Data Breach Response Guide

experian

By Experian® Data Breach Resolution

2017-2018 Edition

Foreword

With data breaches increasing at record-breaking speed, reaching an all-time high in 2016 with 4,149[1] incidents worldwide and 1,091[2] in the U.S. alone, it's critical now more than ever that businesses and consumers take their security seriously.

As we often say at Experian, it's not a question of *if* but *when* an organization will experience a security incident. What was once considered a major risk for large data-heavy organizations *only* is now regarded as a universal concern. The fact of the matter? Cybercriminals don't discriminate, and we're seeing new, sophisticated attacks emerge regularly. From ransomware incidents like WannaCry and Petya capable of crippling computers and critical infrastructure – as well as disguising state-sponsored attacks – to W-2 phishing scams that expose thousands of people every year with losses totaling in the billions, these attacks are impacting organizations of all sizes and sectors. If managed poorly, a major security incident can be devastating to an organization, leading to costly lawsuits, regulatory action, reputational damage and loss of customers and/or trust.

Yet, despite the growing likelihood of experiencing a security incident, companies are still not confident in data breach preparedness and senior leaders are not actively engaged in response planning. According to Experian's 2016 annual data breach preparedness study, less than half of organizations are prepared to respond to a breach involving confidential information and intellectual property, and an even smaller fraction feel confident in their ability to retain consumer and business partner trust following a breach.[3] What's more, companies are not keeping up with the evolving threat and regulatory landscape – a vital effort to ensure preparedness for emerging risks like ransomware attacks, international breaches and compliance with global security regulations such as the EU's Global Data Protection Regulation (GDPR).[4]

The silver lining? We're seeing encouraging growth in the number of organizations developing and implementing data breach response plans. In fact, the percentage with plans in place increased from 61 in 2013 to 86 in 2016.[5] Additionally, more organizations are implementing security training programs for employees and stakeholders.

Ultimately, there are "leaders" and there are "laggards" when it comes to data breach incident response planning. While some organizations are taking incident response planning seriously, others are simply "checking a box" and relying on incomprehensive plans. But, it's never too late to become a leader.

For those who are just getting started or need to audit their existing plans, this guide covers preparedness from every angle. We want this guide to be a useful tool for every organization looking to improve its security posture because the potential for a data breach is not going away. The sooner an organization gets ready, the better.

Sincerely,
Michael Bruemmer
Vice President
Experian Data Breach Resolution

[1] 2016 Year End Data Breach Quick View Report, Risk Based Security
[2] ITRC Data Breach Report 2016, Identity Theft Resource Center
[3,4,5] Fourth Annual Study: Is Your Company Ready for a Big Data Breach? Ponemon Institute, 2016

Table of Contents

Introduction

As the number of cyber threats facing organizations continues to grow and regulations become increasingly prescriptive, companies need more than just a generic plan that sits on the shelf.

Instead, they need a thorough data breach response plan that is regularly updated and practiced, ensuring effectiveness. Whether it is a few thousand or a few million records compromised, the need for a comprehensive plan remains the same.

According to the Identity Theft Resource Center (ITRC), there were 1,091 reported U.S. data breaches in 2016 across all industries, exposing more than 36 million records. A record-high year, 2016 saw a 40 percent increase from the 780 reported breaches in 2015. This year, as of September 13, there have already been 1,002 data breaches, with more than 163 million exposed records.[6]

"Since we started tracking data breaches in 2005, we have witnessed a steady increase in events year after year. Given the current landscape, it's no longer a question of 'if' your company will be attacked but 'when.' Therefore, it's crucial that every company take the necessary steps to not only train its employees on cybersecurity best practices, but to also have a plan of action in place should it become a victim of such an attack." – Eva Velasquez, ITRC CEO & President.

In this reality, it goes without saying that the data breach response plan has become a critical component of doing business in the modern era. For companies who have yet to create one – or need a refresh – this guide illustrates how to best create, implement and refine a comprehensive data breach response plan for the security challenges that lie ahead.

Since 2005, more than

1,046,870,879 records have been compromised

as the result of a data breach.[6]

Identity Theft Resource Center: 2017 Data Breach Category Summary

Report Date: 9/13/2017

Totals for Category:	# of Breaches	% of Breaches	# of Records	% of Records
Banking/Credit/Financial	64	6.4%	2,780,837	1.7%
Business	527	52.6%	149,238,244	91.5%
Educational	98	9.8%	1,112,151	.7%
Government/Military	49	4.9%	5,767,061	3.5%
Medical/Healthcare	264	26.3%	4,234,355	2.6%
Totals for All Categories:	**1,002**	**100.0%**	**163,132,648**	**100.0%**

Total Breaches: **1,002** | Records Exposed: **163,132,648**

2017 Breaches Identified by the ITRC as of: **9/13/2017**

[6] 2017 Data Breach Stats, Identity Theft Resource Center

Engaging the C-Suite

A culture of cyber security must span top to bottom, with C-Suite members leading the charge.

