KING & SPALDING

Client Alert

Privacy & Information Security Practice Group

February 25, 2014

Five Things Every In-House Counsel Should Understand About The NIST Cybersecurity Framework

While many in industry, particularly those in the Defense Industrial Base and government, have been sounding the alarm over cybersecurity for many years, only recently has it penetrated the American psyche. In fact, lately it seems as if a week does not pass without another front page story of the latest cyber-attack and loss of personal or proprietary information.

Along with this public awareness, policymakers have intensely debated the security of computerized data and the ability of public and private entities to respond to unauthorized penetration of computer networks. Indeed, concerns over data security have become ubiquitous across industries, and the risks associated with data breaches have reached everyone from those on Main Street to those in the C-Suite and the Boardroom.

Last year, President Obama tasked the National Institute of Standards and Technology (NIST) to create a Cybersecurity Framework to help protect critical infrastructure sectors. As described in our last Client Alert, on February 12, 2014, NIST released the Cybersecurity Framework, a copy of which can be found here. Given the breadth of what counts as "critical infrastructure," including Energy, Financial Services, Agriculture, Transportation, Health, Internet, E-commerce, and other sectors, this Framework may well have broad impact. In light of the Framework's voluntary standards, the question for in-house counsel is how to use it to best advise their clients on the many legal issues related to cybersecurity.

Here are some tips on how to best utilize the Framework and understand the path forward:

1. The Framework May Help Companies Weather Investigations and Avoid Liability.

Companies may be better positioned in investigations and litigation if they can show the Framework informs their cybersecurity practices. This is not to say that companies should adopt the Framework wholesale. In fact, the Framework disclaims establishing any sort of industry standard for cybersecurity. Pieces of the Framework may work well in one industrial sector but not in others, making further tailoring appropriate and necessary.

For more information, contact:

J.C. Boggs
+1 202 626 2383
jboggs@kslaw.com

Phyllis B. Sumner
+1 404 572 4799
psumner@kslaw.com

John A. Drennan
+1 202 626 9605
jdrennan@kslaw.com

Alexander K. Haas
+1 202 626 5502
ahaas@kslaw.com

King & Spalding

Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500

Atlanta, GA
King & Spalding LLP
1180 Peachtree Street
Atlanta, GA 30309
Tel: +1 404 572 4600

www.kslaw.com

Additionally, it is likely that critical infrastructure sectors, partnering with sector-specific regulatory agencies and industrial associations, will tailor the Framework for their needs.

But it is reasonable to anticipate that the Framework will be referenced as part of future challenges to companies' data-security programs. Cyber-attacks are hardly uncommon: nearly 50,000 were reported to the Department of Homeland Security (DHS) in 2012 alone. And it is reasonable to anticipate that if a company is identified as the victim of a cyber-attack, both government regulators and class-action plaintiffs' attorneys may scrutinize the company. This happened recently in the retail industry to Target and Neiman Marcus, which were hit with multiple class-action lawsuits, probes by state Attorneys General, and congressional hearings after announcing that large amounts of consumer data had been stolen. As a result, companies should be prepared to answer questions such as, "Did you consider the Framework in establishing your security practices?" and "How do your security programs align with the Framework?"

2. Government Agencies Will Strongly Encourage Companies to Adopt the Framework.

The federal government will press companies to consider adopting the Framework. The stage has already been set. In addition to the Framework, NIST issued a nine-page "Roadmap" that discusses the next steps NIST will take in updating the Framework, and includes plans to hold workshops and meetings to evaluate and modify the Framework. At the same time, the DHS established the Critical Infrastructure Cyber Community (C^3) Voluntary Program as a public-private partnership to increase awareness and use of the Framework. The C^3 program supports the use of the Framework, serves as the point of contact for companies to address Framework issues, and provides a mechanism for companies to share feedback with NIST about how the Framework can be improved. If implemented, these measures will blunt the force of arguments for not adopting the Framework, including the frequently heard claim that the Framework is futile because it will not be able to keep up with technological developments.

