THE PRIVACY ADVISOR
The Official Newsletter of the International Association of Privacy Professionals
iapp

The future of the NIST Cybersecurity Framework

Mark Francis, CIPP/US, CIPT

The Privacy Advisor | Apr 25, 2016

On April 5-7, the National Institute of Science and Technology hosted a Workshop on its "Framework for Improving Critical Infrastructure Cybersecurity." The workshop was extremely well-attended, with more than 900 registrants and hundreds more attending by webcast. It was preceded by a NIST request for information, which prompted 105 responses, many from industry associations representing hundreds of companies. NIST released an Analysis of Cybersecurity Framework RFI Responses on March 24, 2016, which served as a basis for the workshop's agenda and dialogue.

What is the framework?

In 2013, President Obama issued Executive Order 13636 and directed NIST to work with stakeholders in developing a voluntary framework—based on existing standards, guidelines, and practices, for reducing cyber risks to critical infrastructure. NIST released version 1.0 of the framework in February 2014, describing it as a voluntary "risk-based approach to managing cybersecurity risk" for organizations of all shapes and sizes.

- The "core" is the nucleus of the framework and comprises five functions that reflect the full lifecycle of a cybersecurity risk management program: identify, protect, detect, respond and recover. These functions are comprehensively broken down into 22 categories and 98 subcategories, which are mapped to various informative references, such as the Critical Security Controls, ISO 27001 and NIST SP 800-53.
- A "profile" comprises the tier rankings across all categories and reflects a particular state of cybersecurity risk management. For example, a "current profile" reflects the current tier rankings. An organization can prioritize key areas for improvement and set out to achieve "target" profile represented by a higher tier ranking in those areas.

Who is using the framework?

NIST recently cited a Gartner report that the framework is used by 30 percent of U.S. organizations, with projected use of 50 percent by 2020.

According to a March 2016 survey by Dimensional Research, adoption of the framework may reach 43 percent by the end of 2016. Use of the framework was attributed to three key motivations: aligning with cybersecurity best practices (70 percent); business partner requirements (29 percent); and federal contract requirements (28 percent).

What is it good for?

The framework is frequently distinguished as being not a technical standard or set of security controls, but rather a more holistic risk management tool that excels in a number of areas:

- It is layered above technical standards to provide overarching guidance that can drive corporate policies and validate risk management strategies;
- It provides a template for providing corporate directors and officers with an assessment of their organization's cybersecurity posture, program maturity, and residual risks;

- The framework can also be used for corporate budgeting by mapping planned investments and project roadmaps to particular Functions or Categories;
- It also provides a common language for communicating an organization's cybersecurity posture to external stakeholders such as auditors, insurance underwriters, and regulators;
- Since the Framework overlays standards like the CSC, ISO 27001 and NIST SP 800-53, it can be employed as an added tool without the expenses typically incurred when adding, or transitioning to, a new standard; and,
- The framework serves a dual purpose in reducing legal risk. First, the framework embraces many of the cybersecurity practices that are central to consumer lawsuits and government enforcement actions (such as governance, policies and incident response), and thereby prepares organizations to effectively mitigate their legal exposure. Secondly, organizations using the framework can point to government stewardship and public-sector recognition as affirmative evidence that their security program is "reasonable," which is typically the fundamental question in a legal context.

Do we need an upgrade to 1.1 or 2.0?

The majority of respondents to the NIST RFI (by 3:1) believe an update to the framework is warranted, and workshop participants echoed this sentiment. Desired updates to the Framework Core include more emphasis on supply chain risk management and updating or expanding the informative references. NIST is also working on further guidance for the core's "recovery" function. The "tier" model was also identified as an area for improvement, given that it is currently being applied somewhat subjectively. NIST indicated that it plans to work towards a "version 1.1," not a more drastic "2.0," in part to minimize the impact of any changes on organizations already using of the framework.

While there is broad interest in funneling sector-specific guidance through NIST to maintain some uniformity, some sectors (including energy, finance and telecommunications) have already released industry or regulatory guidance based on the Framework, and there is an increasing likelihood of diverging framework archetypes.

NIST stewardship: do we stay or do we go?

Although everyone praises NIST for its development of the framework, RFI respondents and workshop participants split on whether to transition governance of the framework to another institution.