First and foremost, the success of any data breach response plan begins with close involvement from the executive team. Without engagement and leadership from senior leaders and board of directors, developing, maintaining and implementing effective response plans can pose a significant challenge for organizations.

However, by illustrating some of the severe implications of a data breach – such as significant financial and reputational damage – and involving the C-Suite not just during but ahead of an incident, response teams can gain their support in fairly short order.

The following data points can help you "make the case" for data breach preparedness:

34%: Organizations that claim the board understands their specific security threats[8]

57%: Say their company's board of directors, chairman and CEO are not informed and involved in plans to deal with a possible data breach[7]

Of those that are involved, only 17% regularly review the details of the company's breach response plan; 20% provide detailed feedback about the data breach response plan; and 16% participate in a high-level review of the organization's data protection and privacy practices

$126: The average cost per record of a data breach due to human error or negligence[12]

55%: Organizations that had a security incident or data breach due to a malicious or negligent employee[9]

$1.56 million: Post data breach response costs in the United States in 2017[13]

66%: Admit employees are the weakest link in their efforts to create a strong security posture[10]

29%: Organizations that do not require the CEO and C-level executives in their companies to take mandatory security trainings[11]

$4.13 million: The cost of lost business for U.S. organizations in 2017 after a breach[14]

[7, 8] Fourth Annual Study: Is Your Company Ready for a Big Data Breach? Ponemon Institute, 2016
[9, 10, 11] Managing Insider Risk Through Training & Culture, Ponemon Institute, 2016
[12, 13, 14] 2017 Cost of a Data Breach Study: Global Analysis, Ponemon Institute & IBM, 2017

Creating your plan

Creating your plan

Start with a bullet-proof response team

A data breach can take a heavy toll on any business, large or small. Having a response plan and team in place can help you prevent further data loss in the event of a breach, as well as avoid significant fines and costly customer backlash.

The actual discovery of a data breach is not the time to decide who will be responsible for leading and managing the incident. It's critical to assemble your response team well in advance, as this group will play an important role in coordinating efforts between your company's various departments. Working collaboratively, the team should include the internal members, external partners and influencers outlined below.

Assemble your breach response team to ensure end-to-end preparedness.

Your internal breach response team should include the following:

Customer care

This group will be very important to keep abreast of what is occurring as they will be on the front lines to answer questions and concerns from your customers. They will be responsible for:

- *Developing or assisting with crafting phone scripts*
- *Logging call volume and top questions and concerns by callers*

Executive leaders

Include your company's key decision makers to help ensure you have the needed leadership, backing and resources to properly develop and test your plan. This will help to:

- *Ensure decisions made by the team have the support of executive management*
- *Have a line of communication to the board of directors and other stakeholders such as investors*

Having an incident response team either in-house, via a third party or a combination of both – can shave off $19.30 per compromised record. [15]

HR

Since data breaches can affect employees, appoint HR representatives to:

- *Develop internal communications to inform employees and former employees*
- *Organize internal meetings or webcasts for employees to ask questions*

[15] 2017 Cost of a Data Breach Study: Global Analysis, Ponemon Institute & IBM

Creating your plan

Start with a bullet-proof breach response team (cont'd)

Incident lead

Typically a Chief Privacy Officer, or someone from an internal or external legal department, your incident lead will:

- *Determine when the full response team needs to be activated in response to an incident*
- *Manage and coordinate your company's overall response efforts and team, including establishing clear ownership of priority tasks*
- *Act as an intermediary between C-level executives and other team members to report progress and problems, as well as act as the liaison to external partners*
- *Ensure proper documentation of incident response process and procedures*

Information technology (IT)

IT and security teams will likely lead the way in catching and stopping a data breach, in addition to owning the following responsibilities:

- *Identify the top security risks to the organization that should be incorporated into written incident response plans*
- *Train personnel in data breach response, including securing the premises, safely taking infected machines offline, and preserving evidence*
- *Work with a forensics firm to identify the compromised data and delete hacker tools without compromising evidence and progress*

Legal

Internal legal, privacy and compliance experts can help minimize the risk of litigation and fines in the wake of a breach. Legal representatives will:

- *Determine how to notify affected individuals, the media, law enforcement, government agencies and other third parties*
- *Establish relationships with any necessary external legal counsel before a breach occurs*
- *Be the final sign-off on all written materials related to the incident*

Public relations

If you need to report the breach to the media and/or notify affected individuals, your PR representative will:

- *Identify the best notification and crisis management tactics before a breach ever occurs*
- *Track and analyze media coverage and quickly respond to any negative press during a breach*
- *Craft consumer-facing materials related to an incident (website copy, media statements, etc.)*

Creating your plan

Engage your external partners

Identifying partners and securing pre-breach agreement contracts is crucial – not only to help you be prepared, but also to keep you from being delayed by cost negotiations in the middle of your response. Ahead of an incident, partners can also help ensure that your incident response plans follow best practices and account for the latest developments in the threat landscape.

Choosing the right partner can be difficult as there has been a flood of suppliers entering the space. If you wait until an issue arises, you may be forced to make a hasty decision to work with less qualified partners or forego relationships with influencers, which can lead to significant risk when managing a breach.

