Data Breach Case Study of Lessons from the Field

Experian® Data Breach Resolution
Top 5 Lessons on Breach Preparedness & Response

Data breaches just don’t quit, and, for the most part, that’s bad news for consumers and businesses. But there’s good news too, in the lessons learned from recent events. The business community now has multiple points of reference about what works and what doesn’t in breach preparedness and response.

Experian® Data Breach Resolution works closely with companies in breach response, and we’ve seen firsthand the mistakes and successes that companies can experience. Here are the top five takeaways garnered from years of experience with actual incidents.

Legal Notice
The information you obtain herein is not, nor intended to be, legal advice. We try to provide quality information but make no claims, promises or guarantees about the accuracy, completeness or adequacy of the information contained. As legal advice must be tailored to the specific circumstances of each case and laws are constantly changing, nothing provided herein should be used as a substitute for the advice of competent legal counsel.
1. Encrypt, Encrypt, Encrypt

The Problem: Hacking, a lost or stolen portable device, an accidentally or maliciously shared password: These are common causes of breaches both big and small. The best case scenario for a company is to be able to say, “Yes, something happened, but the data was encrypted.” In other words, the hacker or thief got nothing – no usable data that could lead to identity theft cases or black market sales. Unfortunately, a breach of unencrypted data is more common. In several recent breaches involving lost or stolen hard drives, the data was indeed unprotected. That leaves businesses not only having to notify customers that their sensitive data was exposed but also to explain why they weren’t using encryption – one of the very building blocks of data security.

Case in Point: A loan agency experienced a break-in at its headquarters and realized a portable device containing personal identifying data was missing. The organization notified law enforcement, issued a press release and notified affected individuals. About a month later, state law enforcement officials recovered the stolen device. It appeared the data had not been accessed. The organization breathed a sigh of relief knowing the outcome wasn’t nearly as catastrophic as it could have been considering that the one device contained millions of records.

Key Takeaway: Don’t overlook basic data security measures, especially encryption. Use it on active and stored data. Use it on portable devices, such as thumb drives and external hard drives. Use it for emails. But don’t use it on old data that’s no longer needed because you shouldn’t keep it anyway. Destroy it.
2. Be Transparent

The Problem: A breach happens and companies want to save face. That’s understandable. But, for some, that means not being open about the breach and talking about it as little as possible. The result? Affected individuals begin to suspect the breach is actually much worse than the company is letting on, and trust in the organization begins to wane. On the opposite end of the spectrum, being open about the breach helps maintain those customer relationships that are so costly to lose.

Case in Point: One university had the guts to be open and transparent about a data loss incident, setting a good example for other organizations no matter the industry. Upon discovery of the incident, the university quickly issued a press release and created a website with frequently asked questions for affected individuals. That’s in addition to notifying individuals and providing identity protection for them.

Key Takeaway: Don’t hide from a breach. Be there for your customers to put their worries at ease. When you own up to the fact that a breach happened and demonstrate that you’re handling it well, people, including key stakeholders in your organization, will respect you for it. And you won’t have to answer questions about what you’re hiding and why.

Forty-four percent of consumers who have been notified of a breach believe the breached company is hiding something, the Ponemon Institute found in 2012.¹

¹ Consumer Study on Data Breach Notification, Ponemon Institute (2012)
3. Know Your Breach Population

The Problem: Determining what data and what people have been affected in a breach helps to define your notification requirements. But keep in mind that while people want to be notified of breaches, they don’t want to be over notified, i.e. notified of a breach that doesn’t really put them at risk. So even though many state and federal regulations have tight turnarounds for notifying affected individuals, you don’t want to jump the gun. Notifying before you’ve isolated the breach population and before you know what information has been exposed can create confusion. You may notify too many or the wrong individuals. Or you may have to send out additional notifications once you better understand what really happened. And you can be sure the media will have a field day if notification snafus come to light.

Case in Point: In a recent breach at a mortgage provider, the company notified everyone in its database and later realized that only about half of them had potentially been affected in a hacking incident. Some individuals received more than one notice, making them even more nervous about the breach. The excess notifications prompted such a high volume of calls that the organization was soon overwhelmed. It just goes to show what can happen when you notify before isolating the breach population.

