Risk Assessment Landmines in Data Security Breach Litigation

by Karen Painter Randall and Steven A. Kroll

In the wake of large-scale data breaches impacting every industry, businesses and even government agencies have been making significant strides to protect the confidential and personal information of clients and employees. While many industries have devoted a significant amount of time and money to ensure that sufficient policies and procedures are implemented to protect against a cyber attack, other smaller businesses often dedicate less resources or simply lack awareness of the latest cybercrime trends.

In light of the uptick in cyber attacks, 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 mandate what security measures should be in place and how they should be audited. Health Insurance Portability and Accountability Act (HIPAA),[1] Payment Card Industry Data Security Standard (PCI DSS), Federal Information Security Management Act (FISMA), Sarbanes-Oxley Act of 2002 (SOX),[2] and Gramm–Leach–Bliley Act (GLBA)[3] 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 timeframes. However, the issue that arises regarding the creation of an internal risk assessment is its discoverability in subsequent litigation and whether the information contained within these reports is protected by the attorney-client privilege and work product doctrine.

In the context of cyber risk, an internal risk assessment requires companies to perform the following tasks: 1) conduct network vulnerability assessments; 2) provide ecommendations to remediate potential vulnerabilities; 3) review cybersecurity policies and procedures; and 4) review its internal network. Whether companies that suffer data security breaches 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 supports the conclusion that a company's internal network is safe and secure, yet it is then subsequently breached by a hacker, this assessment could also be used against the company in litigation. For example, in *In re Zappos.com, Inc., Customer Data Security Breach Litigation*,[4] Zappos' company website allegedly declared that "…shopping on Zappos.com is safe and secure—guaranteed." Following a data breach, the plaintiff consumers used this statement as a basis to overcome a motion to dismiss based upon a theory of negligent representation.

Similarly, any statement made within an internal risk assessment regarding areas of concern, or the safety and secureness of a company's internal network, could be used against the enterprise making such representations.

This is not to say an organization should never implement such risk assessments, as they are often required by other com-

panies in order to do business, as well as by applicable regulations. Moreover, a risk assessment can serve as a valuable risk management tool to a company in identifying and remedying potential vulnerabilities, as well as a defense or mitigating factor to a potential lawsuit. Performing risk assessments can also help ensure best practices. As a result, in-house and/or outside counsel must be cognizant of the acceptable way to conduct and document risk assessments in order to solidify a company's claim to privilege.

When a written risk assessment report has been prepared by a non-lawyer, the potential protections from discovery 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 the information is subject to disclosure.[5] 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 whether the privilege would be found to apply.

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 is retained by the organization to provide legal advice regarding data security vulnerabilities, and to develop a strategy for risk minimization. As part of this process, outside counsel, rather than the organization, would retain an independent cybersecurity consultant to assist in the due diligence analysis and in the preparation of a cyber risk assessment report, which may detail the organization's vulnerabilities, threats and lack of controls, as well as recommendations for addressing these issues. The consultant 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 cyber risk assessment, is protected by the attorney-client privilege. Moreover, the outside consultant's role would also be clearly defined as assisting counsel in preparing a legal analysis for the organization, thereby protecting against the disclosure of the communications to any third party.

Furthermore, organizations must be counseled to take sufficient precautions to maintain the confidentiality of the final report to prevent a 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, whose privilege it is to waive becomes a much harder question to answer.

The general rule is that when an officer or director 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 and maintaining an internal risk assessment, the corporation's general counsel should be clear on who is entitled to have access to and review the document to protect against an inadvertent disclosure.

A recent decision in litigation over the data security breach suffered by Target Corp. sheds important light on the scope of such protections. In *In re Target Corp. Customer Data Sec. Breach Litig.*,[6] the court found that Target submitted several declarations and exhibits to substantiate the company's privilege and work product claims regarding its response program. Following the large-scale cyber attack on Target, a two-track response program was created. The first track involved a team of forensic experts who were engaged on behalf of several credit card brands, and the second track was created to assist counsel in conducting an investigation of the data breach to enable them to provide legal advice to Target.

During discovery, Target produced all communications with forensic experts from the first track, but withheld communications and work product prepared by the Data Breach Task Force and experts engaged by counsel as part of the second track. In denying the plaintiffs' motion to compel the production of discovery from Target, the court held that the work of the second track was focused not on remediation of the breach, as the plaintiffs contended, but on informing Target's in-house and outside counsel about the breach so Target's attorneys could provide the company with legal advice and prepare to defend the company in litigation. Moreover, the plaintiffs could not overcome Target's work product protection because Target had already produced documents and other tangible things, including

forensic images, from which the plaintiffs could learn how the data breach occurred and about Target's response to the breach.

