Data Security Assessments: Are You Prepared For A Breach?

Main Contact(s)

William R. Covino

Related Practices

General Litigation

Health Care Litigation and Risk Management

Nursing Home/Assisted Living Litigation

Professional Liability Litigation

By William R. Covino on May 18, 2017

Will Covino's article on Cyber Risk to Lawyers which appears in the ABA/BNA publication Lawyer's Manual on Professional Conduct appears here. For the PDF version in the ABA/BNA publication click here.

Be prepared for a data breach. It is no longer a question of if, but when your law firm's cybersecurity will be compromised. Due to the wake of large-scale data breaches impacting nearly every industry, attorneys can no longer place their heads in the sand and ignore the ongoing changes in technology.

At the Spring 2017 National Legal Malpractice Conference, Karen Painter Randall, a Partner at Connell Foley, LLP, moderated a panel who addressed the continual need for lawyers to review and update their law firm's cybersecurity policies and procedures. The panel included Daniel Quinn, a Partner at Carr Maloney PC; Judy Selby, a Consulting Managing Director at BDO USA LLP; and Richard Sheinis, a Partner at Hall Booth Smith, PC.

The panelists provided a comprehensive and understandable presentation concerning how lawyers can obtain a competitive advantage in preparing for, and responding to, threats posed to cybersecurity. The panel's discussion focused on four topics: (1) why lawyers should be concerned with cybersecurity; (2) the ethical obligations of lawyers to understand cybersecurity; (3) the risks associated with public disclosures concerning cybersecurity; and (4) how internal data security risk assessments can help law firms prepare for inevitable data breaches.

Should Lawyers Be Concerned About Data Breaches?

Lawyers should be concerned about data breaches regardless of their age and regardless of whether they work in a small, medium, or large firm for the following three reasons:

1. Clients are expecting cybersecurity procedures in place to protect their confidential and personal information. Clients are more frequently sending detailed risk assessment questionnaires and teams of auditors to assess cybersecurity programs;

2. Law firms who have had their cybersecurity breached have lost clients and, in some cases, closed their doors for business within six months of the data breach; and

3. Data breaches are costly. The average cost for a data breach is $4 million dollars. Data breaches may also subject a lawyer to an ethical complaint or lawsuit; an investigation by regulatory authorities; or personal embarrassment.

Ethical Obligations Associated With Cybersecurity

Because lawyers are ethically required to preserve and protect the confidential and personal information of their clients, a necessary corollary to this proposition is that lawyers must have a competent understanding of the changes in cybersecurity to fulfill this duty.

To remind lawyers of this ongoing and continual obligation, the American Bar Association amended its

comments to Rules 1.1 and 1.6 of its Model Rules of Professional Conduct. These comments provide that for a lawyer to maintain the requisite knowledge and skill, "… a lawyer shall keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology…" and the "…unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation [of his or her confidentiality obligation]… if the lawyer has made reasonable efforts to prevent the access or the disclosure." As of March 1, 2015, these amendments have been adopted by 27 states in one form or another.

The panel discussed the meaning of "reasonable efforts" under the Model Rules of Professional Conduct. On one end of the spectrum, a solo practitioner would likely be deemed to not be using reasonable efforts if he or she used a computer from the 1990s without any firewall protection. On the other end of the spectrum, a large law firm would likely be deemed to be using reasonable efforts if they employed a full-time team of IT specialists to provide cybersecurity. Most law firms fall between these two extremes.

The panel recommended that lawyers should have an IT specialist to assist their law firm. The specialist should have access to the confidential information maintained by the law firm, the potential risks that someone may obtain unauthorized access to this confidential information, and the safeguards available to prevent unauthorized access to this confidential information.

Similarly, the panel advised, the law firm should consider having the IT specialist provide recurring updates to the law firm about changes in cybersecurity, as well as to hold security awareness trainings. These trainings would remind law firms of the importance of cybersecurity and instill in firm employees a constant awareness of the technological changes affecting the law firm's confidential information.

What You Say Can Be Used Against You

The panel's third topic focused on a growing issue in cybersecurity: lawsuits against companies based on public disclosure of data breaches. Companies must be mindful that the contents of a public disclosure made before or after a data breach may be used against the company in subsequent litigation.

For instance, the panel discussed two recent cases concerning advertisements made about the strength of a company's cybersecurity. In *In re Zappos.com, Inc., Customer Data Sec. Breach Litig.* , 3:12-cv-00325-RCJ-VPC, 2013 BL 239619, (D. Nev. Sept. 9, 2013), the Court denied a defendant's motion to dismiss on a negligent misrepresentation claim because the company's website advised shoppers that "shopping Zappos.com is safe and secure – guaranteed." In *In re Adobe Sys. Privacy Litig.*, 66 F. Supp. 3d 1197, 1221 (N.D. Cal. 2014), the Court denied Adobe's motion to dismiss because "Adobe maintains that its security measures were adequate and remain adequate," but Adobe had failed to comply with several standard industry practices.

Similarly, the panel discussed a recent case concerning a company's response to a data breach. In *Remijas v. Neiman Marcus Group, LLC* , 794 F.3d 688, 694 (7th Cir. 2011), the Seventh Circuit held that a company's decision to offer its customers a credit monitoring service (a relatively standard practice to obtain good will) served an admission that the customers faced an imminent risk of harm.

The lessons from these cases are clear: say what you mean and do what you say. Plaintiffs will use

guarantees regarding data security measures to support a claim of deception in subsequent data breach litigation. Such statements, if made, should be carefully drafted with the assistance of counsel and reviewed for accuracy. Likewise, lawyers should note, companies that offer credit monitoring services should include a statement to clarify the reason(s) for making the offer, to reduce the risk that a court will deem the offer as an improper admission.

Internal Risk Assessments – The Gold Standard of Due Diligence

The panel's final topic focused on internal risk assessments. In light of the significant increase in cyber-attacks, many corporate clients are now demanding that businesses include in their Requests for Proposals a statement of what data security programs they have in place or provide them with copies of internal risk assessments. An internal risk assessment has four components. It requires a company to provide a network vulnerability assessment, provide recommendations to remediate potential vulnerability, review its cyber policies and procedures, and review its internal network.

The benefits and dangers associated with internal risk assessments are obvious, and the assessments may not always be shielded from discovery. A detailed internal risk assessment may provide a plaintiff with all of the evidence he or she needs to establish a claim in subsequent litigation or may provide a company a defense or mitigating factor against such a lawsuit.

Attempts to prevent the disclosure of internal risk assessments have been met with mixed success. Companies may be able to withhold an internal risk assessment based on a self-critical analysis privilege, which in some jurisdictions will protect the disclosure of a company's analysis of its own safety procedures. A company may also be able to withhold an internal risk assessment based on the attorney-client privilege by employing outside counsel to manage its review process. 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.

A key takeaway from the panel's discussion is that discoverability of internal risk assessments is an extremely fact-sensitive inquiry. Companies should work through internal and/or outside counsel when preparing these cyber risk assessments so that the information obtained may be protected under the attorney-client privilege. Moreover, a comprehensive legal strategy for developing a data security risk assessment offers a more realistic opportunity for an organization to shield the final product from discovery.

To contact the editor on this story: S. Ethan Bowers.

Will Covino is an Associate at Peabody & Arnold LLP in Boston who focuses his practice on professional liability defense, cybersecurity, and general litigation matters.

