizations to better understand the cybersecurity risks imposed through their supply chains.

Organizations purchasing IT equipment or services can request a Framework profile, providing the buying organization an opportunity to determine whether or not the supplier has the proper security protections in place. Alternatively, the buying organization can provide a Framework profile to the supplier or vendor to define mandatory protections that must be implemented by the service provider's organization before it is granted access to the buying organization's systems.

Spending Security Budgets Wisely

In an environment where cyberthreat information is not readily available, organizations struggle with understanding how much security is enough security, leading to organizations implementing unnecessary cybersecurity protections. Through the use of the Framework, standards for care can be established for each critical infrastructure sector. Organizations can leverage these standards to determine the appropriate level of security protections required, ensuring efficient utilization of security budgets.



The diagram above provides questions to help determine if and how an organization can benefit from implementing the Framework. Discussing these questions and their responses will help organizations determine how well their current cybersecurity efforts are protecting them against cyber attacks. Based on the answers to these questions, they will better understand which of the benefits presented in this article will apply to their organization should they implement the Framework.

Where do you start with implementing the Framework?

A major challenge in adopting the Framework is simply getting started. Organizations typically have limited resources and familiarity with the Framework to help them leverage their existing cybersecurity, compliance and audit programs, policies and processes.

At a minimum, directors and their management should become familiar with the Framework. Additionally, directors (or some committee thereof) should have a deep discussion with management about the organization's Implementation Tiers. The Implementation Tiers allow an organization to consider current risk management practices, the threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints.

Educating managers and staff on the Framework to ensure all organizations are on the same page is also an important step toward the successful implementation of a robust cybersecurity program. The previously mentioned CForum is a source for success stories, lessons learned, questions and information useful to organizations implementing the Framwork. This information about existing Framework Implementations may help organizations with their own approaches. Additionally, organizations can seek out cybersecurity service providers skilled in helping organizations with the education, awareness and planning required to implement the Framework across an entire enterprise.

Though "voluntary," it cannot be overstated that the Framework is "a National Standard" developed with input from industry experts, collaborators and businesses with years of cyber experience. As stated by the Chairman of the House of Intelligence, Mike Rogers, "there are two kinds of companies. Those that have been hacked and those that have been hacked but don't know it yet.[7]" Given that it is almost inevitable that an organization will be hacked, there will be a time and a place where it may need to demonstrate to customers, investors, regulators, and plaintiff's attorneys that it gave thought to, and implemented, cyber security measures in order to defend its most critical intellectual property assets, or its most critical business and customer information. Implementing the Framework will not only allow organizations to improve cyber security measures, but also to effectively demonstrate due care.

This article was first published by The D&O Diary *on August 13, 2014.*

1. *Companies Wrestle With the Cost of Cybersecurity*, February 25, 2014, available at http://online.wsj.com/news/articles/SB10001424052702304834704579403421539734550.
2. Executive Order 13636 of February 12, 2013, *Improving critical Infrastructure Cybersecurity*, available at http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.
3. The National Institute of Technology and Standards (NIST) "Framework for Improving Critical Infrastructure Cybersecurity version 1.0", February 12, 2014, available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.
4. (Sarkar, 2014), available at http://www.fiercegovernmentit.com/story/fcc-chairman-pitches-new-industry-driven-regulatory-model-enhance-cybersecu/2014-06-13.
5. See "Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus," available at http://www.sec.gov/News/Speech/Detail/Speech/1370542057946.
6. The Cybersecurity Forum (CForum) is a not-for-profit, publically available site dedicated to the evolution and implementation of the Cybersecurity Framework, available at http://Cyber.securityFramework.org.
7. Graham, Scott, Interview: Greg Toughill, DHS, USA on Cybersecurity, July 28, 2014, available at http://www.globalgovernmentforum.com/brigadier-general-greg-touhill-cybersecurity-department-of-homeland-security-interview/.

About the Authors: Tom Conkle is the commercial services lead for G2, Inc. He assists clients in developing and improving their cybersecurity programs based on their risk tolerance through the use of the Cybersecurity Framework developed by NIST. Paul Ferrillo is Counsel in the Securities Litigation practice of Weil, Gotshal & Manges LLP in New York City.

If you have questions concerning the contents of this issue, please speak to your regular contact at Weil, or to:

Paul A. Ferrillo (NY) Bio Page paul.ferrillo@weil.com +1 212 310 8372