



Legal Team's Role in Investigating and Responding to a Data Breach

By Elizabeth Rogers and Melissa Singleton

Data security incidents continue to pose a serious threat to organizations of all sizes. In 2017 alone, there were 829 data breaches made public, according to the Privacy Rights Clearinghouse. This doesn't even include the hundreds of additional likely cyber incidents that did not rise to the level of requiring public disclosure.

And while the majority of these breaches were a result of hacking or malware, one in four of them was caused by unintentional disclosure of data by an employee. In fact, most cybersecurity experts warn that it is a matter of when—not if—your company will be a victim of cyber crime.

The stakes are already quite high for organizations and are rising each year. Consider these sobering consequences, according to the Ponemon Institute:

- The average organizational revenue loss from a data breach last year was \$7.35 million;
- In 2016, there was a 2.9 percent increase worldwide in the loss of customers as a result of a breach, most of which occurred in the financial, health care and services industries; and
- The negative impact of a data breach on consumer trust in a company's brand is long-lasting.

There is no substitute for being well-prepared in advance of a cyber incident. It's important to have in place a number of things that will help your organization more effectively deal with an inevitable data breach attack.

Of course, the commercial impacts are one thing, but the legal and regulatory consequences are another matter. The ongoing cyber crime threat has led to increased focus from regulators and law enforcement agencies to ensure that organizations fulfill their appropriate obligations for post-breach notifications. In turn, this has cranked up the pressure across all corporate departments—from Legal to IT to Compliance—to coordinate their internal processes with a focus on quickly identifying a breach, taking swift action to remediate the damage, initiating immediate legal steps to protect the enterprise, and complying fully with all regulatory obligations.

The purpose of this white paper is to explore the challenge of responding to a cyber incident and to provide insights regarding how to manage the process of data breach investigations and notifications.

