PROTECTING DATA SECURITY RISK ASSESSMENTS FROM DISCLOSURE IN SUBSEQUENT BREACH LITIGATION

Karen Painter Randall and Steven A. Kroll Connell Foley LLP

In light of the rise on cybercrimes, many corporate clients are now demanding that businesses, including law firms, expressly state in their Request for Proposal (RFP) what data security programs they have in place before retaining their services. For example, it has been reported that J.P. Morgan Chase & Co., Morgan Stanley, Bank of America Corp., and UBS AG are just a few of the larger financial institutions that have subjected outside law firms to greater scrutiny regarding their cybersecurity. This includes law firms completing 60-page questionnaires about their threat detection and network security systems, as well as some vendors sending their own security auditors into firms for interviews and inspections. Similarly, corporations are being proactive and performing their own internal risk assessments in order to understand and identify their cybersecurity risk in relation to organizational operations, organizational assets, and individuals. Furthermore, an increasing number of organizations are bound by governmental regulations that dictate what security measures you should have in place and how they should be audited. HIPAA, PCI, FISMA, Sarbanes-Oxley, and Gramm-Leach-Bliley all dictate how to secure different types of data and the systems that manage it, and also require regular security posture assessments, though they vary on specific requirements and time frames.

CLIENTS DEMANDING STRONGER CYBERSECURITY FROM LAW FIRMS

The increase in cybersecurity risk assessments is the result of the strong push from clients causing organizations, such as law firms, to be more proactive regarding the implementation of cybersecurity protocol. For example, the European Union's General Data Protection Regulation, which goes into effect in May 2018, will require law firms based in the EU and those with EU clients to disclose data breaches to clients. TruShield, an IT security company, reported in 2015 that the legal industry was the second most targeted sector for a cyberattack. Even more alarming, the 2016 report revealed that small law firms were now the most targeted. As vendors, law firms are attractive targets. They not only hold valuable client information, but also are regularly emailing attachments to clients, providing a possible means to infect client systems. Moreover, law firms are viewed as high-value targets for the rapidly growing use of ransomware and extortion schemes because they have historically weak defenses and are seen as able to pay large ransom sums. Accordingly, it is no surprise that compliant clients are demanding that law firms also protect the sensitive and confidential data entrusted to them by the client. Requests are now made

to complete extensive questionnaires about threat detection and network security systems, as well as some sending their own security auditors into firms for interviews and inspections.

WHAT IS A CYBERSECURITY RISK ASSESSMENT?

In the context of cyber risks, an internal risk assessment requires companies to do the following tasks: (1) provide network vulnerability assessments; (2) provide recommendations to remediate potential vulnerabilities; (3) review its cyber policies and procedures; and (4) review its internal network. Whether an organization that suffers a data security breach may claim attorney-client privilege and/or work product protection in connection with these documents and communications is often disputed. For example, if a company performs an internal risk assessment that identifies areas of vulnerability and concern, but fails to remedy the problem, this would clearly provide sufficient evidence of notice to establish a claim for negligence against the company. Conversely, if an internal risk assessment reaches a conclusion that a company's internal network is safe and secure, yet then is subsequently breached by a hacker, this could also be used against the company in litigation, as any statement made within an RFP or internal risk assessment can be used against the enterprise making such representations.

This is not to say that organizations should never implement such risk assessments as they are often required by other companies on the condition of retention, as well as per applicable regulations. Moreover, a risk assessment can serve as a valuable tool to a company in identifying and remedying potential vulnerabilities, as well as a defense or mitigating factor to a potential lawsuit. As a result, in-house and/or outside counsel must be cognizant of the best way to execute these types of internal risk assessment documents in order to solidify a company's claim to privilege.

