PAUL
HASTINGS
STAY CURRENT
A CLIENT ALERT FROM PAUL HASTINGS

March 2014

America's New Cybersecurity Framework: Help or New Source of Exposure?

BY BEHNAM DAYANIM, RYAN NIER & ELIZABETH DORSI

Data theft is on the rise, and the federal government is concerned. In 2013 alone, there were over 1,400 data breaches in the U.S. resulting in the exposure of an estimated 740 **million** records, costing an average of $5.5 million **each**. These breaches can tarnish reputations, cost millions in remedial damages, litigation defense, and lost business, and in some cases, doom companies.

President Obama views these breaches of private data collections as a threat to the nation's critical data infrastructure. In 2012, he issued an Executive Order calling for the National Institute of Standards and Technology (NIST) to create a voluntary Cybersecurity Framework that could help improve national cybersecurity practices. Just over one year later, in February of this year, NIST released the final version of its "*Framework for Improving Critical Infrastructure Cybersecurity*," which is aimed at improving cybersecurity practices for companies in "critical infrastructure" (*e.g.*, the energy grid, financial institutions and telecommunications).

In light of the recent spate of high-profile data breaches and resulting litigation, **all** businesses dealing with sensitive information (*e.g.*, proprietary data and personal information), should be working to develop an affirmative plan to limit their exposure to cybersecurity threats and to reduce their liability in the event of a breach. The Framework should become a consideration along the way. While compliance is currently voluntary, and its terms are often vague, it is a helpful guidepost: it offers what may well evolve into *de facto* best practices for security and afford a defense in the event of regulatory investigations or litigation arising from a breach.

Executive Order 13636: Improving Critical Infrastructure Cybersecurity

Critics often have been quick to attack many bills addressing cybersecurity risks or data protection as too prescriptive in the substance of their requirements and insufficiently flexible to account for the varied ways in which business is and will be conducted in a digital environment. The Framework reflects that concern, focusing on process and risk-based analysis rather than on defined, "one-size-fits-all" substantive solutions.

The 41-page Framework resulted from an extensive set of workshops and discussions by NIST with a wide range of stakeholders, including but not limited to cyber-businesses. NIST also released a companion "*Roadmap for Improving Critical Infrastructure Cybersecurity*," which is intended to guide continued development of the Framework. The Roadmap emphasizes that it is a work in progress and that NIST will continue to solicit industry collaboration and input for future versions. Based on the

Roadmap, organizations should expect additional guidance in areas such as authentication, automated indicator sharing, conformity assessment and data analytics.

A High-Level Roadmap: What You Should Know

The Framework is designed to help organizations **describe** the strength of their current cybersecurity program, develop an adequate cybersecurity program to decrease risk of breaches, and **identify** and **prioritize** opportunities to reach their desired cybersecurity state. The Framework's risk-based approach is divided into three areas: the Framework Core, Implementation Tiers and Framework Profile.

The ***Framework Core*** is the heart of the program. It consists of five high-level functions (identify, protect, detect, respond and recover) which are further divided into categories and subcategories that are associated with cybersecurity outcomes (*i.e.*, understanding cybersecurity risks to operations) and the technical or management activities that support each outcome (*i.e.*, identifying and documenting asset vulnerabilities). Each subcategory additionally includes a list of "information references" to existing standards, guidelines and practices. Companies may find the ***Core*** helpful in identifying the broad range of issues that their current cybersecurity policies should address, communicating these issues to executives, and locating existing guidelines for particular issues.

The ***Implementation Tiers*** are intended to help an organization normalize its cybersecurity policies by selecting a "Tier" corresponding to how it views its own risks and risk management processes. The tiers range from *ad hoc* and reactive practices in "Partial" (Tier 1) to risk-informed and responsive practices in "Adaptive" (Tier 4). Organizations are urged to select the tier that best describes both their current and desired levels of cybersecurity in each Core category. Self-evaluation of an organization's current and target tiers can help to assess the strength of its current policies and associated risk tolerance for each category.

