Data Breaches and the Role of the In-House Attorney

Brad Brian and Grant Davis-Denny
Munger, Tolles & Olson
355 South Grand Avenue, 35th Floor
Los Angeles, CA 90071-1560
213.683.9100
www.mto.com

Your company is undoubtedly under attack right now from hackers. A 2014 survey of 567 U.S. executives by the non-profit Ponemon Institute found that 60 percent of respondents' companies had suffered a known data breach in the last two years. Although Ponemon reports that the average data breach cost U.S. businesses close to $4 million, the consequences can be far more severe. Target's data breach has cost the company over $250 million.

Lawyers are naturally tempted to treat cyber security as an IT problem. This is a mistake. While most attorneys lack a computer science degree and don't feel comfortable discussing firewalls, lawyers can play a vital role in protecting against and responding to a data breach.

When a company finds itself joining the majority of businesses that have suffered a data breach, lawyers invariably will be critical members of the team addressing some or all of the following issues:

- The extent and nature of the confidential information that has been breached and a strategy for communicating with those whose data has been breached;
- Varying breach notification requirements that exist in virtually every U.S. state;
- Contract implications with third parties;
- Regulatory enforcement actions;
- Consumer and employee class actions;
- Insurance coverage;
- For public companies, their securities disclosure obligations;
- Business partner litigation (think credit card companies and issuer banks); and
- Shareholder litigation targeting directors and officers.

While these issues may require consultation with outside counsel who have expertise in data security, in-house counsel will play a key role in the aftermath of a data breach.

In-house counsel's role in data security should not just begin after the occurrence of a data breach. Lawyers can and should help their companies reduce the risk of a hack before it occurs.

In-house counsel have a vital role to play in making sure that their companies' data security standards at the very least meet legal requirements designed to protect against hacking. Company counsel should be actively engaged in designing cyber security policies and ensuring compliance with those policies with an eye toward evolving standards for security.

Unfortunately, determining what the law demands is no simple task. In the U.S., there is a patchwork of federal and state legal standards. At the federal level, these standards often apply only in certain sectors, such as HIPAA in the healthcare industry and Gramm-Leach-Bliley in the financial services industry. Massachusetts, however, has adopted cybersecurity requirements that apply broadly to all companies that collect information from that state's residents.

To appreciate the uncertainty companies face when it comes to figuring out the appropriate level of data security, consider the standard that the Federal Trade Commission (FTC) uses in bringing enforcement actions: whether it deems a company's cybersecurity policies to be "deceptive" or "unfair." What is unfair when it comes to data security? According to one recent court decision, *Federal Trade Commission v. Wyndham Worldwide Corporation*, 799 F.3d 236 (3d Cir. 2015), determining unfairness "is a cost-benefit analysis … that considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity." That court may deserve the understatement-of-the-year award for its "acknowledge[ment] [that] there will be borderline cases where it is unclear if a particular company's conduct falls below the requisite legal threshold." An in-house lawyer, often aided by outside counsel, needs to help guide the executive team with respect to the standard of care to which they will be held accountable by various agencies.

A complete list of data security legal issues that companies may face is well beyond the scope of this article. But here are some questions in-house attorneys can pose and help answer, either alone or in consultation with outside counsel, in order to both promote compliance with legal requirements and reduce the risks of a harmful cyber-attack:

Do we have robust data security policies and are we complying with them?

Counsel should begin by ensuring that their companies have robust data security policies. Counsel must then follow up to make sure that their companies are complying with the businesses' own data security policies and are being accurate in their representations to consumers. Over-promising on cybersecurity is like ringing the dinner bell for government regulators and class action plaintiffs' lawyers. Exaggeration, bold marketing claims, and loose language have no place in a company's representations to consumers. Unless a company really does use industry-leading firewalls to guarantee 100% protection of its consumer's data, it shouldn't claim that it does have those features.

How do our data security policies compare to our industry peers' policies?

This is an important question for in-house counsel because data security regulators and courts are likely to consider industry standards in judging whether a company's policies are adequate. Outside counsel can work with cybersecurity consultants and a company's IT department to identify areas for improving compliance with industry standards.

Is company leadership paying enough attention to cybersecurity?

In-house counsel can play a key role in ensuring that data security receives the attention that it deserves at the board and c-suite level. The board and key executives should regularly examine and discuss potential data security risks to the company. Ponemon's survey results suggest that companies that invest in cyber security, appoint a high-level security leader, and form a senior-level security council can generate significant savings when it comes to the costs of dealing with a data breach. In light of the increasing prevalence of cybersecurity litigation alleging that directors and officers breached their fiduciary duties—including D&O lawsuits filed after the Target, Wyndham Worldwide, and Home Depot data breaches—promoting active corporate governance of data security not only makes good business sense, but also can help to protect company leadership from litigation.

Do our employees know how to avoid common hacking methods?

Many companies' Achilles' heel when it comes to cyber-defense isn't a technological one, but rather a human one. Hackers frequently use spear-phishing emails that are designed to trick unwitting employees into disclosing their usernames and passwords or into clicking on email attachments that will launch malware on company systems. Security awareness training is an integral component of any data security program.

Sometimes, IT departments focus on the technology and not on the employees, partly because that is where their expertise lies and partly because they do not feel empowered to tell executives or employees what to do. Counsel can help with both challenges. Business attorneys can translate complex technical concepts into terms that everyone can understand and can help make clear to team members at all levels that cybersecurity is a legal and company priority.

Are our vendors secure?

Businesses frequently provide network access not only to their employees, but to vendors as well. When vendors have such capabilities, they must also be secure or they can become weak links in the customers' defenses. Vulnerable vendors are where the Target and Home Depot data breaches began.

Attorneys are well-positioned to ask the right questions to identify unsecure vendors. In-house counsel can help their IT and procurement departments to prepare vendor contracts that require compliance with data security standards, mandate that vendors respond to reasonable requests for information about their security practices, allow for audits of the vendors' data security practices, and hold vendors accountable in the event of a security lapse.

Is our cyber-insurance coverage adequate?

Cyber-insurance coverage can help to reduce the financial costs to your company in the event of data breach litigation. Attorneys with expertise in spotting exclusions, liability caps, and other coverage limitations can assist in evaluating whether a company has adequate cyber-insurance coverage.

Are we prepared to respond in the event of a data breach?

Attorneys play a critical role in the initial hours and days after a data breach is discovered, including advising the company on evidence preservation, data breach notification requirements, and strategies for reducing damages. In-house counsel can prepare in advance of a breach by making sure that the company has a written incident response plan ("IRP"), has practice implementing the IRP through table-top exercises, and has retained outside counsel to be available in the event of a data breach. Companies should also consider identifying in advance of a breach an experienced incident response forensics firm, although such a firm should be engaged by counsel in order to help protect applicable privileges. Finally, if a legal department does not have sufficient expertise in house, it should evaluate the possibility of retaining outside attorneys to advise the company on complying with data security laws.

In short, data security is not just an IT problem today. Lawyers have a critical role to play in protecting companies from cyber-intrusions. ●