Key Takeaway: As soon as a breach occurs and you know sensitive data may have been affected, start working with your data breach resolution provider to ready notifications. Then put them on standby. This way you’re good to go once you determine who needs to be notified, what data was affected and what the risks are. Pulling the trigger before you have the facts can do more harm than good, but of course you want to be mindful of notification deadlines at all times.

In a recent study, 57% of participants indicated they only want to be informed of an incident if the breached organization is certain they are at risk.\(^2\)

---

\(^2\) Consumer Study on Data Breach Notification, Ponemon Institute (2012)
4. Prep a Call Center

The Problem: When you notify affected individuals of a breach, they're going to have questions. And if you think one person in your organization can handle all of the incoming calls, you're likely mistaken. Companies have been flooded with calls following breach notification, quickly overwhelming their own call center staff. Remember, you want to be transparent about the breach in order to ease concerns. If affected individuals have questions but can't reach anyone for answers or explanations, their concerns are only going to magnify. So anticipate receiving more calls than you think you will.

Case in Point: A hospital group experienced an incident involving a lost hard drive. Knowing they wanted a call center to be on point for affected individuals, the hospital contracted with Experian®, which had a call center up and running within 48 hours of signing the contract. Call center agents were prepped and ready to take calls well before affected individuals received their notification letters. The hospital had learned from prior breaches just how inundated an internal call center can become and made the smart choice to outsource this service.

Key Takeaway: A properly staffed and educated call center demonstrates to affected individuals that you care about their concerns. It’s an important statement to make, as many consumers question their relationships with an organization following a breach. To make the best impression with affected individuals, consider outsourcing your call center. This helps take the pressure off your own organization and ensures affected individuals have the attention they deserve.
5. Don’t Flub Notifications

The Problem: Breach response all comes down to the notification letter. It’s your primary chance to smooth things over with affected individuals. When the notification letter goes right – i.e. it tells affected individuals what happened, what you’re doing about it, what data was affected, what their risks are and what you’re doing about that – you can bet that you’ll lose fewer customers over the breach. When notification goes wrong – i.e. the letter is brief, vague and offers no protection tips or a protective monitoring service – it’s another story. Unfortunately, this latter direction is the one companies often take. And that leaves affected individuals – potentially millions of them, depending on the size of the breach – feeling vulnerable and confused. Remember to notify the right people, notify them once and don’t just notify them, educate them.

Case in Point: A breach at a university required hundreds of thousands of notification letters to go out. The problem? The organization had old contact information, so notification letters were sent to the wrong addresses or came back with “address unknown” – adding to the notification expense. To keep costs and repeat mailings down, verify you have current addresses by working with a vendor with address append services before notifications go out.

Key Takeaway: Think about the wants and needs of your breach population before you send out notification letters. Sixty-three percent of consumers in a recent survey want some form of compensation following a breach. Why? Because they feel they have a higher risk of identity theft. And they’re right. Fifty-eight percent of respondents agreed an identity protection product is proper compensation. So be sure to include an offer for a free year or longer of identity protection in your notification letter. In many recent breaches, companies have helped to avoid lawsuits by providing identity protection and credit monitoring for affected individuals, who in turn also receive education about protecting themselves.

4 Consumer Study on Data Breach Notification, Ponemon Institute (2012)
5 Consumer Study on Data Breach Notification, Ponemon Institute (2012)

Of 213 breaches recorded in the first half of 2012, 63% had no reported attributes, such as the cause of the breach, indicating that companies are being less transparent about incidents today than in previous years.
Of course these aren’t the only lessons learned from the trenches. A data breach is a complex incident, and each and every one is different. Here are a few more pointers taken from actual incidents to help you prepare, respond and recover:

• Test every aspect of your response plan, not just the most common scenarios. Don’t have a response plan? Download the free Data Breach Response Guide at Experian.com/DataBreachGuide.

• Keep a log of all portable and mobile devices and to which department or employee they are assigned. This will help you know when one is missing.

• Use the highest security measures for all of your data, including backup data, which you may want to store off-site. Be sure all areas of data storage are properly secured so not just anyone can walk in and take off with your files or hard drives.

• Keep employees in the loop regarding data security policies, including when it is and isn’t proper to download and save data to a portable device. Refresh your policies and retrain employees frequently.

• Never assume a vendor’s data security policies and employee training are up to snuff. Ask before you enter into a relationship with one. Be sure vendors understand your expectations for being notified of data loss and that they’ve clearly outlined their data protection measures for you.