The ***Framework Profile*** compares the outcomes and activities from the Framework Core with the assessment of an organization's current and target Implementation Tiers for each of the categories. Put another way, the Profile is intended to assist in applying and adjusting the Framework Core in accordance with the selected Implementation Tiers (*i.e*. taking a company from the Tier where it sees itself now to the target Tier). Organizations can use the Framework Profile to identify the specific outcomes and activities to prioritize in order to efficiently strengthen their cybersecurity programs.

Implementing the Framework

The Framework outlines a seven-step implementation plan to "illustrate how an organization could use the Framework to create a new cybersecurity program or improve an existing program." The implementation plan clarifies how the Core, Tiers, and Profile can be used as part of a comprehensive cybersecurity policy:

1. **Prioritize and Scope.** Identify high-level objectives and priorities. Make strategic decisions regarding cybersecurity implementations.

2. **Orient.** Identify threats to, and vulnerabilities of, the systems and assets identified as priorities in step one.

3. **Create a Current Profile.** Develop a Current Profile by indicating which outcomes from the Framework Core are currently being achieved.

4. **Conduct a Risk Assessment.** Analyze the likelihood of a cybersecurity event and the impact that the event could have on the organization.

5. **Create a Target Profile.** Develop a Target Profile that focuses on the assessment of the organization's desired Framework Core outcomes.

6. **Determine, Analyze, and Prioritize Gaps.** Compare the Current Profile to the Target Profile to determine gaps. Create a prioritized action plan and determine the resources required to address those gaps.

7. **Implement Action Plan.** Determine what actions to take to address the gaps identified in the previous step. Monitor current cybersecurity practices against the Target Profile.

More Process Than Substance

If the Framework sounds nebulous, it's because it is. In many respects, it provides little substantive guidance for organizations interested in complying with and adopting its structure. That lack of granularity reflects a deliberate policy choice. As the Framework itself acknowledges, it is not a "checklist of actions to perform" or "a one-size-fits-all approach" because organizations "have unique risks—different threats, different vulnerabilities, different risk tolerances." Instead, the Framework is intended to complement an organization's risk management process and cybersecurity program. On balance, that decision likely was the only one NIST could make. What makes sense for a financial institution may not make sense for a public utility, and what makes sense for a public utility may not make sense for a health-care institution. Each industry, and each player within that industry, must balance the risks it faces with the value of the information it maintains, and each may come to a different conclusion as to what that calculation entails.

Nevertheless, that justifiable concern with avoiding an overly prescriptive approach has left organizations with some uncertainty, and the Frameworks' very existence creates new potential legal obligations and liabilities.

For example, each organization must determine its own Current Profile or Target Profile (*i.e.*, the level of cybersecurity an organization is currently achieving or desires to achieve). Organizations are instructed to "consider [their] current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints." Similarly, the Framework does not establish a general goal Tier that organizations should strive to reach. Instead, it simply urges progression to higher Tiers "when such a change would reduce cybersecurity risk and be cost effective."

Moreover, the Framework Core is presented as a high-level overview aimed more at an organization's executives than at those actually implementing and assessing technical cybersecurity procedures. The Framework Core is therefore best approached as a series of questions that an organization should consider, instead of a "to-do" list to reduce cybersecurity risks.

Potential Legal Exposure

Of greatest note, perhaps, is that the Framework, although voluntary, may soon become mandatory for many companies. The President's executive order directing development of the Framework also instructed federal regulators of critical infrastructure entities to assess their existing authority to require implementation of the Framework by their regulated parties. Just who is "critical" and which agencies ultimately exercise that authority remains to be seen, but we soon may witness transformation of the Framework into a mandatory procedure for many companies. Moreover, even those for whom the Framework remains voluntary may find themselves at risk of legal liability if they fail to follow the Framework. Regulators or private litigants may question the adequacy of the company's security precautions and, in the event of breach, defendants may start to find that the Framework has established a "reasonable standard of care" for purposes of liability.

