Clients&FriendsMemo

NIST's Draft Update to Cybersecurity Framework Focuses on Third-Party Vendors and the Cost-Effectiveness of Cybersecurity Programs

February 1, 2017

On January 10, 2017, the National Institute of Standards and Technology ("NIST") released a proposed update to its popular cybersecurity blueprint for organizations and businesses, known as the *Framework for Improving Critical Infrastructure Cybersecurity* (the "Framework").[1] The updated Framework, titled "Draft Version 1.1," includes, among other things, new provisions for assessing the cybersecurity risk posed by third-party vendors and the addition of a new section on measuring the cost effectiveness of cybersecurity programs. The proposed changes are NIST's first attempt to update the Framework since it was issued in February 2014 pursuant to President Obama's February 2013 Executive Order 13636, "Improving Critical Infrastructure Cybersecurity." Based on feedback from users, responses to its official request for information, and workshop comments, NIST has identified certain areas of the Framework that needed refining, clarification, or enhancement. Draft Version 1.1 is the result of that effort.

NIST has invited public comment on the draft (with comments due by April 10, 2017) and plans to convene a public workshop in May 2017 to discuss proposed changes. NIST intends to release a final Version 1.1 sometime in Fall 2017.

The NIST Framework – A Brief Overview

The NIST Framework provides a risk-based set of guidelines that organizations can use to perform five core cybersecurity functions: (i) ***identifying*** vulnerabilities; (ii) ***protecting*** against cyber threats; (iii) ***detecting*** attempted intrusions and attacks; (iv) ***responding*** effectively to such attempts; and (v) ***recovering*** from successful intrusions or breaches. The Framework does not purport to provide a standard against which organizations should measure their cybersecurity efforts; rather, it offers conceptual guidance for organizations in developing, assessing, or improving their cybersecurity programs, processes, and procedures. In short, the Framework provides a means through which companies can focus their attention on cyber risk assessment and mitigation.

---

[1] *See* 15 U.S.C. § 45(a). The FTC has brought dozens of cybersecurity enforcement actions under Section 5(a), alleging that companies have engaged in "unfair or deceptive acts or practices" by failing to implement reasonable cybersecurity practices or misrepresenting to consumers the nature of the companies' cybersecurity programs.

The Framework has been well-received by organizations in the United States. According to Gartner Research, 30% of U.S. organizations were using the NIST Framework by the end of 2015; Gartner predicts that usage will rise to 50% by 2020.[2] The Framework also is viewed favorably by regulators. For example, the Federal Trade Commission ("FTC"), which seeks to promote data security through enforcement of Section 5 of the FTC Act,[3] has noted that the Framework's approach is "fully consistent" with how the FTC assesses companies' data security practices.[4] Nevertheless, the FTC warned that it does not view compliance with the Framework alone as meeting all of the FTC requirements under section 5 of the FTC Act.[5]

Key Proposed Changes in Draft Version 1.1

Draft Version 1.1 includes a number of tweaks and refinements, but two changes stand out as particularly important for organizations to consider: third-party vendor management and cybersecurity measurement.

First, consistent with a recent focus by businesses and regulators on the cybersecurity threats posed by third-party vendors,[6] Draft Version 1.1 includes considerations for vendor risk management, including guidance for businesses in (i) determining cybersecurity requirements for suppliers and partners; (ii) enacting cybersecurity requirements through contracts; (iii) communicating to suppliers and partners how those cybersecurity requirements will be verified and validated; and (iv) verifying that cybersecurity requirements are met.

The draft also adds a new section, titled "Measuring and Demonstrating Cybersecurity," that provides recommended metrics and measurements that organizations can use to evaluate the "relative cost effectiveness of various cybersecurity activities" and how those cybersecurity activities impact business objectives. Other changes in Draft Version 1.1 include clarification of the Framework's Implementation Tiers[7] and Profiles,[8] updated FAQs, and updated Informative References.

---

2 Cybersecurity Framework Use Infographic, https://www.nist.gov/image/cybersecurityframeworkuseinfographicjpg.

3 *See* 15 U.S.C. § 45(a). The FTC has brought dozens of cybersecurity enforcement actions under Section 5(a), alleging that companies have engaged in "unfair or deceptive acts or practices" by failing to implement reasonable cybersecurity practices or misrepresenting to consumers the nature of the companies' cybersecurity programs.

4 Andrea Arias, The NIST Cybersecurity Framework and the FTC, Business Blog (Aug. 31, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc.

5 *Id.*

6 *See, e.g.*, Joseph Moreno & Joseph Facciponti, "Law Firm Data Breaches Demonstrate the Expanding Scope of Cyber Attacks" (Jan. 17, 2017), http://www.cadwalader.com/resources/clients-friends-memos/law-firm-data-breaches-demonstrate-the-expanding-scope-of-cyber-attacks.

7 The Framework Implementation Tiers describe the degree to which an organization's cybersecurity risk management practices adhere to Framework's guidance. Accordingly, organizations that have informal, ad hoc cyber risk management

Conclusion

Draft Version 1.1 is a reminder that businesses periodically should reevaluate their cybersecurity programs in light of changing industry norms and recommended best practices and, in particular, that businesses should focus on the cybersecurity risks associated with third-party vendors. The comment period for Draft Version 1.1, which is open until April 10, 2017, provides a prime opportunity for organizations and relevant trade and industry groups to weigh in on the suggested amendments and to propose modifications or changes.

If you have any questions, please feel free to contact any of the following Cadwalader attorneys.

Joseph Moreno	+1 202 862 2262	joseph.moreno@cwt.com
Joseph Facciponti	+1 212 504 6313	joseph.facciponti@cwt.com
Keith Gerver	+1 202 862 2381	keith.gerver@cwt.com
Peter Carey	+1 202 862 2339	peter.carey@cwt.com

programs are designated as "Tier 1 – Partial" while organizations that can respond to sophisticated cyber threats "in real time" through "continuous monitoring" of systems are designated as "Tier 4 – Adaptive."

[8] A Framework Profile is a list of cyber activities that an organization has selected based on its business needs and risk assessment.