Bloomberg BNA

BNA's
Corporate Counsel Weekly™

BNA Insights

Use Outside Counsel to Control Data Breach Loss

BY RICHARD M. MARTINEZ, SETH A. NORTHROP AND BENJAMEN C. LINDEN

One of the first people a distraught chief information officer or chief executive officer will call when a company's data security has been breached is the general counsel. But who should that general counsel call? The first reaction might be to call an outside auditing or security firm, or the organization's own technical experts, for an immediate analysis of the problem and risk to the corporation. However, there are very good reasons why that first call ought to go to outside counsel.

Naturally, prevention and remediation take priority. But outside counsel can play a unique and critical role in responding to a security breach, and that involvement can have profound implications when litigation inevitably occurs. Outside counsel can provide expertise to navigate the complexity of corporate and governmental compliance. And involving outside counsel early on may provide a shield against later discovery of materials related to the organization's internal investigation and remediation efforts.

It's Not the Time for a Misstep

An organization facing a data breach will find itself placed under a microscope by the public, business partners, governmental agencies and even legislative bodies.[1] The organization will be frantically working to investigate the breach, mitigate the effects, and plan and execute a public communication plan.

As the organization works the logistics of the breach, it often will face a dizzying set of contractual and regulatory obligations. Even the most sophisticated in-house legal departments will struggle to spot each of these issues while attempting to minimize corporate risk after the breach.

The timing of a corporation's engagement of outside counsel can have a profound impact on controlling disclosure of the post-breach turmoil and investigation communications.

Moreover, corporations experiencing a data breach face a multitude of differing state requirements for responding to the breach. For example, many states—such as Delaware, New Jersey and Pennsylvania—require companies to notify affected individuals of a breach only where there is some risk of harm to consumers. Other states—including California, New York and Minnesota—require disclosure independent of a "risk of harm" analysis.

Further, many states not only require notification to consumers impacted by the breach, but also to

[1] *See, e.g.*, Heidi Przybyla, *Congress Democrats Seek Hearings on Target Data Breach*, BLOOMBERG NEWS, Jan. 14, 2014; *see also* Elizabeth A. Harris, Nicole Perlroth & Nathaniel Popper, *Neiman Marcus Data Breach Worse Than First Said*, N.Y. TIMES, Jan. 23, 2013.

Richard Martinez is a trial attorney at Robins, Kaplan, Miller & Ciresi LLP, Minneapolis. His practice focuses substantially on technology, primarily in the areas of intellectual property litigation, cybersecurity and data privacy. His practice is also active in matters before the International Trade Commission. Contact him at rmmartinez@rkmc.com. Seth Northrop is a trial attorney, and former entrepreneur, at the firm. His practice focuses on intellectual property and global business and technology sourcing. He has substantial experience with complex business litigation disputes involving various technologies, including software and hardware design, analytics, networking, database and e-commerce systems. Contact him at sanorthrop@rkmc.com. Benjamen Linden is an associate at the firm, practicing in intellectual property litigation. Contact him at bclinden@rkmc.com.

 ISSN 0886-0475

various state agencies. In addition, although there are no current federal statutory equivalents,[2] various federal agencies like the Federal Trade Commission also may require some form of reporting.

Governmental regulations, however, are not the only obligations that in-house counsel should worry about satisfying. Corporations also may have reporting or auditing obligations arising from their contractual agreements with vendors, customers or other third parties, as well as compliance demands, such as those found in the Payment Card Industry Data Security Standards.[3]

Engaging outside counsel will immediately put expertise in the hands of a general counsel suddenly charged with crisis management. This knowledge will help craft a well-defined response plan that incorporates the applicable statutory, regulatory and contractual requirements the organization faces.

Seeking Cover in Litigation

Litigation almost certainly will follow a significant data breach. In fact, as courts and agencies like the FTC and the Securities and Exchange Commission develop an ever-growing body of data breach law, the number of post-breach lawsuits have increased.[4] Within just days of the data breach at Target, dozens of lawsuits had been filed in state and federal court.[5]

The timing of a corporation's engagement of outside counsel can have a profound impact on controlling disclosure of the post-breach turmoil and investigation communications. These communications, if disclosed out of context, may not accurately portray the breach's cause or impact. Such revelations may unnecessarily damage the organization and negatively impact future litigation.