What's more, the government is likely to offer substantial incentives for companies to adopt the Framework. Not only did President Obama direct various agencies (including DHS, Commerce, and Treasury) to identify incentives, but last summer, the White House released a list of the incentives under consideration. The list is extensive: developing cybersecurity insurance; conditioning federal critical infrastructure grants on adoption; instituting access preference to government technical assistance; establishing liability limitations; streamlining regulations; establishing rate recovery for price-regulated industries; and pursuing cybersecurity research. While offering some of these incentives would require congressional action (*e.g.*, liability limitations), others potentially could be offered by the Executive Branch without Congress's involvement (*e.g.*, access preferences).

3. The Framework May be Just What the Doctor Ordered.

For companies that have been looking for a way to launch or improve a cybersecurity program but finding themselves struggling with where to start on this highly complex project, the Framework is good news. The Framework reflects NIST's cradle-to-grave approach to cybersecurity, addressing everything from making an initial assessment of the company's capacities and needs to responding to, and recovering from, an attack. The Framework also provides a process by which companies may tailor their security programs to the risks they actually face. This can be done on an ongoing basis: companies can and should update their security programs as their needs and vulnerabilities change, technology advances, and costs shift. Further, especially for some small and mid-sized companies, the Framework offers practical guidance on how to structure and execute credible security programs. And whatever the size of the company, because the Framework furnishes a common taxonomy and set of reference points that everyone from executive managers to IT staff members can use easily, the Framework may help to bridge potential divides between employees with disparate levels of understanding of cybersecurity or different cybersecurity concerns. While the concerns of the IT office may look very different from those of, say, the Privacy office, the Framework gives us all a way to intelligently discuss the issue of cybersecurity.

4. The Framework May Be Extended Informally Outside Of The Critical Infrastructure Sectors.

Although the Framework is addressed to companies in defined critical infrastructure sectors, there is little reason to suppose that its reach will be limited to them. Cybersecurity is a pressing concern in virtually all industries, and the Framework's broad vocabulary is not specific to any critical infrastructure sectors. Indeed, many of the informative references cited by the Framework were developed for uses outside the critical infrastructure sectors. Cybersecurity-related investigations and lawsuits involving companies outside of these sectors could well reference the Framework.

Further, supply-chain pressures (noted in the NIST Roadmap as requiring further study) may broaden the Framework's reach. Companies that are not considered part of the critical infrastructure sectors but that do business with firms in those sectors may wish to adopt the Framework to demonstrate to their business partners that they have appropriate security programs in place. Similarly, companies that serve as contractors or subcontractors for critical infrastructure sector members may face contractual pressures to adopt the Framework.

5. The Framework Is Just The First Step.

Action will shift during the coming year to sector-specific agencies and industry associations as NIST works to tailor or implement the Framework for specific industries. Industries could adopt the Framework as an "industry standard," outline a set of best practices, or even simply draft implementation guidance. Because pieces of the Framework may work well in one industrial sector but not in others, a tailored and thoughtful approach to cybersecurity issues is necessary. That said, it is easy to imagine how government investigators and the plaintiffs' bar could use the Framework against targets of cyber-attacks. It is also likely that state Attorneys General, for example, will continue to investigate cyber breaches that adversely impact the citizens of their states.

The private sector, however, should be circumspect about making public assertions concerning its adoption or use of the Framework. The Federal Trade Commission (FTC) has begun bringing lawsuits against entities related to their cybersecurity policies and practices and likely will insert itself into policing company statements to the public concerning the Framework where there is a possibility of deceptive or misleading statements that are made in violation of the broad strictures of Section 5 of the FTC Act.