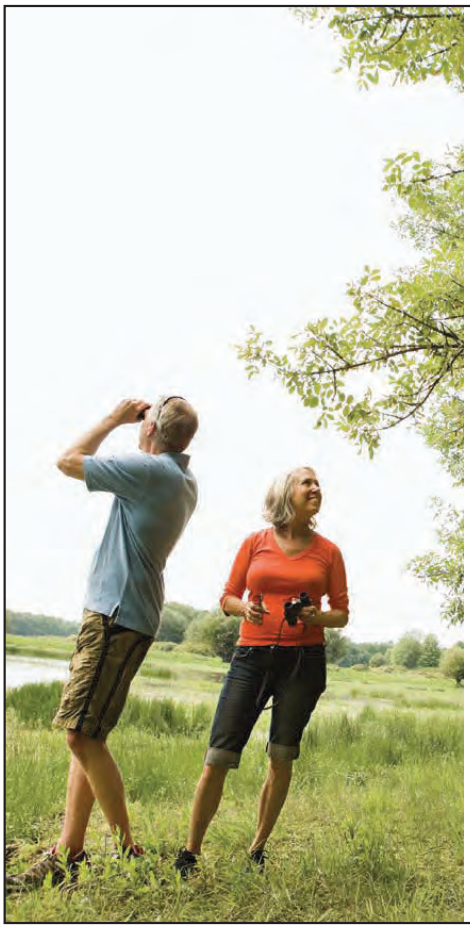
While this opinion relates to internal investigations following a data breach, the same principles can be applied to the preparation of an internal risk assessment. Namely, these assessments should be prepared at the request of the counsel to provide legal advice to a company, and to help defend against the threat of litigation should a data breach occur.

In sum, when preparing cyber risk assessments, it is advisable that businesses work through internal and/or outside counsel so the sensitive information obtained may be protected by the attorney-client privilege and work product doctrine. Moreover, applying a comprehensive legal strategy while developing a data security risk assessment will help preserve the attorney-client privilege and shield the final product from discovery in subsequent data breach litigation. ⚖

Karen Painter Randall, *a certified civil trial attorney and complex litigation partner with Connell Foley LLP in Roseland, is founder and chair of the firm's cybersecurity and data privacy practice group. A member of the International Association of Privacy Professionals, she counsels clients, including law firms, on the data protection and regulatory compliance laws tailored to the enterprise and develops proactive plans to reduce the risk of a cyber attack.* ***Steven A. Kroll*** *is an associate with Connell Foley LLP in Roseland. In addition to representing professionals in various areas, he concentrates his practice in the areas of professional liability, cyber liability, general insurance litigation and employment law handling matters in both New Jersey and New York.*

ENDNOTES

1. Health Insurance Portability and Accountability Act of 1996, 1996 Enacted H.R. 3103, 104 Enacted H.R. 3103, 110 Stat. 1936.
2. Sarbanes-Oxley Act of 2002, 107 P.L. 204, 116 Stat. 745.
3. Gramm–Leach–Bliley Act, 15 U.S.C.S. § 6801 *et seq*.
4. *In re Zappos.com, Inc*., Civil Action No. 12-cv-00325 (RCJ-VPC), 2016 WL 2637810 (D. Nev. May 6, 2016), *reconsideration denied sub nom. Zappos.com, Inc.*, Civil Action No. 12-cv-00325 (RCJ-VPC), 2016 WL 4521681 (D. Nev. Aug. 29, 2016).
5. *Wylie v. Mills*, 195 N.J. Super. 332, 339 (Law Div. 1984).
6. *In re Target Corp. Customer Data Sec. Breach Litig*., MDL No. 14-2522 (PAM/JJK), 2015 WL 6777384 (D. Minn. Oct. 23, 2015).



Gregory Roberts
Chartered Retirement Planning Counselor
First Vice President
Wealth Advisor

1200 Lenox Dr., Ste. 300
Lawrenceville, NJ 08648
609-844-7911
patricia.l.dintino@morganstanley.com

When you retire, your money should keep working.

Someday you'll stop working, and at that point, you'll have to depend on your retirement income. To work toward building that income, you'll need a strategy.

With more than 28 years of experience,I can help you create a strategy for goals like retirement, estate planning and leaving a legacy. Let's put your money to work. Call me today to set up an appointment.

Morgan Stanley

Morgan Stanley Smith Barney LLC, its affiliates and Morgan Stanley Financial Advisors do not provide tax or legal advice. Clients should consult their tax advisor for matters involving taxation and tax planning and their attorney for matters involving trust and estate planning and other legal matters.

© 2013 Morgan Stanley Smith Barney LLC. Member SIPC. CRC588469 (12/12) CS 7338805 MAR013A 03/13