Some Takeaways

Despite its generality, there are a few areas in which the Framework provides more concrete guidance for organizations wishing either to decrease their cybersecurity risks or limit their liability stemming from data breaches. These best practices are also consistent with some state regulations regarding the sharing of personal information, such as the California Shine the Light law, Cal. Civ. Code § 1798.83, and state data breach notification laws. Additionally, organizations that handle credit card transactions may find that many of the recommended outcomes and activities are consistent with the Payment Card Industry Data Security Standard (PCI DSS) requirements that they have already implemented.

First, several of the subcategories listed in the Framework Core identify cybersecurity assessments or policies that should be documented. To demonstrate consideration of and compliance with the Framework, companies should ensure that existing cybersecurity policies and assessments include several components:

- "Asset vulnerabilities are identified and documented" (ID.RA-1);
- "Threats, both internal and external, are identified and documented" (ID.RA-3);
- "Organizational risk tolerance is determined and clearly expressed" (ID.RM-2);
- "Audit/log records are determined, documented, implemented, and reviewed in accordance with policy" (PR.RT-1); and
- "Newly identified vulnerabilities are mitigated or documented as accepted risks" (RS.MI-3).

Second, in addition to documenting compliance with particular Framework Subcategories, organizations should consider documenting compliance with the Framework's proposed seven-step implementation plan. The Framework's deliberate ambiguity regarding specific security measures renders it primarily instructive as a guide for the **process** that organizations should use to evaluate and improve their cybersecurity programs. That same ambiguity allows enterprises to determine what measures best suit their risk profile. In the event of a data breach, this documentation should help organizations demonstrate compliance efforts.

Third, the Framework repeatedly emphasizes the need for constant re-assessment of cybersecurity policies. Several of the Subcategories explicitly call for periodic reassessment of policies and risks. Even more importantly, the primary difference between Tier 3 (Repeatable) and Tier 4 (Adaptive) is the "continuous improvement" through incorporating new information and the organization's ability to "actively adapt to a changing cybersecurity landscape." In addition to reassessments after data breaches or attacks, organizations should consider re-evaluating their cybersecurity policies and procedures on a periodic basis.

Fourth, where additional data security protections are cost-prohibitive, organizations should consider documenting the expected implementation costs and benefits. Although the Framework provides only general guidance on how such cost benefit analysis should be conducted, the Framework's repeated emphasis that such a tradeoff is appropriate may provide protection if regulators or litigants later question the absence of particular security measures.

The Cybersecurity Framework represents a first step in the federal government's attempt to establish a comprehensive data security framework. Although it is at this point completely voluntary, it provides an indication of the government's cybersecurity interests and suggests several areas of concern. Organizations should strongly consider documenting their compliance with the Cybersecurity Framework, in preparation for future regulations and as an additional protective measure in the event of a data breach.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

San Francisco

Thomas A. Counts
1.415.856.7077
tomcounts@paulhastings.com

Elizabeth A. Dorsi
1.415.856.7209
elizabethdorsi@paulhastings.com

Ryan C. Nier
1.415.856.7226
ryannier@paulhastings.com

Washington D.C.

Behnam Dayanim
1.202.551.1737
bdayanim@paulhastings.com

Stay*Current* is published solely for the interests of friends and clients of Paul Hastings LLP and should in no way be relied upon or construed as legal advice. The views expressed in this publication reflect those of the authors and not necessarily the views of Paul Hastings. For specific information on recent developments or particular factual situations, the opinion of legal counsel should be sought. These materials may be considered ATTORNEY ADVERTISING in some jurisdictions. Paul Hastings is a limited liability partnership.

IRS Circular 230 Disclosure: As required by U.S. Treasury Regulations governing tax practice, you are hereby advised that any written tax advice contained herein or attached was not written or intended to be used (and cannot be used) by any taxpayer for the purpose of avoiding penalties that may be imposed under the U.S. Internal Revenue Code.