February 14, 2014

Framework for Managing Cybersecurity

On February 12, the National Institute of Standards and Technology (NIST) released a voluntary cybersecurity framework designed to address the heightened business and security risks that come from increased reliance on information technology and industrial control systems.* The growing interconnectivity of these systems and their increasing use to deliver critical business services and support business decisions have exacerbated the potential impact of a cybersecurity incident on an organization's business, assets and reputation.

NIST's recommended cybersecurity framework urges banks, utilities and other critical infrastructure operators to adopt a set of industry standards and best practices to manage cybersecurity risks. The framework is the result of collaboration between government and the private sector, and it encourages organizations to consider cybersecurity risks as part of their overall risk management processes. It augments requirements already in effect for some businesses, such as the North America Energy Reliability Corporation's Critical Infrastructure Protection plan applicable to electric industry participants. For financial services providers, NIST's recommended framework has been endorsed by the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC). Established in 2002, the FSSCC is the coordinator for financial services providers for the protection of critical infrastructure, focusing on operational risks.

NIST's recommended cybersecurity framework is designed to provide common terminology to discuss cybersecurity issues and describes mechanisms for organizations to:

1. evaluate their current cybersecurity readiness;
2. articulate their cybersecurity goals;
3. identify and prioritize opportunities for improving their cybersecurity procedures;
4. assess progress toward their cybersecurity goals; and
5. communicate about cybersecurity risks both internally and externally.

There are three parts to the cybersecurity framework: the Framework Core, the Framework Profile and the Framework Implementation Tiers. The Framework Core provides detailed guidance for developing a set of cybersecurity procedures that are common across critical infrastructure sectors. The common standards, guidelines and practices are designed to facilitate communication about cybersecurity activities between an organization's management and those implementing the organization's cybersecurity systems. The Framework Core provides guidance and best practices for five functions: to identity cybersecurity threats; to protect critical information technology and industrial control systems; and to detect, to respond to and to recover from hostile cybersecurity events. The Framework Core identifies categories and subcategories for each function.

The Framework Profile of an organization is based on the categories and subcategories that the company selects for each function of the Framework Core. Organizations can use their Framework Profiles to determine their current state of cybersecurity readiness, describe a desired state of readiness and identify opportunities to reach this goal.

The Framework Implementation Tiers provide a method for organizations to evaluate their level of risk and threat awareness and to categorize the effectiveness of their security procedures. The tiers range from Partial (Tier 1) to Adaptive (Tier 4). Lower-tier responses are reactive and informal; higher-tier responses are adaptive and integrated throughout an organization's structure.

The NIST framework also includes recommendations on how organizations can better protect individual privacy and civil liberties through integration of privacy controls into their cybersecurity and risk management structures.

The cybersecurity framework is technology-neutral and relies on standards, guidelines and practices currently in use in the private sector. The framework seeks to create global standards that may be used across borders. In order for the framework to remain effective, NIST indicates that it will update and revise the framework as new practices, technologies and cybersecurity threats develop.

While the framework is described as voluntary and is targeted at selected industries, businesses in all industries should anticipate that their compliance programs will be measured against it and would be well-served to assess their cybersecurity readiness with reference to the framework. Jim Bowers, the head of Day Pitney's Compliance Risk Services group, has written in greater depth about growing cyber threats and NIST's efforts to develop the cybersecurity framework. For more information on this topic, see his article "Mitigating Data Breach Liability: In Search of a Best Practice."

Our team would be pleased to assist you in developing a cybersecurity readiness plan consistent with the newly issued cybersecurity framework.

*NIST Framework for Improving Critical Infrastructure Cybersecurity