
epiq clarity
Strategies for Preventing and Responding to a Data Breach
Author:
Brookes Taney, Epiq
People. Partnership. Performance.

Increasingly, it's not a matter of if, but when you'll encounter a data breach threat. The stakes are high: Cyber-criminals are getting smarter, security demands are getting tougher, litigation stemming from data breaches is on the rise, and regulatory agencies are taking note.

Increasing Risk of Breaches

Data breaches and hacking have been in the news a lot lately – and that trend is on the rise, with cyber incidents taking center stage. Corporate targets are expanding – in the past, only large retailers holding credit card information were targets. Now, health organizations holding HIPAA and SSN information – which are strictly regulated – as well as many other large organizations, are being targeted for reasons beyond pure financial gain.

The Sony data breach in 2014 was a watershed moment in terms of data breaches. This was a targeted attack that sought only to do harm, not to net financial gain for the hackers. Interestingly, this breach targeted types of information that weren't previously protected in the same way that more "sensitive" information, such as personally identifiable information (PII), might be.

Defining Data Breaches

There are currently 48 different sets of regulations governing data breach notification in the U.S., and a "data breach" is defined slightly differently in each jurisdiction. However, generally, a data breach is an unauthorized acquisition, access or use of personally identifiable information. A breach compromises the security, confidentiality or integrity of personal information.

It's important for legal and business practitioners to know that using the word "breach" in communications triggers certain legal obligations, including notification obligations. It's important to remember that, until proper diligence has been conducted regarding a cyber incident, to use the word "incident" rather than "breach" to ensure notification obligations are not activated until needed.

Negligence vs. Intentional: Who's Liable?

How the data was leaked is immaterial to the trigger of a notification statute. However, if there is litigation related to the breach, this is where negligence may come into play. Class action litigation resulting from a data breach is increasingly common.

Notably, Sony Corp. agreed to pay as much as $8 million to settle claims from employees over the theft of their personal information. So while notification obligations apply irrespective of assignation of fault, doing everything you can to both protect against and remediate damage from a data breach is of utmost importance in order to limit liability.

What Types of Information are at Risk of Breaches?

Some types of information are more commonly breached than others. For example, protected health information, nonpublic but personally identifiable information (PII); personal financial information such as credit card or bank account numbers; customer data; trade secrets or intellectual property; and executive targets.

Although protecting this at-risk information is important, there is much unaddressed risk around other types of information. The "crown jewels" of information shouldn't be the only types of information risk, legal and IT professionals should be working to appropriately protect.

Breach Obligations, Liabilities & Litigation

Each U.S. state differs with regards to what constitutes a data breach, how PII is defined, and how notifications must work. As both technology and data breach incidents increase and evolve, more and more diverse data points are being added to the list of things considered PII – such as email addresses, usernames, passwords, security questions, and so forth.

Many information security laws and statutes are aimed at proactive prevention – New York and Massachusetts are both good examples of strict legislation in this area, and we may see more states start to follow suit.

Additionally, states attorneys general are all very interested in this, including in the notification requirements. Even when statutes don't specifically require an attorney general be notified of a breach incident, most states attorneys general want to be notified when a breach occurs in their jurisdiction Thus, legal practitioners must be proactive and ensure they're working with the right stakeholders before, during and even after an incident.

Litigation related to data breaches is on the rise, and the plaintiffs' bar sees this as a continued growth area. Aside from class action litigation, shareholder derivatives action is on the rise, and savvy corporate boards and shareholders should take notice.

Data Breach Risks

Financial Impact, Data breaches come with a multifaceted set of risks. At its core, the financial impact can be vast. According to the Ponemon Institute, the cost per record of a data breach is $214. That cost spread out over hundreds, thousands or even millions of records can quickly multiply.

The main expenses are related to retaining counsel as well as notification and call center vendors, the expense of credit monitoring services, and, for a hack or malware incident, the direct costs of forensics and investigation. Because of the additional cost of forensics and investigations associated with hack and malware incidents, the costs associated with these types of breaches tend to be up to four times higher than other types of breaches.

Reputational Harm. The fallout from a data breach also includes reputational harm. Depending on your company's insurance plan, the cost of a crisis management firm may be a covered expense. A crisis management firm can work to minimize the exposure the data breach has in the press, work with executives to respond to PR questions and work on messaging to employees, customers, clients, vendors and the press.