PROTECTING AN INTERNAL RISK ASSESSMENT

When a written risk assessment report has been prepared by a non-lawyer, the potential protections from discovery in later data breach litigation are limited, as organizations will not be able to rely on traditional discovery protections such as trade secret or work product for such documents. One potentially applicable protection is the "self-critical analysis" privilege, which protects from disclosure analyses of a company's own safety procedures. In New Jersey, in order to raise the self-critical analysis privilege a company must show that: (1) the information that is the subject of a production request must be the criticisms or evaluations or the product of an evaluation or critique conducted by the party opposing the production request; (2) the "public need for confidentiality" of such analysis must be such that the unfettered internal availability of such information should be encouraged as a matter of public policy; and (3) the analysis or evaluation must be of the character that would result in the termination of such self-evaluative inquiries or critical input in future situations if this information is subject to disclosure.[1] Because of the lack of case law on the use of the self-critical analysis privilege in the context of a data security risk assessment, it is unclear if it would meet the aforementioned requisites.

Alternatively, an organization can attempt to protect an internal risk assessment from disclosure by employing outside counsel to manage the review process. Under this circumstance, outside counsel would be retained by the organization to provide legal advice regarding data security exposures, and to develop a strategy for risk minimization. As part of this process, outside counsel, rather than the organization, would retain an independent cyber consultant to assist in the due diligence analysis and in the preparation of a cyber risk assessment report detailing the organization's vulnerabilities, threats and lack of controls, as well as recommendations for addressing these issues. The report would be prepared at the request of counsel, which would then be incorporated into a more comprehensive report for the organization. Accordingly, a company would be in a position to assert that the report, including the results of the internal risk assessment, is protected by the attorney-client privilege. Moreover, the outside consultant's role would also be clearly defined to assist and in furtherance of counsel in preparing its own legal analysis.

Furthermore, organizations must be counseled to take sufficient precautions to maintain the confidentiality of the final report so as to prevent waiver of the attorney-client privilege. In a traditional attorney-client relationship, where the client is a single person, it is easy to determine whose privilege it is to waive. However, in the context of a corporation, which may include a board of directors, shareholders, and thousands of employees communicating with general counsel, this becomes a much harder question to answer. In general, when a member of a company is soliciting legal advice from counsel, an attorney-client relationship will be deemed to be formed. Furthermore, the authority to waive the attorney-client privilege, in the corporate context, does not belong to each and every employee of the corporation, but rather its officers and directors. Therefore, when preparing an RFP and/or internal risk assessment, a corporation's general counsel should be clear that it is being prepared to solicit legal advice, as well as who is responsible for managing and controlling the creation of these documents to protect against an inadvertent disclosure.

CONCLUSION

In sum, it is advisable that companies work through internal and/or outside counsel when preparing these data security risk assessments so that the information obtained may be protected under attorney-client privilege. Moreover, a comprehensive legal strategy for developing a data security risk assessment offers a more realistic opportunity for an organization being able to shield the final product from discovery in subsequent data breach litigation than merely relying on non-attorney client protections.

Karen Painter Randall is a Complex Litigation Partner with Connell Foley LLP in Roseland, N.J., and chair of the firm's Cybersecurity and Data Privacy and Professional Liability Practice Groups. She provides representation and advocacy services to professionals and businesses in a wide variety of complex litigation matters and is a veteran trial attorney in state and federal courts. Ms. Randall, vice chair of USLAW's Data Privacy & Security Practice Group and a former chair of USLAW's Professional Liability Group, is designated a Certified Civil Trial Attorney by the Supreme Court of New Jersey.

Steven A. Kroll is an Associate with Connell Foley LLP in Roseland, NJ. He is a member of the firm's Cybersecurity and Data Privacy Practice Group. In addition to representing professionals in various areas, Mr. Kroll concentrates his practice in the areas of professional liability and employment law matters in both New Jersey and New York. Mr. Kroll received his J.D. from Rutgers-Newark School of Law in 2009, cum laude, *and received the distinguished award of Order of the*

[1] *Wylie v. Mills*, 195 *N.J. Super.* 332, 339 (Law Div. 1984).