Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Top Tips For Data Breach Readiness And Response

Law360, New York (March 25, 2015, 11:03 AM ET) --

Elizabeth C. Rogers

Thirteen years after California passed the first-ever breach notification law in 2002, there are now only three states that do not have one — Alabama, New Mexico and South Dakota. While most states have embraced the need for consumer identity theft remedies and notification legislation, there are almost as many differences in each state's law as there are states. It is within this context that the federal government has become more proactive in addressing the public outcry that immediately followed the massively invasive cyberattack on Sony Pictures Entertainment Inc. by proposing a national standard for definitions of sensitive personally identifiable information and a deadline for breach notification.

Until Congress agrees on uniform responsibilities and liabilities, however, companies operating in the U.S. must traverse the patchwork of laws in 47 states and the District of Columbia, in addition to the regulations of multiple federal agencies that have assumed oversight roles for privacy and security practices. Among this state of uncertain standards, what recommendations are trusted advisers providing to their clients?

Several practical solutions are available to businesses in partnership with their privacy lawyer, to mitigate the risks of a breach occurrence while contemporaneously laying the foundation for a litigation defense strategy in the event that one occurs. These tactics will go a long way in reducing the cost of a breach and/or the potential cost of a settlement with regulators and/or class action litigants. So, without regard to whether any law requires these following steps, a trusted adviser will help you to establish the proper standard of care that applies to their data and the employees and other authorized third parties who handle it.

Develop a Robust Privacy and Information Security and Awareness Training Program

When it comes to news about data breaches, the hackers and criminals are the headline grabbers, but statistics show that most data breaches are caused by threats from the inside — or employee mistakes and system glitches caused by employees taking shortcuts. According to Michael Bruemmer, vice president of consumer protection at Experian PLC, of the 3,100 incidents that Experian Data Breach Resolution serviced in 2014, "81 percent had a root cause in employee negligence. The most common

issue was the loss of administrative credentials — username and password — but also included lost media, firewall left open, lost laptop, etc.," he said. While user error and employee laziness are the most vulnerable links in a company's privacy perimeter, these are also the most under-reported and, therefore, least emphasized areas of a company's time and resources.

Therefore, a must do for companies in 2015 is to hand-select training that aligns with federal and state laws relevant to its industry and data classification. Besides teaching all levels of staff what data requires protection by law, companies also must focus on mitigating the risks that arise from everyday threats. These critical lessons include how to detect and avoid a phishing campaign and rules for password strength and complexity.

If threat-monitoring technologies (e.g., data loss prevention tools and/or others) are deployed throughout the company's networks and systems, be sure to include awareness of the lack of privacy expectations in the training as well as critical user-friendly information about how the technology operates and what it does. Many companies are also increasingly in need of guidance about laws and best practices that apply to mobile data on smartphones and other portable devices. For example, in a global company, this data may "cross borders" if hosted by a cloud provider in a foreign jurisdiction. Therefore, keep in mind that the key drivers behind any training program that is developed or purchased should be awareness of what data is processed by the company, where and when it is processed, and by whom.

Develop a Written Information Security Response Plan

A written incident response plan and cybercrisis communications guideline not only helps to calm the scene during response activities, but it also serves as an effective link in a company's litigation defense strategy. Multistate companies should consider mapping their plan according to the strictest state's law controlling their data. For example, companies with a California presence would be prudent to have a plan whose operative breach notification deadline is mapped to the state. An obvious benefit of mandating responsive behavior according to the strictest laws that control the company is the ability to satisfy standards that are less strict in other jurisdictions of operation. Another positive result for mandating the strictest standards for post-breach response is the ability to demonstrate to federal and state regulators that the company takes its consumers' welfare seriously.

The process of drafting or updating an ISRP is also one of the most effective ways of bringing all key stakeholders to the same table for a holistic approach to information privacy and security. In other words, to the extent applicable, [invite a board member, members from the offices of risk management, compliance, general counsel, communications and human resources, in addition to the traditional members of the response team from information security, privacy and information technology. This assembly of thought leaders will not only provide valuable perspectives from their own respective trenches but also will gain an understanding of and preparation for key first steps that should be taken in the immediate aftermath of a breach. Again, this effort shows a post-breach jury or federal and/or state regulator that the company is aware of its responsibilities to protect consumer data and to provide them with the notice that the strictest law requires if it is compromised.