Traditional Approach

The traditional approach to responding to data breaches has been primarily reactive. Organizations may even have very detailed breach and privacy plans, but the plans may not be applied to all information types, putting data at risk.

Many organizations are beginning to realize the reactive approach is not effective, and are shifting to a more proactive approach – knowing what data is stored where, how to effectively control it, and looking for problems before they occur.

Savvy organizations know that while they may not be able to eliminate the risk of a breach entirely, they can mitigate the risks with a few smart practices, applied with diligence.

Practical Tips: A Proactive Approach

Security awareness training: The first line of defense for an organization is often its employees. Having users understand their responsibilities with respect to handling information and knowing what NOT to do (such as visit untrusted web sites or opening email attachments from untrusted people) goes a long way toward preventing many problems before they begin.

Information governance: Having an up-to-date inventory of your information assets and server locations is crucial for not only understanding your data breach risk, but also for swift and effective data breach response, and can even help to limit liability after a data breach.

Information governance, or IG, is a combination of privacy programs, litigation readiness and records retention programs. It serves to answer the questions: What data do we have? Where is it stored? Is it managed securely? What policies govern it? Who has access to it?

A good information governance program will enable organizations to delete unneeded data in a timely fashion and apply cross-organizational controls. IG can also be helpful for eDiscovery and other types of regulatory compliance, controlling intellectual property, as well as helping employee productivity – by reducing the amount of time employees spend searching for information. In this way, a good IG program can also help bridge the gap between compliance and the business units.

Ongoing vulnerability assessments: Regularly scheduled vulnerability analyses that define, identify and classify information security holes in networks and other IT infrastructure are key to risk mitigation when it comes to data breaches, as well as active and

ongoing application of security patches and updates.

Tabletop exercises and current, updated incident response plans: Conduct hands-on tabletop trainings with all appropriate parties – run through a real-life scenario – both the breach itself as well as the response plan and response plan execution. This kind of preparation is critical and can make a huge difference in the success or failure of a real-life exercise.

Team alignment: Get both your internal response team and your external response team(s) in place before you need them. Pre-vet your privacy counsel and data breach notification vendor, so that if you do face a data breach threat, you won't be bogged down in contract negotiation or fielding RFP responses at the 11th hour.

Overall, regulators, lawmakers and awarding judges will be much friendlier toward organizations that have taken a proactive approach to preventing data breaches by having policies, procedures and plans in place for incident prevention and response than those that haven't.

Eating the Elephant: One Bite at a Time

There is a tension between wanting both a broad and effective information governance and data breach prevention program while also wanting to break such a large project down into manageable bites. That's why the most effective programs build consensus among many different stakeholders to ensure cross organizational buy-in. Organizations may even want to consider creating a steering committee to engage stakeholders and work from a consensus-based approach.

For further questions you can contact Brookes Taney.

P: +1 952 607 59351

E: btaney@epiqglobal.com

Epiq Data Breach Response Solutions

Our solutions include comprehensive data breach notification services including precision mailings and dedicated contact centers, as well as identity and credit monitoring to minimize or eliminate the impact of an identity theft incident. Should a data breach result in a negotiated settlement, we work closely with you to develop legal notice plans, facilitate claims review and processing, and ensure that class members receive appropriate remedies.

We manage all aspects of the process under one roof, including data acquisition and research, forms, noticing and contact center setup and support. This gives you a convenient, single point of contact throughout and enables us to drive the most effective response for you by eliminating inefficiencies introduced by cross-vendor coordination. You also have the assurance of knowing that every one of our facilities meets or exceeds the industry's most rigorous data security standards.

Following our proven project management methodology and best practices, we deliver successful outcomes every step of the way. Our standard turnaround is less than 5 days, the fastest in the industry, and rush service is also available. In case the incident requires additional support, we can provide you with comprehensive eDiscovery and class action administration.

We also offer 'no-retainer fee' proactive breach agreements to cut down on implementation time should a breach occur.

Proactive planning benefits include:

- Assistance in building scripts, templates, project plans

- Time to properly vet and audit Epiq processes to ensure the highest security compliance standards

- Call Center modeling

- Lock-in pricing for set time periods

- Participation in mock breach scenarios/tabletop exercises