U.S. RELEASES **CYBERSECURITY FRAMEWORK** FOR CRITICAL INFRASTRUCTURE

by Jenny Mangelsdorf

For some companies, the worst fallout from a cyberattack may be hits to earnings, loss of competitive edge or enduring damage to customer relationships. However, for owners and operators of critical infrastructure, a successful attack could affect a nation. To curb that risk, the U.S. National Institute of Standards and Technology (NIST) has released a Cybersecurity Framework. While the government hasn't tied mandates to the new framework, other incentives will prompt its use.

President Barack Obama directed the development of the framework last year when he issued Executive Order 13636, Improving Critical Infrastructure Cybersecurity, and Presidential Policy Directive 21, Critical Infrastructure Security and Resilience, to help owners and operators of critical infrastructure reduce their risk of attack.

The directive, which establishes U.S. policy on critical infrastructure security, has three strategic goals aimed at improving functional relationships, information exchange and operations decisions. The order includes strengthened federal distribution of cyberthreat information and the development of the Cybersecurity Framework.

"Enhancing national and homeland security through better cybersecurity is the whole purpose of the order, directive and new framework," says Sam Visner, CSC global cybersecurity vice president and general manager. "The president has asked owners and operators to play a stronger part in securing the nation's infrastructure. At the same time, owners and operators can gain real value from those actions."

Voluntary use and incentives

Use of the new framework, while voluntary for owners and operators of critical infrastructure, may be tied to incentives in future versions. For example, those complying with the framework's guidelines might receive prioritized technical assistance for nonemergency cybersecurity incidents. The potential for improving cybersecurity by using the new framework will also motivate organizations.

"Companies that meet all of the framework's recommendations should expect a higher level of cybersecurity than those that do not," says Guy Copeland, CSC global cybersecurity senior principal, Information Infrastructure Advisory Programs.

Another incentive for using the framework will be to reduce legal risks, as experts expect that organizations that do not follow the framework will face increased common law liability. With NIST coordinating the framework's year-long development effort, which included comments, changes and thousands of hours of private sector participation, the framework has the attributes of an industry standard, says Gerald Ferguson, a partner with law firm BakerHostetler and co-leader of the firm's national Privacy and Data Protection team. "Once industry members are invited to be the framework's custodians, there won't be any doubt that [the framework] will function as an industry standard," he adds.

The framework includes a set of tiers that describe the degree to which an organization's cybersecurity risk management adheres to the framework's goals. The levels range from "Tier 1, Partial" (reactive, informal responses) to "Tier 4, Adaptive" (agile, risk-informed approaches that indicate rigor and sophistication).

"Those who think that market incentives won't motivate companies to adopt the framework are not taking into account the extent to which private litigation impacts companies in the United States," says Ferguson. "Companies should be ready for class action suits to act as enforcers of the framework, and those defending their cybersecurity practices in litigation or regulatory investigations should be prepared to show that their practices adhere to Tier 4."

Just as standards and threats continue to increase in sophistication, the framework will continue to evolve to adopt lessons learned and new advances in cybersecurity. As NIST continues its coordinating role, with the framework's release, the Department of Homeland Security (DHS) has launched the Critical Infrastructure Cyber Community C^3 (pronounced "C Cubed") Voluntary Program to encourage use of the framework, and to help build a strong stakeholder community that will be key in developing standards and employing them to better protect infrastructure nationwide.

Suzanne Spaulding, acting under secretary for the National Protection and Programs Directorate, notes in a Feb. 12, 2014, DHS blog that "the C^3 Voluntary Program emphasizes three C's:

- Converging critical infrastructure community resources to support cybersecurity risk management and resilience through use of the framework;
- Connecting critical infrastructure stakeholders to the national resilience effort through cybersecurity resilience advocacy, engagement and awareness; and
- Coordinating critical infrastructure cross-sector efforts to maximize national cybersecurity resilience."

"We've enjoyed partnering with the government on the framework's development and look forward to continuing to do so as it shapes the voluntary program," says CSC's Copeland, who is also co-chair of the DHS Cross-Sector Cybersecurity Working Group and was an active participant in the framework's development.

Opportunities to reduce risk

Both the framework and other deliverables generated by the order and directive, such as access to threat data (see sidebar), provide opportunities for companies that are willing to participate in new DHS programs.

"Organizations need to understand what they are being asked to do in support of national and homeland security, what standards the government believes are pertinent to their business, what regulations are relevant, and what information they are being encouraged to share," says Visner. "They also need to make sure they understand that these are actions they want to take and that they are positioned to leverage these opportunities."

In the future, the order and directive may drive additional voluntary practices, and possibly new regulations, incentives and mandates, for identified critical infrastructure operators and owners. The DHS' new C^3 Voluntary Program will first focus on supporting those operating in the 16 critical infrastructure sectors identified in last year's directive, along with associated sector-specific agencies.

"We are seeing the same threats in the systems of our manufacturing and financial services customers as we do at sensitive government facilities," says Visner. "Make no mistake — these are weapons-grade threats, and the intent to do harm is unprecedented. Cybersecurity has moved from an issue of compliance to an issue of existence." ■

JENNY MANGELSDORF is a writer for CSC's digital marketing team.

New Access to Threat Data

Alongside the new Cybersecurity Framework, another key deliverable prompted by the executive order is the opportunity for organizations to obtain valuable, previously unavailable threat data. Used properly, such data could prevent attacks.

The order directs the government to share a greater amount of timely cyberthreat data that infrastructure owners and operators can use to protect their systems. DHS addressed that through the launch of the Enhanced Cybersecurity Services program, which the government uses to share classified information with IT and communications technology providers to better secure their critical infrastructure customers' networks.

"This is not the kind of data that is intended to help the moms-and-pops battle malicious attempts to get into their systems; this type of data addresses threats that could result in large-scale disruption or damage," says Guy Copeland, CSC global cybersecurity senior principal, Information Infrastructure Advisory Programs. "For example, this could include data on nation-states trying to damage our electric power distribution system, steal intellectual property from aerospace manufacturers or counteract our weapons systems."

To take advantage of this new source of data, owners and operators of critical infrastructure have to develop a capability that enables them to quickly access, understand and use this information. Companies also need to determine what information is appropriate to share with the government and other designated operators and owners.

Learn more at **csc.com/cybersecurity.**