The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 3, Number 8 April 19, 2017

LAW FIRMS

What In-House and Outside Counsel Need to Know About ACC's First Model Cybersecurity Practices for Law Firms

By Jill Abitbol

Law firms are often targeted by sophisticated criminals and state actors seeking the wealth of confidential data they maintain. The publicized breaches of major law firms last year served as a wake-up call for the legal industry, signaling the importance of having effective cybersecurity measures in place. On the heels of these breaches, on March 29, 2017, the Association of Corporate Counsel (ACC), which represents over 42,000 in-house counsel across 85 countries, released a set of model cybersecurity practices.

The ACC's "*Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information*" (Guidelines) are intended to help in-house counsel set expectations with respect to the data security practices of their outside counsel. The Guidelines "will serve as a benchmark for law firm cybersecurity practices," an ACC press release states.

Development of Guidelines in Response to In-House Counsel Concerns

Protecting corporate data has increasingly been a chief concern for in-house counsel. ACC's Chief Legal Officers 2017 Survey found that two-thirds of in-house legal leaders ranked data protection and information privacy as "very" or "extremely" important. In response to this growing concern, the ACC released the "first-of-its-kind" Guidelines to help "in-house counsel as they set expectations with their outside vendors, including outside counsel."

The Guidelines were developed in a joint effort between in-house counsel members of the ACC and several law firms specialized in data security related issues, demonstrating the importance of cohesion between in-house and outside counsel when handling sensitive corporate data.

"I'm thrilled at the prospect of some industry norm and standard across the board," Justin Hectus, CIO and CISO of Keesal, Young and Logan, told The Cybersecurity Law Report. He noted, however, that "there will be a real dividing line at some point, to the extent that it doesn't already exist, between firms that are willing to commit to excelling in all of these areas and firms that are either not able to or won't commit to it." Most mid-sized to larger firms "would hopefully tell you that they have most of these security measures in place already," he added.

Standard or Starting Point?

These Guidelines should be viewed as "a starting point," Hectus suggested, adding that it is "difficult to propose a one-size-fits-all set of minimum cybersecurity standards." Not all data is treated equally, he pointed out. Thus, "tailoring access and controls based on the sensitivity of the data is a critical component" of cybersecurity.

Keeping Within the Spirit of the Guidelines

The applicability of some of the Guidelines' recommendations will depend on the circumstances and the size of the firm. "There are certain aspects of the Guidelines that I might want to push back on with a client. The key there is that you just need to explain to the client why any gap is not putting them or their data at risk and that you have reasonable compensating controls that ensure that you're living within the spirit of the document, if not the letter of the document." Thus, the Guidelines serve as the basis for "where the conversation needs to start, but not necessarily where it ends."

Hectus clarified that he does not believe "everything is negotiable, at least in a substantial fashion. These are incredibly challenging times, where the bad guys have the advantage. They only have to get it right once, and we have to get it right every time, in order to keep our data and our clients' data secure." Given this challenge, "it would be short-sighted to say that you don't need to have really comprehensive controls in place in order to manage cyber risk," he added.

Wording Like a Contract

The Guidelines are worded to sound like contract terms, although they indicate in the introduction that the "document is not intended to establish any industry standards for any purpose for either the company client or the outside vendor, including, but not limited to, contract, professional malpractice, or negligence." Finding the wording "interesting," Hectus said that he considers it "a baseline that legal departments may consider requiring," and "a streamlined and consistent approach to setting expectations." Additionally, with the language worded this way, it could serve as a "draft contract or a good start for a model contract."

The Guidelines' 13 Information Protection and Security Controls

The Guidelines address a broad range of data-security-related measures including: data breach reporting, data handling and encryption, physical security, employee background screening, information retention/return/destruction, and cyber liability insurance. While certain measures may be too burdensome under the circumstances, they include a number of measures firms will need to consider carefully.

1) Policies and Procedures

The Guidelines recommend that outside counsel have appropriate organizational and technical measures in place to protect confidential information of the company it represents (Company Confidential Information, defined in the Guidelines as "any information that is proprietary to Company and is not publicly available"). This includes having a number of listed security and privacy policies and procedures in place, such as physical and environment security policies, personnel training and incident response and problem management procedures, which are reviewed annually. Outside counsel should also have adequate resources and management oversight to ensure proper development and maintenance of these policies.

2) Data Retention

The Guidelines provide that outside counsel shall only retain Company Confidential Information for as long as necessary to satisfy the purposes for which it was provided unless applicable law requires otherwise. This provision also sets forth specific types of data and circumstances that are excluded from the requirement, such as day-to-day email exchanges and latent data such as deleted files and other non-logical data types.

Noting these exclusions, Hectus said this requirement was "well articulated" and that it is the first time he has seen a document return and destruction policy put together this well.

3) Data Handling: Encryption and Breach Reporting

It is "highly recommended" by the Guidelines that outside counsel encrypt all Company Confidential Information that resides on outside counsel's systems, servers, backup tapes, etc., including information on the servers of third parties with which outside counsel has contracted. The Guidelines also provide suggestions for encryption in transit, encryption of data stored on portable devices or transmitted over non-secure communication channels, and encryption of Company Confidential Information transferrable to removable media and mobile devices, specifically recommending that "two-factor authentication should be employed for remote connectivity using a mobile device, tablet or laptop."

