May 25, 2016

LAW BUSINESS TECHNOLOGY
BUSINESS TECHNOLOGY LAW
TECHNOLOGY LAW BUSINESS
THE RECORDER
daily at www.therecorder.com
An ALM Publication

Don't Let Your Firm Get Hacked (But Here's How to Prepare for the Worst)

By Neda Shakoori

When millions of documents leaked from Panama offshore law firm Mossack Fonseca last month, it was the biggest data breach ever. And with the number of cyberattacks consistently on the rise, coupled with an ever-changing universe of data privacy and data protection laws and regulations, lawyers can expect to be called upon for both incident planning and incident response with increasing frequency.

Organizations of all sizes and types are at risk of an imminent data breach compromising their systems and exposing their crown jewels. Data breaches cause, among other things, financial and reputational harm to organizations, various harms to consumers, employees, and clients. To make matters worse, these data breaches can, and do, result in legal consequences, arising from lawsuits brought by regulatory agencies, consumers, and employees.

With these realities in mind, attorneys can expect to play an increasingly vital role in helping ensure organizations are (1) abiding by ever-changing laws and regulations surrounding cybersecurity, data protection, and data privacy; and (2) receiving proper advice and counseling in situations involving a data breach.

The Legal and Regulatory Landscape

The prevalence of cyber attacks and data breaches has resulted in federal and state legislation, regulations, and guidance relating to cybersecurity and data breaches. The legislation, regulations, and guidance are meant to ensure and assist organizations with protecting their systems and information from cyber attacks. While enacted with the goal of keeping citizens and the country safe and secure, the regulations and legislation are not streamlined and, often times vague and ambiguous—requiring that organizations maintain "acceptable standards of cybersecurity" or that they "maintain a reasonable level of security." Additionally, many of the regulations are industry-specific, ranging from healthcare to financial services to insurance. There is no one size fits all approach. These facts create a challenge for most organizations attempting to navigate the waters of cybersecurity laws and regulations.

Given the complex web of cybersecurity and data breach laws and regulations, a considerable amount of time and resources should be devoted to addressing an organizations cybersecurity needs. Many organizations have in-house counsel who focus primarily on cybersecurity and data breach laws, requirements, and best practices. For those that do not, retention of counsel, whether in-house or outside counsel, is critical.

Neda Shakoori, McManis Faulkner

Advice and Counseling

Given the importance of compliance with cybersecurity laws and regulations, organizations need proper and timely advice and counseling. This advice and counseling should come from in-house counsel, ideally

in conjunction with outside counsel. The scope of the advice and counseling should encompass cybersecurity readiness and response, and everything in between.

Cybersecurity readiness and response requires a thorough plan, one that includes cooperation from multiple departments within an organization. In most, if not all, organizations, the approach requires executive level buy-in. Securing this buy-in requires a dialogue which should consist of: (1) an overview of cybersecurity laws and regulations; (2) industry standards and best practices, which should include a summary of the organization's ability or inability to adhere to standards and best practices and, if currently insufficient, the resources necessary to achieve, at a minimum, baseline standards; and (3) the consequences of a breach, from financial harm to litigation, to reputational harm.

Once executive level buy-in has been achieved, a cybersecurity team should be created for the purpose of drafting and revising cybersecurity policies and protocols, overseeing training and implementation of the policies and protocols, reviewing and analyzing operational reports, and participation in responding to cybersecurity incidents. The oversight team should consist of members from as many departments within the organization as possible, from legal and IT to human resources and business teams. Inclusion of members from numerous teams enables each team to communicate, brainstorm, and develop solutions for everything from the needs and concerns of their respective departments to cybersecurity threats that exist within their departments.

Perhaps one of the most critical functions of an oversight team is the development and implementation of a cybersecurity incident response plan. The plan is essentially a complete roadmap of how to respond to a cybersecurity incident—from what was breached, to who to contact subsequent to a breach, to what measures need to be immediately taken to reduce damage resulting from the breach. Such a plan again requires communication across all departments for purposes of determining: (1) the various types of data the organization possesses and guidance on steps to follow for breach of each type of data; (2) classification of the type of breach (phishing scam v. denial of service v. internal breach); (3) the ideal response for the particular type of breach; (4) the teams or individuals who are to assist with the breach (IT, legal department, law enforcement); (5) the various tools available to address the particular type of breach; and (6) steps to be taken once the breach has been contained. Depending on the type of organization, there may be many more components to the incident response plan. However, these basic components provide a useful launching pad.

The top-down approach to cybersecurity readiness additionally requires an operational team dedicated to communicating with and reporting to the oversight team regarding successes and failures of internal cybersecurity audits, cybersecurity vulnerabilities, and, in the event of a breach, all information surrounding what was breached, when the breach occurred, the location(s) of the breach, how the breach occurred, and who is responsible for the breach. The operations team should also be charged with running cybersecurity breach simulations for purposes of determining how individuals within the organization will react, as well as to uncover vulnerabilities in the organization's systems. All of this information should be regularly communicated to the oversight committee to ensure the organization is well-equipped and ready to handle a cybersecurity incident.

Considering there are federal and state cybersecurity and data breach laws and regulations, cybersecurity readiness is even more critical. The discussion and plan should be focused on prevention of a breach, especially so given the reality that most organizations can expect a breach at some point in time. Prevention of a breach is the ideal scenario. However, organizations are remiss if they are not also focusing on what to do once a breach occurs. Today's lawyer, whether in-house counsel or outside counsel, can expect to be called upon for both incident planning and incident response with increasing frequency—a call of duty which can be met with proper planning and guidance.

Neda Shakoori *is an attorney in the Commercial and Business Litigation group at McManis Faulkner. Shakoori also established and leads the firm's e-discovery practice, wherein she provides management, consulting, and training on all e-discovery matters for the firm and the firm's clients.*