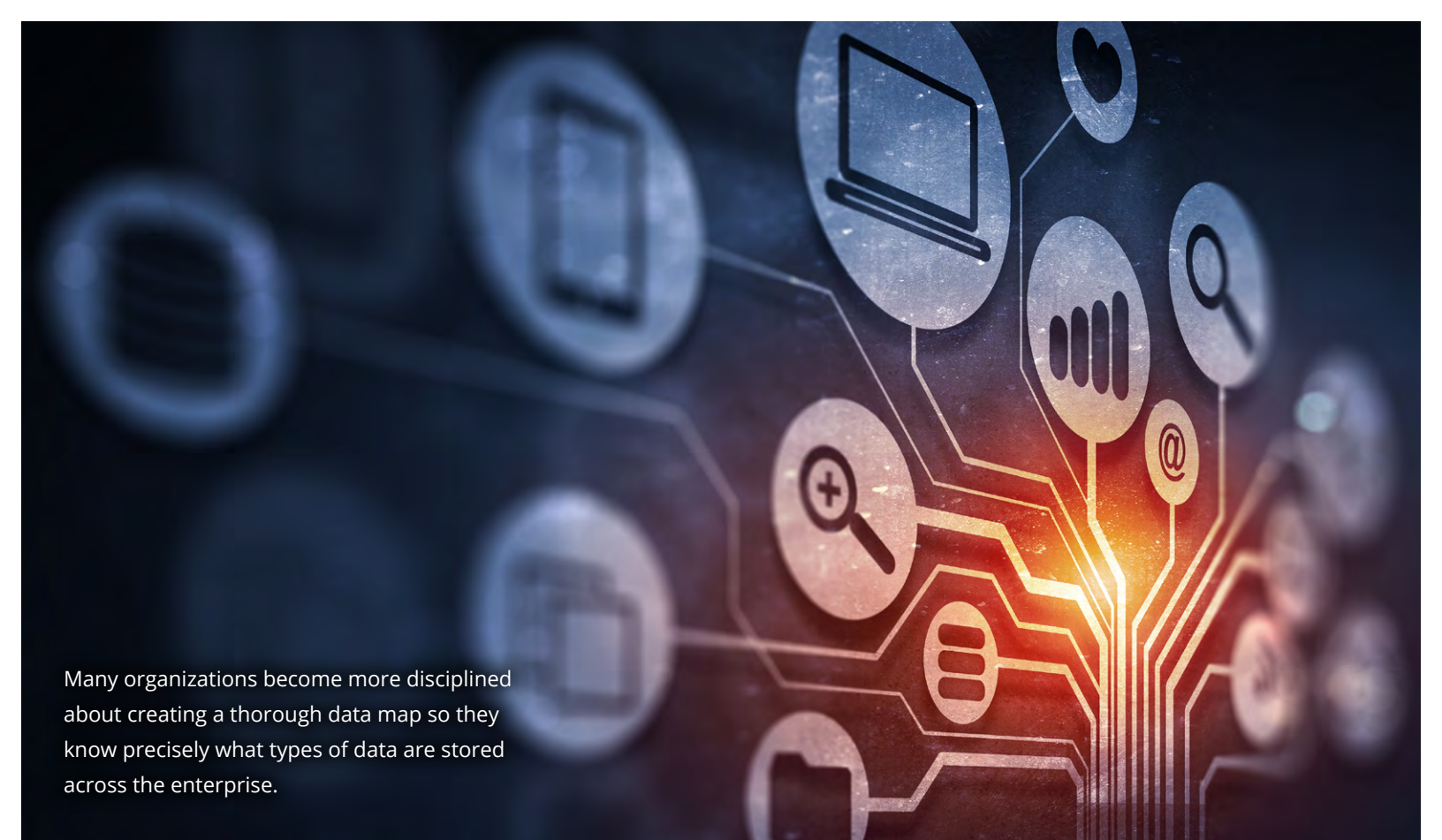
Planning for Incident Response

There is no substitute for being well-prepared in advance of a cyber incident. It's important to have in place a number of things that will help your organization more effectively deal with an inevitable data breach attack.

First, make sure that you have a comprehensive incident response plan. While there are a number of template plans available online, it's important to customize your plan to your unique organizational structure and industry. This plan should identify the various stakeholders involved—including both internal and external professionals—and outline their specific responsibilities in the event of a breach.

The members of the response team should vary depending on the nature and breadth of the incident, with more serious breaches involving a larger circle of individuals. In this process, be very careful to establish reporting channels that protect the attorney-client privilege, as the incident response plan will require notifications and document sharing across the members of the team. For this reason, the first phone call made by an in-house counsel notified of a major data breach should be to outside counsel, who can better protect the integrity and confidentiality of the incident response. Third-party experts, such as forensic examiners, should often be retained by outside counsel in order to follow court precedent regarding the scope of the attorney-client privilege during breach response.

Once the plan is in place, schedule time for conducting tabletop exercises and perhaps even full-bore simulations to run through the execution of the incident response plan under mock conditions. You will likely learn a lot about where your plan falls short by holding these drills. For example, many organizations discover the importance of proper "cyber hygiene" in their day-to-day operations and become more disciplined about creating a thorough data



Many organizations become more disciplined about creating a thorough data map so they know precisely what types of data are stored across the enterprise.

map so they know precisely what types of data are stored across the enterprise—and where those data storage facilities are located, either in physical locations or in the cloud.

After the practice exercises have been conducted, it is important to perform a thorough post-incident analysis. Document exactly how everyone responded, identify areas for improvement, and look closely at whether proper simulated notifications took place during the exercise. This should be determined by the applicable regulatory bodies, the size of the breach and the nature of the data that was compromised in the drill. These global, national and state notification requirements change often, so incident response planning should be revisited each year to make sure all protocols are current.

Responding to a Breach

When the phone rings with news of a confirmed data breach, it is important that in-house counsel proceeds swiftly from the very first moments of the initial identification to the initial stages of the post-breach investigation. There are some primary issues that must be assessed when responding to a breach.

Type of data breached

The type of information that was compromised will drive your first determination: was this a corporate information security incident or was this a reportable incident that requires notification to regulatory agencies and/or other external stakeholders? For example, did it involve the disclosure of personally identifiable information (e.g., Social Security numbers or private medical records)? This is where your incident response planning will pay off, providing you with the criteria for making the proper determination and—if appropriate—triggering your data breach notification protocols.

Notification requirements

Once you have an understanding of the type of information that was breached, the next step is to understand clearly your legal requirements. If the facts on the ground indicate that there is no cause for external notification, then you can proceed directly to the post-breach investigation. If the targeted data only involved a small population of individuals and does not trigger a legal requirement, then you may choose to notify those affected individuals directly. If there is

a serious breach that triggers mandatory notifications, then it's important to provide both the affected individuals and all relevant regulatory agencies with information about the incident as quickly as possible.

Contractual disclosures

There are also potential business-to-business contractual disclosure requirements that may be activated by the cyber incident. For example, major vendors, data processors, strategic business partners and even insurance carriers often have very specific language in their contracts with other companies that mandate the disclosure of data breaches when they hit certain thresholds. It's important to meet those contractual obligations in a timely manner.

Everyone should have a clearly defined role and should feel empowered to do their job in the sequence and manner laid out by the incident response plan.

Chain of custody throughout investigation

Another crucial post-breach area that requires careful attention is to make sure you maintain proper documentation of the investigation and protect the chain of custody so the evidence collected is defensible. The first step in this process is to hire a good forensic investigator with experience working on data breach investigations. Then work closely with that professional to follow your information governance process and create the proper documentation that will maintain that chain of custody. Also, make sure that your internal and external forensic investigation team members are using court-approved digital forensics software tools

throughout the workflow of data collection, analysis and preservation.