Smaller and newer firms may have "an easier time" with the Guidelines' encryption requirements because there are "readily available software-as-a-service solutions that handle encryption," Hectus predicted. Larger and more established firms, on the other hand, may "have trouble pivoting" to adopt new technologies to meet these requirements. He noted, for example, that his firm's previous document management system made it "really difficult to implement encryption at rest without performance issues. That was an impetus for it to switch to a new document management system last year."

The Guidelines also recommend outside counsel to report any data security breach that potentially involves Company Confidential Information to the company within "24 hours of discovering an actual or suspected event."

"Twenty-four hours is a super tight response time," Hectus opined, adding, "this is a requirement where, if somebody wanted to push back and clarify the language, it would make sense." He believes the 24-hour timeframe is intended to prompt a conversation about what monitoring tools or alerts firms need to have in place to be made aware of a compromise.

4) Physical Security

The Guidelines also recommend several physical security protections for law firms that host Company Confidential Information on their systems and servers such as, "at least," picture ID badges, camera surveillance and a perimeter intruder alarm.

5) Logical Access Controls

The Guidelines recommend outside counsel be required to have logical access controls, such as defined authority levels and job functions, unique IDs and passwords and two-factor or stronger authentication for employee remote access, to manage access to Company Confidential Information.

6) Monitoring

Outside counsel should be expected to monitor its networks, employees, subcontractors and contingent workers for malicious activity that can affect Company Confidential Information.

7) Vulnerability Controls and Risk Assessment

This section recommends that outside counsel conduct vulnerability tests, including annual penetration testing, and assessments of any system that contains Company Confidential Information. It also recommends that outside counsel be required to have software controls in place to eliminate and minimize the introduction of security vulnerabilities.

"Everything in this section, including intrusion protection and prevention and methodical and timely patching, amounts to a good road map for cyber hygiene," Hectus said. While it would seem that something like "patching" is a common practice among firms, when they get breached, it is "most commonly a result of unpatched systems, poor password procedures or carelessness – simple stuff," he said, adding that "there are readily available tools and services out there that help you accomplish the recommendations listed in this section." While it used to be "that you had to have a big infrastructure and staff in order to run these solutions, there are a lot of solutions on the market today that scale pricing in favor of smaller companies."

8) System Administration and Network Security

The Guidelines suggest outside counsel should be required to have operational procedures and controls to ensure its systems are configured and maintained according to certain industry standards such as ISO and NIST. Outside counsel should also have antivirus protection installed, updated malware and threat detection, and network security controls including the use of firewalls, layered DMZs and updated intrusion-detection and -prevention systems.

9) Security-Review Rights

This section suggests that companies review and inspect outside counsel's systems and policies and procedures that affect Company Confidential Information.

10) Industry Certification/Additional Security Requirements

It is "recommended but optional" that outside counsel achieve ISO27001 certification. The Guidelines state that these certifications "reduce the time and effort required by in-house IT security departments to perform security assessments on third parties in possession of Company Confidential Information."

The optional ISO recommendation is interesting, Hectus explained. When having this "conversation with auditors, I always ask, 'If we had this type of certification, would this process of kicking the tires go away? Essentially, would that investment of time and money save us time and money on the audit side?' The answer is always, 'No, we would still come in and do the audit.'"

Thus, while Hectus believes ISO certification is "a worthwhile process to go through, it's not for everybody. And I appreciate the way that they treated it in the Guidelines," he added.

11) Background Screening

Outside counsel should be required to screen employees, subcontractors and contractors and certify annually to the company that these individuals have passed screening requirements.

12) Cyber Liability Insurance

The Guidelines recommend that outside counsel should be required to obtain and maintain cyber liability insurance with a minimum coverage level of $10 million. The $10 million minimum "is more significant than I have seen with any client," Hectus said, explaining that his firm only has "a few clients that mandate cyber insurance coverage and I believe the highest minimum that has been set is $5 million." He said that he "would be surprised if most firms have $10 million in cyber insurance."

Recommended minimum aside, the "benefits of having cyber insurance in place actually go beyond just transferring the risk," Hectus advised. He believes "the process of procuring cyber insurance is a helpful add-on to this type of evaluation because you have to go through a cybersecurity readiness audit in order to get a good premium and you have to ensure that you're accurately representing your controls to your carrier, so that you have coverage when you need it." Additionally, cyber insurance companies "have great resources available to you, not just post-breach, but also in in terms of incident response readiness."

See also "*Building a Strong Cyber Insurance Policy to Weather the Potential Storm (Part One of Two)*" (Nov. 25, 2015); *Part Two* (Dec. 9, 2015).

13) Subcontractors

The Guidelines state that outside counsel should be held responsible for all subcontractors they use that have access to Company Confidential Information. Companies should have a written agreement with those subcontractors that imposes the Guidelines on them.

Hectus finds it helpful that the Guidelines identified examples of subcontractors because conversations about security controls often focus on cybersecurity and, in that context, a third party might be a cloud provider, but firms might not be readily thinking about including the "copy vendor or offsite storage vendor."