Of course, every final draft of an ISRP should be immediately followed by at least a daylong session of tabletop exercises. Unfortunately, most any newspaper from any city on any day of the week will provide the tabletop organizer with the ideal scenario. Consider having a two-day session and wait to let the stakeholders know that it's an exercise until the second day. Consider extra emphasis on privilege issues arising from communications between computer forensics experts and, if applicable, whether

separate counsel should be hired for the board to consider disciplinary issues and potential shareholder litigation. Also, make sure that the risk management or compliance offices know their roles about when to trigger notice to the cybersecurity insurance providers.

Develop a Healthy Relationship with Breach Response Vendors and State and Federal Regulators Before a Breach Occurs

One of the key tools in any breach response kit is a strong relationship with breach response vendors and staff members of federal regulators and the state attorney general's consumer protection and/or privacy divisions. While it's easy to paint any breach in black and white (in terms of the consumer victim up against the company with a negligent security system), most regulators know that the company is often a victim too. We all now realize there will never be a silver bullet for breach prevention and so regulators, too, are aware that hacks will occur no matter how mature a company's breach mitigation strategy may be.

With respect to regulators and law enforcement, one option to consider (in appropriate circumstances and only after consultation with your legal counsel) is making arrangements through your lawyer to meet attorneys general, the Secret Service, Federal Bureau of Investigation and any other relevant regulator to introduce your company's business and discuss data security issues as part of your information protection strategy. It shows that your organization is serious about data protection and privacy and may help to earn your regulators' trust and respect. By meeting those who protect consumers before a data compromise occurs, your company will have established a prior personal relationship that may help when it comes time to report a data breach. Regulators may be more inclined to offer advice, listen to the company's side of the story and give your company the benefit of the doubt about risk mitigation steps that they have taken.

Also, your company will not want to be making difficult decisions about third-party vendors in the middle of a breach response. There are several categories of third-party vendors who perform critical functions and are needed during a data breach. The most relevant businesses to investigate provide the following services: Computer forensics, breach notification, crises communications, consumer remedies (credit monitoring and identity theft), call centers and legal services. So, if at all possible, consider several options in each category and set up meetings so you will know which ones will provide your company the most effective breach response tools and solutions.

If your company develops partnerships post-breach, it's best to breath calmly and stay away from the panic button to minimize crises-induced damage. While many companies are in denial and do not want to notify anyone, others are too quick to publish notifications that have inaccuracies or misstatements. So, finding that Goldilocks "just right" timing is something that usually can be finessed only with the advice of a counselor who has dealt with regulators before. Companies need subject matter experts to help them define and document all conversations. Post-breach conversations with regulators, without advance input from or representation by a trusted adviser, is tremendously risky. Your privacy attorney will advise you that a key to successful resolution of regulatory investigations, in the aftermath of a breach, is communication that is timely, transparent and responsive. Keep your privacy attorney involved throughout the entire response process so that all notes and reports are privileged, no matter how minor the call.

Conclusion

A data breach today causes more than just financial damage, although the financial cost can be

significant. Data breaches are now high-profile events that can result in significant reputational losses and have a long-lasting adverse impact on a company's business. Because technology is advancing rapidly and hackers are becoming increasingly sophisticated, preventative practices and response strategies should be constantly evolving. A proactive approach that includes all relevant internal and external stakeholders is the best means for developing risk mitigation strategies. Offensive security strategies won't always prevent breaches, but advanced planning and training will help contain damages should the worst happen. Proper preparation today may save a lot of perspiration tomorrow.

—By Elizabeth C. Rogers and Alan N. Sutin, Greenberg Traurig LLP

Elizabeth Rogers is a shareholder in Greenberg Traurig's Austin, Texas, office. Prior to joining the firm, Rogers served as the first chief privacy officer in Texas state government and developed a model privacy program that she shared with other data privacy professionals in agencies throughout Texas and other states.

Alan Sutin is a shareholder in Greenberg Traurig's New York office, where he serves as co-chairperson of the firm's global intellectual property and technology practice group, which includes the firm's privacy and data security team.