Cybersecurity In 2014: A Look Back At The NIST Framework

Law360, New York (December 16, 2014, 10:00 AM ET) –

One of the more significant cybersecurity developments in 2014 was the release of the "Framework for Improving Critical Infrastructure Cybersecurity"[1] by the National Institute of Standards and Technology. Directed by the White House in Executive Order 13636, the framework was released on Feb. 12, 2014, and was the result of a yearlong collaborative process between the public and private sectors to develop voluntary standards for managing cyber-risk to critical infrastructure. The framework outlines a strategy for use by organizations to improve their policies and procedures for managing cyber-risk and for responding to cyber incidents.

We outline here some of the key qualities of the framework — namely, its adaptability, structure and voluntary nature — and outline several framework-related developments during the preceding year.

The Framework Is Flexible

The framework is intended to assist the broad array of entities that provide services as, or operate using, critical infrastructure, i.e., those systems or assets that if incapacitated or destroyed, would have a debilitating impact on national security, economic security, or public health, such as transportation, financial services, energy and utilities, government, and the Internet. In April 2014, the U.S.Department of Homeland Security, acting pursuant to Executive Order 13636, identified entities and assets that qualified as "critical infrastructure" and confidentially notified the relevant owners and operators.[2] DHS has indicated that it may identify and notify others in the future.

The framework is meant to be updated and improved in response to industry feedback. Consistent with this approach, NIST held meetings convened by associations at state, regional and national levels throughout the year, and it continues to do so. Most recently, NIST held a workshop on Oct. 29 and 30, 2014, after soliciting responses to a request for information from stakeholders, including the private sector, academia and government, regarding their experience with the framework.[3] Participants reported using the framework for a variety of purposes, including communicating with executive leadership, raising awareness within an organization, and sharing expectations with business partners and suppliers. Some participants also reported using the framework to benchmark performance within or between organizations.

In conjunction with the release of the framework, NIST also issued a "Roadmap for Improving Critical Infrastructure Cybersecurity"[4] that outlined the next steps for advancing the framework and its implementation and areas for which NIST will continue to seek comment, including international cybersecurity, cybersecurity workforce, data analytics, authentication, federal agency cybersecurity alignment and supply chain risk management.

The Framework's Structure Is Risk-Based

The framework is structured such that it can be used both by entities that have sophisticated cybersecurity programs in place and by those that are only beginning to develop their programs. The framework encourages organizations to prepare a profile of the organization's cyberattack readiness and then identify a target profile that reflects its desired readiness based on an analysis of the likelihood and impact of a cybersecurity event. The framework can then be used to implement an action plan to help an organization move from its current profile to its target profile.

The framework uses three categories to facilitate the efficient and effective implementation of standards for managing cyber-risk to critical infrastructure and to be accessible to senior-level and operations-level personnel alike: (1) the framework core, (2) the framework profile, and (3) the framework implementation tiers.[5]

The framework core utilizes core functions, such as identifying and protecting organizational systems and data in need of protection, and detecting and responding to a cybersecurity event. The framework core functions are divided into categories and subcategories, which reference existing industry security

standards such as NIST, ISA, ISO and COBIT standards. The framework borrows these standards to facilitate the implementation of the framework across all industries and within existing standards-specific compliance programs. As an additional resource for users, NIST released a midyear Cybersecurity Framework Reference Tool, which allows a user to search and review the framework core by functions or categories, run word searches, and export data into various file types.[6]

The framework profile describes how the framework core may be used by a critical infrastructure organization to create a plan to reduce its cyber-risk. The framework's implementation tiers provide a ranking system that assists organizations in assessing the sophistication of their cyber-risk management practices. The framework profile and implementation tiers, when used together, are intended to provide an organization with a flexible roadmap to achieve its cybersecurity goals.

After considering the framework core functions, an organization should compare its current and desired cybersecurity profiles and create an action plan to eliminate any identified gaps. NIST does not provide industry or sector templates to facilitate an organization's analysis of current and target profiles. Rather, it allows for a high degree of flexibility in self-assessments.