In the pressure-packed early moments of responding to a data breach, it is important to rely on your advance planning and the expertise of your respective team members, trusting them to do what they do best. Everyone should have a clearly defined role and should feel empowered to do their job in the sequence and manner laid out by the incident response plan. Resist the urge to meddle in areas beyond your area of expertise, even when it comes to something as seemingly innocuous as powering the software tools on or off. Stay in your lane and urge your colleagues to do the same.

Post-Breach Role of In-House Legal

So what is the best lane for in-house legal professionals to occupy in the post-breach response and investigation? The first thing to do is identify and embrace the respective roles of the in-house and outside counsel. One approach that seems to work well is to think of the in-house lawyer as the conductor of a train, in charge of making sure the post-breach response stays on track and that all of the key decisions are made in a timely manner. Think of the outside lawyer as the conductor of a symphony, in charge of making sure that everyone is in tune and that the proper notes are being played so that the "audience" hears a cohesive story from the company. These mutually supportive roles help to make sure that the organization minimizes exposure that may arise from state or federal laws.

For the in-house legal team charged with driving the train, here is a five-step checklist of key responsibilities to consider, based on a collection of best practices learned from managing cyber incidents of all sizes and types:

1. Provide ongoing counsel—Keep an eye on all the moving pieces of the investigation and be prepared to chime in with direction from time to time. Someone needs to keep the trains moving.



It's important to identify and embrace the respective roles of the in-house and outside counsel.

2. Champion for collaboration—Involve your IT, Compliance and Security teams as needed to make sure there is cross-division collaboration throughout the investigation. Lean on others when their expertise is involved; be viewed as the central member who is bringing relevant professionals into the loop.
3. “Chaos Coordinator”—Be prepared to manage the inevitable messiness that comes with high-stakes, emergency circumstances such as a cyber incident. This may involve being a traffic cop to get things done and it may involve turning down the temperature when the pressure gets highest.
4. Individual lawyer responsibilities—Know each in-house and outside lawyer’s area of expertise and keep them focused on their roles. An effective team requires an effective coach who gets the best out of each player.
5. Protect attorney/client privilege—It ultimately falls on your shoulders to make sure that all appropriate

steps are taken to protect the privilege throughout the investigation. Be clear-eyed about your ethical duties to the company and its various stakeholders; you may be the individual standing between the loss or the preservation of confidentiality.

Another way that legal professionals can make sure they are keeping the train moving is to require that all of the professionals involved in the post-breach investigation are using the best available software tools to manage the collection, analysis and preservation of data. For example, AccessData’s AD Enterprise is a software product that provides deep visibility into data collected during post-breach investigations, facilitates regulatory and legal compliance obligations, and helps your team respond quickly to an incident while maintaining chain of custody throughout the investigation. The software works in conjunction with AD eDiscovery®, a tool that allows your team members to preserve electronic evidence in a forensically sound manner in the event that you require a court-validated software platform for potential litigation matters.

Conclusion

The first step in an effective post-breach incident response actually happens long before the crime itself with the creation of a comprehensive plan. But it's not enough to develop that plan and stick it on a shelf. Nothing goes according to the way you drew it up in the midst of an actual crisis, so it's important to practice your team's post-breach response with mock exercises and annual drills. This discipline will help your team to revise your data maps so you know where the most sensitive electronic information resides, and to sharpen your knowledge of data breach notification requirements.

In the end, you need to have very clear sequencing for the timing and the nature of your post-breach response. Understand which professionals—both internal and external—will be brought into the loop and in what order, as well as what thresholds trigger additional levels of notifications to other internal and external audiences. Perhaps most important, make sure that you are working with a team of trained professionals inside the company, at your outside law firm, and at a digital forensics investigation firm—all of whom are working collaboratively with the best software tools and optimal workflows to get the job done accurately and efficiently.

About the authors

Elizabeth Rogers is a partner at Michael Best & Friedrich LLP. Melissa Singleton is customer success manager at AccessData. This white paper is based on a live webinar conducted on September 25, 2018. To download the recording, please go to: marketing.accessdata.com/IR-webinar



Whether it's for investigation, litigation or compliance, AccessData® offers industry-leading solutions that put the power of forensics in your hands. For over 30 years, AccessData has worked with more than 130,000 clients in law enforcement, government agencies, corporations and law firms around the world to understand and focus on their unique collection-to-analysis needs. The result? Products that empower faster results, better insights, and more connectivity. For more information, visit www.accessdata.com

Visit us online:

www.accessdata.com



Global Headquarters

+1 801 377 5410
588 West 300 South
London, Utah

North American Sales

+1 800 574 5199
Fax: +1 801 765 4370
sales@accessdata.com

International Sales

+44 20 7010 7800
internationalsales@accessdata.com