LATHAM & WATKINS LLP

DISCUSSING THE TRENDS

Q&A with Jennifer C. Archie, Kevin C. Boyle & Vivian A. Maese

What General Counsel Need To Know About The Latest Cybersecurity Developments

February 26, 2015

In the wake of reported security breaches at a number of significant financial institutions, cybersecurity is garnering more attention and concern than ever before — both within the financial services industry and among public companies in general.

On October 20, 2014, the Securities Industry and Financial Markets Association (SIFMA) published Principles for Effective Cybersecurity Regulatory Guidance, which offers suggestions for government regulation of cybersecurity. In this Q&A interview, Latham & Watkins partners Jennifer Archie and Kevin Boyle, who specialize in data privacy and security, and Vivian Maese, who focuses on regulatory and compliance issues in the financial services industry, weigh in on this new guidance and other recent developments, offering general counsel advice on how they can keep their organizations ahead of the curve.

What is the significance of SIFMA's October 20, 2014 guidance?

Maese: First of all, the regulators of securities industry participants have not been as specific about cybersecurity ever before in any of their rulemaking. Prior to this time, the regulatory authorities have focused on privacy and identity theft, but cybersecurity was not articulated clearly by these regulators. What the SIFMA principles really do is bring to the forefront the importance of the interconnectedness of that securities ecosystem.

The guidance itself — when you sort of get down to what the Securities and Exchange Commission's (SEC) Office of Compliance Inspections and Examinations (OCIE) proposed back in April — what is really very clear is that they have a detailed category-by-category approach to telling us exactly what we need to do in terms of thinking about cybersecurity. It goes section by section, topic by topic — essentially creating the templates for thinking about it. However, what this guidance also indicates is that an off-the-shelf, borrowed from the internet information security policy is not sufficient for compliance. Information security polices going forward really do need to be customized and adapted to the particular institution and thought about in terms of that institution's processes. This very tailored, very custom and very intrusive approach is an important change for the industry. The message is that you've got to live it. You can't just take it off the shelf.

Boyle: The irony of this, coming from someone who has done cybersecurity for a long time, is that this has always been true. There are plenty of companies that have tried to get away with saying, "Just give me a 'standard' policy; we'll do a search and replace to make it ours, put it on the shelf for auditors to see, and the world will be fine." We have the world we do today in part because so many have taken that approach. You have to go through the painful process of identifying what information assets you have to protect, what you ought to be doing to protect them based on regulations and impact from a loss, what you are not doing, and how you are going to fix it. That process leads to a pragmatic security program. Shortcuts lead to breaches.

Archie: If you take a pan-industry approach, the best thinking on security builds on common risk analysis and mitigation approaches across individually regulated environments, which are then adapted to the context, be it banking or securities, consumer information — whatever the context is. The regulators themselves have learned that a templated, non-customized approach in internal corporate security programs is ineffective. The hard work of adapting common security management practices to a company's internal data and corporate structure is actually the most important step.

What are the financial regulators doing about cybersecurity right now? Where is the action?

Maese: Given the traditionally high level of technological sophistication of banks and other financial institutions, the fact that these institutions have been recent victims of bad actors is noteworthy. With this new environment comes new focus. The psychology of safeguarding the perimeter or the moat around the organization, which was the typical approach to cybersecurity that most financial institutions used, is no longer sufficient. I think that the experience of large financial institutions suffering breaches illustrates that the bad actors are becoming more and more sophisticated. Their technological tools are leaps and bounds ahead of where they were when they used to just sort of knock on the door, or engage in phishing scams. Now it is hard for even a technologically sophisticated organization to keep the bad actors at bay.

I think the dynamic is further examination, but also you are seeing both the regulators and institutions acquiring more sophisticated tools. That is where the action is right now — just getting smarter and better about how to protect your organization. Coming directly out of Dodd Frank, with the focus on interconnectedness and risk, the word "interconnectedness" is used throughout the 2,000 pages of the Dodd Frank Act in the context of systemic risk. The systemic risk analysis implies an examination of outsourcing providers, and outsourcing provider needs to be read broadly, not the way we would think about outsourcing 10 years ago. It means almost any third party who has a network connection to you or has your data needs to be scrutinized as much as you need to be scrutinized. The interdependency created in the financial services ecosystem is a very, very high priority and high focus of regulators.

Archie: That scrutiny starts with aligning documentation and aligning risk in the commercial agreements. That creates a lot of hardship on the receiving side or for the party that is contracting with a financial institution. Multi-year agreements may sit on the shelf and need to be updated to align with new regulatory and risk management expectations. The intensified scrutiny of the banks themselves flows down to all the parties performing services for the bank. Banks lease space, banks lease servers, banks hire temporary workers — there is a big downstream impact.

Boyle: A real problem we are seeing is these vendor governance programs can become paper exercises. Companies need to do more than establish written polices and requirements for their vendors. They need to audit and enforce their security requirements on their vendors as well as their own company employees. It is the same peril that people face in thinking they can solve their security problems by filling out a form and putting it on the shelf and saying, "Yes, I have an information security program." You can't just engage in the exercise; you have to live the exercise.

Companies in the "critical infrastructure business" have a new regulator, the National Institute for Science and Technology (NIST). What do general counsel need to know about NIST's Cybersecurity Framework?