Engaging outside counsel early may allow the organization to protect certain elements of its investigation and analysis pursuant to the attorney-client privilege or work product doctrine. This may provide the organization greater flexibility to uncover the root cause of the breach while limiting its potential litigation risk. Additionally, engaging outside counsel may help avoid the careless creation of documents that others might exploit later in litigation.

Attorney-Client Privilege

In general, the attorney-client privilege protects the communication or solicitation of legal services between an attorney and client. This protection extends to communications between in-house counsel and some members of a corporation.[6] Because the privilege only attaches if the communication is made to one acting as the client's attorney (or the attorney's representatives) and only when the communication is in solicitation of legal advice, problems may occur where in-house counsel wears various hats. For instance, if in-house counsel is regularly involved in giving business or technical advice, rather than strictly legal advice, courts are less likely to view his or her communications as privileged. On the extreme side, advice from an in-house lawyer working on the business or management side may be *presumptively* unprivileged.[7]

In-house counsel thus should be extra mindful of their role not only within the corporation, but also when working with outside accounting or contracting firms. For example, even communication of ''legal advice'' between in-house counsel and third-party auditors might not be privileged if it is unclear whether in-house counsel is acting as the contractor's attorney.

In the case of *In re FTC*, in-house counsel advised a corporation's outside advertising agency numerous times on legal issues related to the drafting of advertising materials. The court nonetheless found that counsel was not acting as the advertising agency's attorney and thus the communications were not privileged.[8] Similar concerns arise when communications involve IT staff and outside technical consultants engaged to identify and remedy a data breach.

Even communication of ''legal advice'' between in-house counsel and third-party auditors might not be privileged if it is unclear whether in-house counsel is acting as the contractor's attorney.

By contrast, outside counsel's retention of technical experts or contractors may extend the attorney-client privilege to communications between the contractors and the organization. For example, if outside counsel retained the contractor for the purposes of rendering legal advice, privilege may attach.[9] Thus, whereas in-house counsel's role inside the organization as both a business and legal advisor may compromise certain communications with third-party contractors related to a data breach investigation, the retention of those same contractors by outside counsel, at least for the purposes of rendering legal advice, likely will keep investigatory findings privileged.

Work Product Doctrine

The work product doctrine may be an additional means to shield findings from a post-breach investigation during subsequent litigation.

Whereas the attorney-client privilege applies only to communications, work product applies broadly to ''documents and tangible things that are prepared in anticipation of litigation or for trial by or for another party or its representative (including the other party's attorney, consultant,

[2] On Jan. 8, 2014, in the wake of the Target breach, Senator Patrick Leahy (D-Vt.) introduced the Personal Data Privacy and Security Act (S. 1897). The bill enhances criminal penalties for data theft and empowers the Federal Trade Commission, and in some cases the U.S. Department of Justice, to enforce data security and breach notification requirements.

[3] The Payment Card Industry (PCI) Data Security Standards provide technical and operational requirements and apply to merchants and companies that store, process and/or transmit cardholder data. The major payment card brands enforce the requirements. PCI SECURITY STANDARDS COUNCIL, *At a Glance Standards Overview* (2008) *available at* https://www.pcisecuritystandards.org/pdfs/pcissc_overview.pdf.

[4] Sasha Romanosky, David A. Hoffman & Alessandro Acquisti, *Empirical Analysis of Data Breach Litigation*, __ J. EMPIRICAL LEGAL STUDIES __ (forthcoming), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1986461.

[5] Randy J. Maniloff, *Class-Action Lawyers Hope Target is a Bull's-Eye*, WALL ST. J., Jan. 2, 2014.

[6] *Ames v. Black Entm't Television*, 1998 U.S. Dist. LEXIS 18053, at *10 (N.D. Ill. Nov. 17, 1998).

[7] *Breneisen v. Motorola, Inc.*, No. 02 C 50509, 2003 U.S. Dist. LEXIS 11485, at *3 (N.D. Ill. July 3, 2003).

[8] *In re FTC*, 2001 U.S. Dist. LEXIS 5059, at *1, 3 (S.D.N.Y. Apr. 19, 2001).

[9] *United States v. Kovel*, 296 F.2d 918, 922 (2d Cir. 1961).