In view of NIST's great work to date, one group recommends keeping the status quo. A second group believes that transition may be beneficial in the future but would be premature at this time. A third group counsels a quicker transition to a venue with greater private sector influence in framework development. In addition, the third group suggests that foreign governments and organizations are reluctant to use the framework while it is managed by a U.S. government agency, whereas stewardship by a respected non-governmental organization could result in broader acceptance and international relevance. While this view does have merit, the framework's domestic success is likely due to NIST, as many U.S. companies see business and legal upsides to using a Framework (i) developed by the government (ii) at the behest of an Executive Order (iii) with subsequent approval by many influential regulatory agencies.

There was, however, consensus on the desired characteristics of any potential successor: a neutral non-profit organization with international reach, respected for technical proficiency, and willing to keep the framework free, with participation open to all interested parties.

While NIST and other stakeholders will likely continue evaluating potential transition of the framework to another institution, it appears that NIST will continue overseeing the project for the foreseeable future. NIST also emphasized that it would seek to maintain an active role in the framework's stewardship even after any transition.

Everyone wants everyone else to share

There was near unanimous consensus that the cybersecurity community would benefit greatly from increased sharing of framework-related practices. A number of sharing paradigms were discussed, including:

- Open forums for sharing practices;
- Published use cases that can help organizations assess implementation and costs (such as the Intel publication);
- Practical steps for getting started with the Framework, especially for small and midsize businesses;
- Guidelines for more objectively assessing Tiers and Profiles, possibly calibrated by sectors and business needs;
- Lessons learned, with an eye towards the people, process and technology perspectives;

- Sector-specific implementation guides (like the Best Practices guidance prepared by the FCC with industry participants); and
- Measurement tools and validation tests (discussed below).

Unfortunately, very few businesses have expressed interest or willingness to publicly share such information because there is little tangible upside but a number of potential downsides. First, cybersecurity is viewed by many as a competitive advantage. Second, many organizations fear that their shared "best practices" will eventually be used as a heightened cybersecurity baseline in regulations and legal standards for reasonableness. Third, they are concerned that information they share will be used against them by government authorities, litigants, or malicious actors. Disclosures to NIST in return for anonymity could be undermined by FOIA requests, and while submissions offered through industry associations could be an option, that carries its own set of challenges, including potential antitrust issues.

How do you measure success?

There is strong interest in a standard set of metrics for the Framework, particularly self-assessment, conformity or confidence tools. They could prove very useful when reporting to corporate officers and directors, or when exhibiting an organization's cybersecurity posture to external stakeholders such as auditors, insurance underwriters, and regulators. Although some self-assessment tools have been developed (such as the DHS's Cyber Resilience Review), there is no consistent approach tied to the framework.

Unfortunately, little headway was made on this topic. For example, it is unclear if metrics should take the form of a more robust tier/profile system, a "compliance" checklist, or some other template.

It is also unclear if framework conformance should be assessed through narratives or through some methodology for numerical valuation. Ascribing values to cybersecurity risks would be particularly challenging because many cyber practices, such as incident response, are not repetitive activities that are easily measureable. In addition, cyber practices are often applied inconsistently across organizations due to technical, business, legal and regional realities. It can be challenging to accurately condense hundreds of such permutations to a handful of numerical metrics that accurately reflect cyber risk.

Despite these challenges, the strong interest on this topic may prompt efforts towards a standard approach for assessing and quantifying cyber risk based on the framework, in order to "price risk" and more effectively communicate with internal and external stakeholders about cyber risk at the enterprise level.

Harmonization with other standards

CIOs, CISOs and other personnel tasked with proving conformance to cybersecurity standards are suffering from compliance fatigue. PCI-DSS is required for businesses that handle payment transactions, many companies with foreign operations are compelled to certify with ISO 27001, and many businesses are adopting the CSC, especially in view of the California Attorney General's recent report stating that "failure to implement all the [CSC] controls that apply to an organization's environment constitutes a lack of reasonable security." These organizations must also achieve compliance with numerous U.S. and foreign data security regulations, as well as business partners' contractual data security requirements.

Since the framework operates as an overlay for many technical standards, there is a lot of interest in harnessing the framework to harmonize the implementation of technical controls and reduce the burden of individual compliance with numerous standards and requirements.

NIST to forge ahead, encouraging the industry to continue doing its part

NIST aims to release a report on the workshop by mid-May, and will continue to solicit input from public and private sector participants on future posted material. Although there is no silver bullet in cybersecurity, the framework has been found to offer unique value to organizations, and NIST hopes to keep up the momentum by improving the framework's usefulness as a flexible and practical tool for managing cybersecurity risk.

***Mark Francis**, CIPP/US, CIPT, is an associate at Reed Smith LLP in New York, where he specializes in cybersecurity, data privacy and intellectual property.*