Spotlight On The New US Cybersecurity Plan

Law360, New York (October 23, 2013, 12:02 AM ET) --

On Oct. 22, 2013, the National Institute of Standards and Technology (NIST) released its preliminary cybersecurity framework to help owners and operators of critical infrastructure manage cyber-risk. The framework stems from President Obama's Executive Order 13636 on cybersecurity, issued earlier this year.

President Obama ordered the federal government to identify critical infrastructure vulnerable to cyberattacks, acknowledging that the ever rising number of cyberattacks on "critical infrastructure represents one of the most serious national security challenges we must confront." The executive order called for the development of procedures to improve the sharing of information between the public and private sectors about cyberattacks, and a framework that utilizes existing standards where possible to reduce the risk to critical infrastructure (i.e., the systems and assets that if incapacitated or destroyed, would have a debilitating impact on national security, economic security, or public health and safety). Though preliminary, the framework provides early insight into the direction of the final draft, due in February 2014.

The Structure of the Framework

NIST's framework encourages critical infrastructure organizations to (1) create a "current profile" of an organization's existing cyberattack readiness, (2) develop a "target profile" that reflects its readiness based on an analysis of the likelihood and impact of a cybersecurity event, (3) identify "gaps" between the profiles, and (4) implement an action plan that addresses and eliminates such gaps. The framework largely borrows from a variety of existing industry security standards — e.g., International Society of Automation (ISA) standards, International Organization of Standardization (ISO) standards — which should lessen the burdens associated with compliance and avoids a one-size-fits-all approach.

The framework provides guidance in three parts: the framework core, the framework profile and the framework implementation tiers. This structure is intended to facilitate the efficient and effective implementation of the framework.

Framework Core

The framework core presents standards common across various critical infrastructure sectors. It can be used by senior-level and operations-level employees alike. It references certain core functions that include (1) identifying and prioritizing organizational systems, assets, data and capabilities that need to be protected, (2) protecting those systems, assets, data and capabilities with appropriate safeguards to ensure the delivery of critical infrastructure services, (3) detecting a cybersecurity event, (4) responding to that event, and (5) restoring capabilities that may have been impaired by the event.

Each of these core functions is divided into categories, which in turn are divided into subcategories. With each division, the framework's concepts become more concrete. For example, to guide organizations in identifying and prioritizing organizational systems, assets,

data and capabilities as directed, the "identify" function includes "risk management strategy" as a category, by which the organization's priorities and tolerance for risk are used to support operational decisions. The framework then divides risk management strategy into subcategories, including among others an assertion that the organization's tolerance for risk is informed by its role in critical infrastructure and an analysis of the risks specific to the relevant industry sector. For this subcategory, NIST included in the framework references to NIST SP 800-53 Rev. 4 as guidance, an NIST special publication for the computer security community.

By dividing framework core functions that identify high-level cybersecurity activities into categories and subcategories with reference to existing industry standards, the framework core matches preferred cybersecurity outcomes with known solutions.

Framework Profile and Use of the Framework Implementation Tiers

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. Tier 1 demonstrates, for example, a limited awareness of cyber-risk and a lack of any formalized cyber-risk management or system for sharing cyber-risk information. Tier 4, on the other hand, describes an organization that engages in a continuous process of improving cyber-risk management and makes managing cyber-risk part of its culture.

After considering the framework core functions, including their categories and subcategories and the standards referenced in each, an organization is expected to identify its current and desired cybersecurity profiles. Through an identification, assessment and prioritization of gaps between the two, the organization should create an action plan to eliminate these gaps. However, 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-assessing both. When used together, the framework profile and implementation tiers provide an organization with a flexible roadmap to achieve its cybersecurity goals.

What the Framework Means to Organizations

The actions called for in the framework are voluntary. The president has made that clear. However, the potential provision of incentives, such as grants, liability protection and others, may place those organizations that do not comply at a competitive disadvantage. Moreover, compliance with the framework ultimately may be viewed as part of the industry standard of care, against which an organization's actions may be judged. The potential for either may in effect mandate compliance.

The framework is noteworthy for what it does not address — namely, critical issues concerning supply chains and interdependencies, personal data privacy best practices, data analytics and others. As such, it is likely to have its critics, and may be viewed more as guidance to organizations that have more sophisticated cybersecurity measures in place. Rather, the framework could best be viewed as a place to start, rather than the goal for organizations that

face significant and ongoing cyberthreats to their critical infrastructure, intellectual property assets and personal data.

Ultimately, the final version of the framework will provide a big picture outline of cybersecurity issues that organizations can use as a tool to improve their policies, procedures and protocols for managing cyber-risk, and to shape a governance structure to better respond to cyber incidents. Critical infrastructure organizations would be wise to use this framework as an early guide. Organizations are encouraged to participate in the public comment period during the coming 45 days, and during the final NIST workshop to be held Nov. 14 and 15, 2013, at North Carolina State University.

—By Mauricio F. Paez, Richard J. Johnson and Bart Green, Jones Day

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