The Framework Is Voluntary

To encourage adoption of the framework, NIST and the DHS partnered to create the Critical Infrastructure Cyber Community C3 Voluntary Program. In the past year, the C3 Voluntary Program has engaged with "Sector-Specific Agencies" to develop guidance on how to use the framework. The C3 Voluntary Program plans at a later point to extend its outreach to any critical infrastructure and businesses interested in using the framework.[7]

While Executive Order 13636 calls for the creation of incentives to promote adoption of the framework, the administration is still considering a variety of options, including limitations on liability, cybersecurity insurance, grants, public recognition, streamlining regulations, allowing rate-regulated utilities to recover for participation, and granting preferences in the delivery of certain government services.[8]

Many users have expressed concern that Congress or a regulatory authority could make the framework standards mandatory for compliance purposes, or that they will become de facto standards as part of a "set of industry standards and best practices" against which an organization's actions may be judged in litigation and regulatory enforcement actions. The voluntary nature of the framework may also be reduced by any incentives offered to framework adopters, such as by placing those organizations that do not adopt the framework at a competitive disadvantage.

Recent Framework-Related Developments

Framework-related developments in the preceding year include:

- International Cybersecurity: NIST and other U.S. officials have discussed the framework and international coordination of cybersecurity with representatives of the United Kingdom, Japan, Korea, Israel, Germany, Australia, and others.[9]

- Authentication: NIST has partnered with the Identity Ecosystem Steering Group, which is preparing a self-assessment and self-attestation program that it plans to release in early 2015.

- Automated Indicator Sharing: On Oct. 29, 2014, NIST released a draft "Guide to Cyber Threat Information Sharing." The publication provides guidance on coordinating and sharing information across organizations in responding to a cyber incident.[10]

- Supply Chain Risk Management: On June 3, 2014, NIST publicly released the second draft of its publication, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations."[11]

In 2015, we expect that more critical infrastructure stakeholders will adopt the framework and that NIST and the DHS will continue to promote the use of the framework by the private sector and international stakeholders alike.

—By Mauricio Paez, Jay Johnson and Bart Green, Jones Day

Mauricio Paez is a partner in Jones Day's New York office. Jay Johnson is of counsel in the firm's Dallas office. Bart Green is an associate in the firm's Irvine office.

This year-in-review article follows the authors' prior articles published in Law360 on the framework: "Spotlight on the New US Cybersecurity Plan" and "Inside NIST's Final Cybersecurity Framework."

[1] Available at: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

[2] National Protection and Programs Directorate; Notice of Completion of Notification of Cyber-Dependent Infrastructure and Process for Requesting Reconsideration of Determinations of Cyber Criticality, 79 Fed. Reg. 21780 (Apr. 17, 2014).

[3] NIST, "Update on Cybersecurity Framework" (Dec. 5, 2014). Available at: http://www.nist.gov/cyberframework/upload/nist-cybersecurity-framework-update-120514.pdf.

[4] Available at: http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf.

[5] For a more detailed description of the Framework Core, the Framework Profile, and the Framework Implementation Tiers, please see our Law360 article, "Inside NIST's Final Cybersecurity Framework" (Feb. 12, 2014). Available at: http://www.law360.com/articles/509763/inside-nist-s-final-cybersecurity-framework.

[6] Available at: http://www.nist.gov/cyberframework/csf_reference_tool.cfm.

[7] Critical Infrastructure Cyber Community C3 Voluntary Program website (last visited on Dec. 9, 2014). Available at: https://www.us-cert.gov/ccubedvp.

[8] C3 Voluntary Program, Frequently Asked Questions. Available at: https://www.us-cert.gov/sites/default/files/c3vp/ccubedvp-outreach-and-messaging-kit.pdf; see also Michael Daniel, Special Assistant to the President and the Cybersecurity Coordinator, "Incentives to Support Adoption of the Cybersecurity Framework, The White House Blog (Aug. 6, 2013). Available at: http://www.whitehouse.gov/blog/2013/08/06/incentives-support-adoption-cybersecurity-framework.

[9] NIST, "Update on Cybersecurity Framework" (July 31, 2014). Available at: http://www.nist.gov/cyberframework/upload/NIST-Cybersecurity-Framework-update-073114.pdf.

[10] Available at: http://csrc.nist.gov/publications/drafts/800-150/sp800_150_draft.pdf.

[11] Available at: http://csrc.nist.gov/publications/drafts/800-161/sp800_161_2nd_draft.pdf.