Daniel Spitzer
Partner
D +1 (212) 751 4300
dspitzer@hodgsonruss.com

Alba Alessandro
Partner
D +1 (646) 218 7608
aalessan@hodgsonruss.com

Hodgson Russ LLP
1540 Broadway, 24th Floor
New York, NY 10036
F +1 (212) 751 0928
www.hodgsonruss.com

New U.S. Cybersecurity Framework Likely to Become Baseline Standard

On February 12, 2014, the Obama Administration released the first version of its new voluntary cyber security framework pursuant to a presidential executive order issued one year ago in response to Congress's failure to pass cybersecurity legislation. The Framework for Improving Critical Infrastructure Cybersecurity does not instruct companies what to do or what tools or applications to use. Rather, the Framework generally represents a compilation prepared by the National Institute of Standards and Technology – working with the Homeland Security Department and industry stakeholders – of known, publicly vetted standards that can be applied to identify, protect from, detect, respond to, and recover from risks. Some may criticize the Framework as containing little that is ground-breaking or new, but a significant part of its purpose is to create a shared vocabulary for discussing and describing cybersecurity that can be used by a broad range of companies in different industries to create and evaluate risk-management programs. Through the Framework, critical gaps in programs can be identified and plans tailored to meet the specific needs for each user.

Application and Framework Structure

Although the Framework is voluntary, critical infrastructure owners need to recognize that, if a company's cybersecurity practices are ever questioned during a regulatory investigation and litigation, the baseline for what is considered commercially reasonable is likely to become the Cybersecurity Framework. The Department of Homeland Security defines critical infrastructure companies broadly to include banking and finance, communications, critical manufacturing, the defense industrial base, energy, emergency services, food and agriculture, healthcare, information technology, utilities, and transportation systems. These companies should be prepared to document and demonstrate that their cybersecurity practices are consistent with the practices promoted through the Framework.

The Framework is built on three basic components:

Core. A set of common activities that should be used in all programs, providing a high-level view of risk management.

Profiles. These help each organization align cybersecurity activities with its own business requirements, and to evaluate current risk management activities and prioritize improvements.

Daniel Spitzer
Partner
D +1 (212) 751 4300
dspitzer@hodgsonruss.com

Alba Alessandro
Partner
D +1 (646) 218 7608
aalessan@hodgsonruss.com

Hodgson Russ LLP
1540 Broadway, 24th Floor
New York, NY 10036
F +1 (212) 751 0928
www.hodgsonruss.com

New U.S. Cybersecurity Framework Likely to Become Baseline Standard

Tiers. Tiers allow users to evaluate cybersecurity implementations and manage risk. Four tiers describe the rigor of risk management and how closely it is aligned with business requirements.

Government incentives for adoption are expected to include public recognition, cybersecurity insurance and cost recovery programs. In addition, regulatory agencies are working to ensure that existing regulations correspond with the Framework, and government procurement requirements are likely to include conformance to the Framework for contractors and suppliers.

Assistance to Private Sector

The Department of Homeland Security is actively encouraging adoption of the Framework by the private sector and has launched a voluntary Critical Infrastructure Cyber Community program. The DHS Secretary has indicated that the program will provide a "single point of access" to the department's cybersecurity experts for anyone needing assistance. One of its services, the Cyber Resilience Review, has already been widely used by industry. Through the review process, organizations can evaluate their own programs and determine if they are in line with the practices and standards of the Framework.

Conclusion

The Cybersecurity Framework is just a first step in creating a cybersecurity guide for the nation's critical infrastructure sectors and establishes an important precedent by defining common security standards. It also brings together for the first time a useful set of federally endorsed practices for private sector security. It standardizes the questions all CEOs should ask about their companies' security practices as well as those of their suppliers, partners, and customers. Moreover, the Framework is likely become the de facto standard for private sector cybersecurity in the eyes of U.S. regulators and lawyers. Companies are therefore advised to document their compliance in order to be ready to demonstrate their cybersecurity practices are consistent with the practices promoted through the Framework.