COMPUTER AND TECHNOLOGY SECTION

Circuits

Newsletter of the Computer & Technology Section
of the State Bar of Texas

Volume 3: Winter 2015

TABLE OF CONTENTS

The Corner Privacy Counselor: How to Prepare for Breach Readiness and Breach Response

By Elizabeth Rogers

Thirteen years after California passed the first ever breach notification law in 2002, there are now only 3 states (Alabama, New Mexico and South Dakota) that do not have one. And, while most all of the United 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 substantially invasive and massive hack of Sony Entertainment, 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, our multistate clients must traverse the patchwork of laws in 47 states and the District of Columbia, in addition to the regulations of multiple federal agencies who have assumed oversight roles for privacy and security practices. Among this state of uncertain standards, how do we manage our role as trusted advisors for our clients?

For now, we can take comfort in recommending some practical tactics that are designed to mitigate the risks of a breach occurrence while contemporaneously laying the foundation for a litigation defense strategy in the event that one occurs. In either case, these steps 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, we provide a valuable legal service by advising clients to observe the proper standard of care that applies to their data and the employees and other authorized third parties that handle it.

Develop a Robust Privacy and Information Security and Awareness Training Program

When it comes to news about data breaches, the hackers and the criminals are the headline grabbers but, statistics show that most data breaches are caused by insider threats – or employee mistakes and system glitches caused by employees taking shortcuts. According to Michael Bruemmer, vice president of Consumer Protection at the credit reporting and financial services firm Experian, of 3,100 incidents that Experian Data Breach Resolution serviced in 2014, "81% had a root cause in employee negligence. The most common issue was the loss of administrative credentials – user name 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 link in a company's privacy perimeter, it is also the most under-reported and therefore, least emphasized area of a company's time and resources.

Our role as a practical counselor involves helping clients to hand-select the training that is best suited for them according to relevant federal and state laws that control their particular industry sector. Beyond what laws control the industry sector, however, we should also encourage our clients to focus on mitigating the risks that arise from every-day threats, such as how to detect and avoid a phishing campaign and rules for password strength and complexity.

If the client deploys threat monitoring technologies (e.g., data loss prevention tools and/or others), 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 the client has, where and when it is processed and by whom.

Develop a Written Information Security Response Plan ("ISRP")

One of the best favors that a client can do for themselves is to have a prepared Information Security Response Plan (ISRP) for breach response and cyber crisis communications that is mapped to the strictest laws controlling their operations. For example, if company has a California presence, then it would be prudent for the plan's operative breach notification deadline to be mapped to that of California. 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 ideal 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, encourage your clients to 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 a valuable perspective from their own respective trenches but also will have 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 your client 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 day-long session of table top exercises. Unfortunately, most any newspaper from any city on any day of the week will provide the table top 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. Make sure that the risk management or compliances offices know their roles about when to trigger notice to the cyber security insurance, as well.

Help Your Clients Understand the Value of Healthy Relationships 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's 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 bad 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 happen no matter how mature a company's breach mitigation strategy happens to be.

With respect to regulators and law enforcement, reach out to the relevant Attorney Generals, Secret Service, FBI, and any other relevant regulator to introduce your client's business and discuss data security issues as soon as possible. It shows that your organization is serious about data protection and privacy and might earn your regulators' trust and respect. By meeting those who protect consumers before a data compromise occurs, your clients will have established a prior personal relationship that may aid them when it comes time to report a data breach, and the regulators may be more inclined to offer advice, listen to the client's side of the story, and give the client the benefit of the doubt about risk mitigation steps that they have taken.

Also, your client 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 to investigate provide the following services: computer forensics, public relations, notification activities, consumer remedies (credit monitoring and identity theft), call centers, and legal services. So, if at all possible, refer your clients to several options in each category and set up introductions so they will know which ones give them the greatest comfort level before the chaos begins.

If you have been brought in after the fact of breach declaration, be sure to keep your client away from the panic button and allow you to calmly guide them through each step. 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. Point out the requirement for defining and documenting each conversation and point out how risky it is to talk with regulators without advance input from or representation by you. They will need your reminders that a key to successful resolution of regulatory investigations, in the aftermath of a breach, is communication that is timely, transparent and responsive. Encourage your client to involve you throughout the entire process so that all notes and reports are privileged, no matter how minor the call.

Conclusion

Because this is an area of law practice that was born only in this 21st century, we all have much to learn about best practices before and after a security breach. The more that we can collaborate with stakeholders at all levels of all industries, the more practical lessons we will learn and the more prepared we will be, and our clients will be in turn.

About the Author

Elizabeth C. Rogers, a shareholder in Greenberg Traurig's Austin office, focuses her practice on data privacy and cyber security matters, including those related to privacy program development (governance and policy), counseling about global privacy regulations, negotiating privacy and information security controls in third-party vendor contracts, cyber insurance and breach response. Prior to joining the firm, Elizabeth 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.