CCW ISSN 0886-0475

surety, indemnitor, insurer, or agent).''[10] Thus, when investigative documents in the aftermath of a breach are prepared primarily in anticipation of litigation, the doctrine might protect them. However, when documents appear to be the product of a routine investigation and were not prepared primarily in anticipation of litigation, courts are much less likely to protect the work product doctrine.[11]

One way of removing doubt of whether documents were indeed prepared in anticipation of suit is to involve outside counsel. For example, in the *In re Woolworth* case, outside counsel was called in to investigate allegations of accounting irregularities.[12] The resulting notes and report from outside counsel's investigations were sought in the ensuing litigation. The court refused to draw a bright line between what documents were created for a ''business purpose'' and which were in ''anticipation of litigation.'' In finding the corporation's investigation had a litigation-driven purpose, the court noted that ''[a]ll participants knew when Paul, Weiss became involved that litigation—civil, and possibly criminal—as well as regulatory action were virtually certainties.'' [13] Accordingly, where close calls of privilege are involved, the participation and direction of outside counsel may be enough to tip the scales, particularly when the investigation is conducted at the direction of and with oversight by outside counsel.

[10] Fed. R. Civ. P. 26(b)(3).

[11] *E.g.*, *Benton v. Brookfield Props. Corp.*, No. 02-Civ. 6862, 2003 BL 2433, at *2–3 (S.D.N.Y. July 23, 2003).

[12] *E.g.*, *In re Woolworth Corp. Sec. Class Action Litig.*, 1996 U.S. Dist. LEXIS 7773, at *5–8 (S.D.N.Y. June 6, 1996).

[13] *Id.* at *8–9.

Preserving Discoverable Materials

Once litigation becomes ''reasonably foreseeable,'' a party has a duty to preserve evidence. Thus, post-breach litigation need not be either certain nor imminent before destroying relevant documents—even if pursuant to existing document retention protocols—is sanctionable. As an example, in the recent case of *Apple v. Samsung Electronics Corp.*, Samsung was sanctioned in part for failing to suspend the automated 14-day deletion of e-mails in its e-mail system.[14] Accordingly, there will be immediate pressure on the victim of a data breach to quickly take steps to preserve discoverable materials.

There will be immediate pressure on the victim of a data breach to quickly take steps to preserve discoverable materials.

Engaging outside counsel rapidly will assist the organization in ensuring that processes are immediately put into place to preserve these discoverable materials. The organization likely will face some degree of chaos as it works to remedy a breach. This chaos can result in discoverable materials being lost, placing the organization at additional and unnecessary risk during subsequent litigation.

Outside counsel can provide immediate assistance in two specific areas: drafting and circulating adequate hold notices, and preserving existing documentation. The early drafting and circulation of a litigation hold notice is one way an organization responding to a data breach can help preserve relevant documents and minimize the risk of future sanctions.[15] To be effective, however, notices must be timely *and* provide practical guidance in the context of the breach.[16] For instance, the court in *Samsung Electronics Co. v. Rambus, Inc.* found that instructions to employees to ''look for things to keep'' and prohibiting the destruction of ''relevant documents'' failed to satisfy a party's discovery obligations.[17] Scope and cause in the immediate aftermath of a data breach may still be in doubt, but it is critical that a legal hold notice be implemented quickly and with as much specificity as possible.

Likewise, as the remediation of a breach occurs, critical documentation about the state of the environment could be lost. Outside counsel can work side-by-side with general counsel's efforts to control the crisis by putting systems in place to capture and preserve critical documentation not only for potential litigation, but for the organization's root-cause analysis of the breach.

Conclusion

Outside counsel can be an instrumental team member when it comes to dealing with any corporate crisis. This is particularly true when the crisis risks the loss of sensitive or personal data. Because such events require an exceptionally rapid and coordinated response, making the call to outside counsel right away can help to mitigate corporate risk following a security breach, while still allowing for protected attorney-client communications.

[14] *Apple v. Samsung Elecs. Corp.*, No. C 11-1846 LHK (PSG), 2012 BL 173601 (N.D. Cal. July 25, 2012).

[15] *E.g.*, *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 221 (S.D.N.Y. 2003).

[16] *Samsung Elecs. Co. v. Rambus, Inc.*, 439 F. Supp. 2d. 524, 565 (E.D. Va. 2006).

[17] *Id.*