Maese: It is not necessarily obvious where the NIST guidance applies. Financial services is very broadly defined, so you could be a credit card company or even a company taking credit cards and potentially come under the guidance. What I think general counsel really need to know is that it is a voluntary framework. The best our current administration can do is a stop-gap measure because we haven't been able to actually enact any cybersecurity legislation. For several years we have been chasing up to it, so instead of being able to enact the legislation, the president signed an executive order. The principles outlined by NIST seem to think big — like government big — and ultimately they have to be right sized for organizations. So, general counsel need to figure out if the framework applies to their organization and then also become a voice in the formulation of what the principles and rules will be going forward. That is the most important thing to do so that the rules are right sized for companies and not government sized.

I do think this framework creates a standard of care. When we are searching for that standard of care, which we have been doing in the securities industry for some time, I think that, by default, it will be the way in which we think about the country's standard for cybersecurity on a case-by-case basis.

Archie: So if you are planning proactively, you have to be aware that this government-promoted framework may become the de facto standard of care in any dispute where a breach is blamed on weak security controls. What the right sized version is for any particular company, who knows? But it is something that you would not want to have said you didn't look at and you didn't consider in managing the risk for your company.

Boyle: The NIST standard is more about a process rather than specifying particular technical steps that you implement. It goes right back to the point made earlier that effective security won't result from a form exercise. It has to

be a meaningful evaluation and internal process where the company evaluates its unique mix of information assets and risks, develops a strategy to respond, and constantly repeats that process as the threat environment evolves.

Effective cyber defense often necessitates the use of cutting edge tools and techniques. Do these tools and techniques themselves ever raise compliance issues and legal challenges?

Boyle: This ties to Vivian's point that effective security has evolved beyond a moat around data. It is no longer sufficient just to protect the perimeter; one must monitor inside and look for evidence that someone is either trying to break in or has broken in. In order to do that, you often wind up using tools that can be fairly invasive from a privacy standpoint. The tools that one might use range from programs that simply analyze activity looking for indicators of breach — say unusual traffic volumes, log-in patterns, log lengths and so on — to tools that actually look at the content of everything that is traversing the network. This inherently involves scanning emails, text messages and databases with personal information. That activity all raises issues that vary by jurisdiction. If you are a global organization using these tools and consolidating the information across national borders to a security operations center (SOC), that raises still more issues. Using these tools represents a sea change in the approach to information security with significant privacy implications that are often overlooked.

The difficulty for large organizations is that the teams implementing the new tools are quite often in a different group than those responsible for assuring the organization's compliance with privacy rules and regulations around the world. It is a perfect role for a general counsel to step in and ask, "Have we thought about this on an across-the-board basis? Is everybody who ought to be talking, talking?" It is a very constructive role that the lawyers inside an organization can play.

You need not just security by design, but also privacy by design. It has to be an integrated design, so that as the information security tools are developed and deployed in a privacy-by-design mode. Quite often, at least right now, these tools are implemented in a panic mode after there has been a breach and without the opportunity to go and lay the compliance groundwork that is necessary to avoid privacy compliance problems. It helps a lot to think about the privacy issues in advance. Even if you are not going to deploy the tools right now in a defensive mode, you should anticipate the need to potentially use them in responding to a breach and lay the compliance groundwork.

How will these issues affect the general counsel function in the future?

Archie: Five years or so from now, general counsel ought to aspire to the level of literacy on security and technology challenges that they have on accounting. Most lawyers aren't trained as accountants, but corporate attorneys acquire sufficient fluency to follow and help decide and manage legal risks related to very complex accounting questions. I think that where focus is needed in the future is the development of technical expertise inside the legal function. We need lawyers who have the comfort and competence in technology issues so that they can advise at the highest level on hard questions of disclosure, liability and even compliance. We don't get trained in this at law school; teaching data security to lawyers is not customary or even available perhaps, but I think that is going to change. Cyber for lawyers, inventing that expertise — purchasing it outside if you need to — but having a fluent set of legal advisers inside or outside the company is essential.

Additionally, defining breach readiness specifically for your organization is also a top of mind issue today. Just as the technology function is expected to tailor to their particular setting and not be cut and paste, lawyers also cannot have a cut-and-paste approach to data breach response, they have to customize it to their own structure, operations and even internal politics. General counsel should also be testing written response plans in real-world, table-top exercises where they deal with realistic worst-case scenarios, specific to their business. What are your core assets? What is the most important thing that you have to protect? A lot of companies can't tell you that. They have a very flat network and they have a perimeter approach, so they really can't identify the "nuclear" secrets of their company. The number one thing, quite frankly, is to know the number one thing and then to rehearse for responding to attacks on the number one thing. Just as we expect the US Secret Service to have and rehearse a plan to protect the president and his family inside the White House from fence jumpers, you need to know what your version of a fence jumper is and plan and rehearse for that. What is your version of material loss?

For More Information

Read "The General Counsel's Role Before and After a Data Breach Incident," an interview with Latham partners

Jennifer Archie, Gail Crawford and David Schindler.

CONTACTS

Jennifer C. Archie
Washington D.C.
T +1.202.637.2205
jennifer.archie@lw.com

Kevin C. Boyle
Washington D.C.
T +1.202.637.2245
kevin.boyle@lw.com

Vivian A. Maese
New York
T +1.212.906.1302
vivian.maese@lw.com

You Might Also Be Interested In

Data Privacy, Security & Cybercrime

Financial Regulatory