msk

cybersecurity update – how are you impacted?

MSK Client Alert

February 28, 2014

On February 12, 2014, the Obama Administration released the long-awaited Cybersecurity Framework: "a voluntary how-to guide for organizations in the critical infrastructure community to enhance their cybersecurity" (the "Framework"). A year earlier, Executive Order 13636, regarding *Improving Critical Infrastructure Cybersecurity*, was issued. In that Executive Order, the Administration established the need for a governmental partnership with the owners and operators of critical infrastructure to collaboratively develop and implement risk-based standards. Although "voluntary" in nature, it is easily foreseeable that the Framework will become industry standard, raising the specter of how companies, even those who do not deal with government contracting or critical infrastructure, will be expected to meet those standards.

Whether you are securing your supply chain or are, for example, a retailer worried about being hacked, the Framework proposes a unified process by which to evaluate your cybersecurity program: 1) Describe your current cybersecurity posture; 2) Describe your target state for cybersecurity; 3) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process; 4) Assess progress toward your target state; and 5) Communicate among internal and external stakeholders about cybersecurity risk. If you have an intrusion, it seems reasonable that authorities (and your insurance company) will be checking to see how you have implemented this process, even if you are not a government contractor.

The 2013 Executive Order was directed at critical infrastructure and called for the Attorney General, the Secretary of Homeland Security (Secretary), and the Director of National Intelligence (Director) to issue instructions to ensure the timely production of unclassified reports of cyber threats that identify specific targeted entities and to enhance information sharing through an expanded "Enhanced Cybersecurity Services" program.

attorneys

Susan Kohn Ross

practice areas

corporate & business transactions

cybersecurity and privacy

general corporate law

los angeles
t 310.312.2000
f 310.312.3100

new york
t 212.509.3900
f 212.509.7239

washington, dc
t 202.355.7900
f 202.355.7899

The Framework was described as intended to "provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk" and "shall focus on identifying cross-sector security standards and guidelines applicable to critical infrastructure." It was also to "identify areas for improvement" to be addressed through future collaboration with various parts of the private sector, including standards-developing organizations. To enable technical innovation and account for organizational differences, the Framework was expected to provide guidance that is "technology neutral" and enables "critical infrastructure sectors to benefit from a competitive market for products and services" that meet the "standards, methodologies, procedures, and processes" developed to address cyber risks. The Framework was to include guidance for measuring the performance of an entity in implementing it and was also to include methodologies to identify and mitigate its impacts and associated information security measures or controls on business confidentiality and to protect individual privacy and civil liberties.

The Secretary of Defense and the Administrator of General Services were to make recommendations to the President on the "feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration" and were also to deal with steps that could be taken to "harmonize and make consistent existing procurement requirements related to cybersecurity," and this is the area where the private sector has the most interest. Once there are standards in place for government procurement purposes, the affected companies will be mandated to meet those standards and will require their business partners to meet those standards, and, shortly thereafter, it is easily foreseeable that most other companies, whether or not dealing in defense or other government contracting disciplines, will be expected to meet those same standards. For any company that does not, significant issues can be expected, including intrusions, along with class action and shareholder derivative lawsuits.

The Executive Order was far-reaching, but so is the Framework, which represents a year's worth of collaboration between the government and the private sector gathering "thoughts on the kinds of standards, best practices, and guidelines that would meaningfully improve critical infrastructure cybersecurity." At heart, the Framework is an attempt to set forth a common language with respect to five cybersecurity activity core functions and to provide a common set of tools for building and analyzing an organization's activities and responses within each core function. To that end, the Framework is implemented on three levels: the Framework Core, the Framework Profile, and the Framework Implementation Tiers.

The Framework Core (Core) is a set of cybersecurity activities, desired outcomes, and references that are common across "critical infrastructure sectors." The Core covers five concurrent and continuous functions — Identify, Protect, Detect, Respond, Recover — designed to provide a 100-foot view of the lifecycle of an organization's management of cybersecurity risk. For each of these lifecycle functions, the Core then identifies underlying key categories, and subcategories, and matches them with exemplar references, such as existing standards, guidelines, and practices. For instance, under Detection, a key category is detection of anomalies and events. One of the subcategories is establishing and managing a baseline of network operations and expected data flows for users and systems. There are then several potential standards and guidelines listed to assist with that functionality, including COBIT 5 DSS03.01, ISA 62443-2-1:2009 4.4.3.3, and NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2, SI-4.

The second level of the Core is the Framework Implementation Tiers, which essentially provide a numerical representation of how advanced an organization's risk-mitigation procedures are, given the threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints. The Tiers range from Partial (Tier 1) to Adaptive (Tier 4). Because an individual organization's cybersecurity risk is taken into account, not every organization needs to be Tier 4, as doing so would not be cost effective, given a lower level of cybersecurity risk. The Framework notes that, "[w]hile organizations identified as Tier 1 (Partial) are encouraged to consider moving toward Tier 2 or greater, Tiers do not represent maturity levels. Progression to higher Tiers is encouraged when such a change would reduce cybersecurity risk and be cost effective."

Finally, the third level of the Core, the Framework Profile (Profile), represents the outcomes the organization selected from the Framework Categories and Subcategories. A Profile enables the organization to establish a road map for reducing cybersecurity risk in a manner aligned with organizational and sector goals, considers legal/regulatory requirements and industry best practices, and reflects appropriate risk-management priorities. Armed with the profile, and target profiles, the Framework allows the organization to evaluate risk vulnerabilities and create a prioritized action plan to address those gaps.

The question for all companies now is how best to adapt to these new recommendations and do so in a cost-effective and meaningful manner.

For those interested, the final report can be found here.