Finally, there are renewed calls for cybersecurity legislation given that Congress has not enacted major cybersecurity legislation since 2002. While more than 50 federal statutes and almost all states have laws that directly or indirectly address aspects of cybersecurity, there is no overarching federal legislation. Earlier this year, Senate Judiciary Chairman Patrick Leahy (D-VT) and four other Senate Democrats introduced the Personal Data Privacy and Security Act of 2014. The legislation would create a national standard for data breach notification and require businesses to keep consumer information safe from hackers. The bill would also toughen criminal penalties for those who conceal a damaging breach, require companies that keep data to establish safety policies, and update computer hacking penalties.

Senate Homeland Security and Government Affairs Committee Chairman Senator Tom Carper (D-DE) and Senator Roy Blunt (R-MO) have also introduced the Data Security Act of 2014. The bill would require entities including financial institutions, retailers, and federal agencies to better safeguard sensitive information, investigate security breaches, and notify consumers when there is a substantial risk of identity theft or account fraud. Modeled on the Gramm-Leach-Bliley Act of 1999, the proposed requirements would apply to all businesses taking credit or debit card information, data brokers that compile private information, and government agencies that possess nonpublic personal information.

In the House of Representatives, the House Homeland Security Committee passed legislation earlier this month urging collaboration between the public and private sectors in responding to cyber threats and protecting critical infrastructure. The National Cybersecurity and Critical Infrastructure Protection Act of 2013 includes liability protections for private agencies that voluntarily cooperate on cybersecurity measures, cross-industry information sharing on cyber threats, and cyber-incident response teams to support critical infrastructure owners.

Several narrower bills have also been introduced in the U.S. House of Representatives, which include the:

- Cyber Intelligence Sharing and Protection Act (H.R. 624), which focuses on information sharing and coordination, including sharing of classified information;
- Cybersecurity Enhancement Act of 2013 (H.R. 756), which addresses federal cybersecurity R&D and the development of technical standards;
- Advancing America's Networking and Information Technology Research and Development Act of 2013 (H.R. 967), which addresses R&D in networking and information technology, including but not limited to security; and
- Federal Information Security Amendments Act of 2012 (H.R. 1163), which addresses FISMA reform.

The push for a federal breach notification law, which has stalled in Congress for years, has gained new momentum in the wake of the Target and Neiman Marcus data thefts. Just yesterday, Attorney General Eric Holder called for a federal law that would ensure companies warn customers when hackers seize their personal information. Holder said that "a strong national standard" for quickly alerting consumers about compromised information "would empower the American people to protect themselves" and "enable law enforcement to better investigate these crimes, and to hold compromised entities accountable when they fail to keep sensitive information safe."

And if Congress fails to act, the states are likely to continue to fill the gap and, at a minimum, strengthen state disclosure laws in the case of cyber breaches. Currently, 46 states, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands have enacted laws governing data security and data breach notification standards. Unfortunately, inconsistent and conflicting state-by-state standards force public and private entities to comply with multiple regulations, leaving many businesses and consumers in a confusing web of regulation depending on the state.

If you have any questions regarding this or related issues, please contact J.C. Boggs at +1 202 626 2383, Phyllis Sumner at +1 404 572 4799, Alexander Haas at +1 202 626 5502, or John A. Drennan at +1 202 626 9605.

King & Spalding is particularly well equipped to assist clients in the area of privacy and information security law. Our Privacy & Information Security Practice regularly advises clients regarding the myriad statutory and regulatory requirements businesses face when handling—either in gathering, managing, securing, transferring, sharing, selling or disposing of—personal and other sensitive information concerning individuals such as employees, consumers, customers, or patients, in the U.S. and globally. Collectively, the members of King & Spalding's Privacy & Information Security Practice have unparalleled experience in areas ranging from providing regulatory compliance advice, to responding to security incidents, interfacing with stakeholders and the government (both federal and state), engaging in complex civil litigation (such as class actions), handling state and federal government investigations and enforcement actions, and advocating on behalf of our clients before the highest levels of state and federal government.

* * *