Secure appropriate external partners early to ensure end-to-end preparedness.

External breach response partners

Communications

Communications partners should have experience helping companies manage highly publicized security issues and demonstrate the ability to understand the technical and legal nuances of managing a data breach. They will:

- *Help develop all public facing materials needed during an incident*
- *Provide counsel on how best to position the incident to key audiences and help manage media questions related to the issue*

Forensics

Forensics partners need to have the ability to clearly translate technical investigations of a data breach into enterprise risk implications for decision-makers within the organization. They will:

- *Advise your organization on how to stop data loss, secure evidence and prevent further harm*
- *Preserve evidence and manage the chain of custody, minimizing the chance that evidence will be altered, destroyed or rendered inadmissible in court*

Data breach resolution provider

A data breach resolution partner offers various services and can offer extensive expertise in preparing and managing a breach. Your provider should be able to:

- *Handle all aspects of account management and notification, including drafting, printing and mailing or emailing letters. They should have an address verification service*
- *Offer a proven identity theft protection product, comprehensive fraud resolution and secure call center services*

Legal counsel

Legal partners should preferably have an established relationship with local regulatory entities, such as the state Attorney General, to help bridge the gap during post-breach communication. Further, they should have an understanding of and be able to provide guidance on:

- *What to disclose that will avoid creating unneeded litigation risks based on the latest developments in case law*
- *The process to help ensure that anything recorded and documented by an organization balances the need for transparency and detail without creating legal risk*

Creating your plan

Influencers

State attorneys general/regulators

It is important to establish relationships early with your state Attorney General and other regulatory entities to streamline the response process and timeline in the event of a breach. The majority of state notification laws now require that companies notify regulators upon discovering a breach, and it is best if they are familiar with your organization ahead of an issue. To be prepared, you should:

- *Have a contact list and know state and timeframe requirements for notification*
- *Keep abreast of new requirements as they are evolving*

Law enforcement

Some breaches require involvement from law enforcement. Meeting with your local FBI cyber security officer ahead of an incident to establish a relationship will serve you well when managing an active incident. Be sure to collect appropriate contact information now so you can act quickly when needed and inquire about an up-front meeting. During an incident law enforcement can help:

- *Look for evidence that a crime has been committed*
- *In some cases, be the first to discover that a breach has occurred*

What to look for in a partner

While the right external partners can vary for each organization's unique needs, we've identified five important traits to look for when vetting partners for your breach response team:

1. ***Understanding of Security and Privacy***
   Regardless of the line of business, partners should have a background supporting different types of data breaches, along with a well-rounded knowledge of the entire breach life cycle.
2. ***Strategic Insights***
   Partners should be able to provide compelling insights, counsel and relevant tools before and during an incident to help organizations better navigate the response. Can they answer and handle "what if" scenarios?
3. ***Ability to Scale***
   Select partners that can scale to the organization's size and potential need during an incident. While the amount of data and/or people affected may seem small, upon closer investigation it may be revealed to be broader than originally thought
4. ***Relationship with Regulators***
   Where possible, it is also best for data breach partners – particularly legal firms – to have established relationships with government stakeholders and regulators. Organizations that have a collaborative relationship with attorneys general are more likely to have their support.
5. ***Global Considerations***
   If your company has an international footprint, it's important to identify what knowledge base and service capabilities the partner has globally. This can include awareness of the breach laws in different countries or the ability to implement multilingual call centers.

What is a pre-breach agreement?

A contract with a partner that is executed before a data breach occurs that establishes the relationship, so that the partner is ready when you need them.

Creating your plan

Additional considerations

Purchase cyber insurance and regularly evaluate coverage

With the average consolidated cost of a data breach reaching $3.6 million[16], it is vital that companies consider purchasing cyber security insurance to help manage this risk. Yet, only a small fraction (38 percent of organizations) take advantage of such policies.[17]

Along with providing financial protection after an incident, modern cyber insurance policies offer several other valuable resources to companies. These resources include access to leading attorneys, forensics investigators, data breach resolution providers and communications firms that can help you navigate a complex incident. Further, many policies offer additional valuable services ahead of an incident, such as access to risk management tools and pre-breach consultation with response experts.

When selecting a policy, there are several key considerations to keep in mind as part of the process:

- ***Work with an experienced broker:*** *Companies should enter the market with a solid understanding of the type of coverage they need, as well as the right partner to assist with the buying processes. Working with an insurance broker who has specific expertise in cyber insurance will help ensure your company selects the right policy and insurer to meet your needs*
- ***Understand your security posture:*** *Being able to demonstrate a strong security program and the types of security incidents that are most likely to impact the company can help ensure your organization gets the right level of coverage. Working with your insurance broker to demonstrate a strong security posture to insurers can also prove useful when negotiating the terms and cost of a policy*
- ***Ask smart questions:*** *Given that cyber insurance is still relatively new, it's important that you and your broker ask the right questions when selecting a provider. In particular, make sure you understand the potential exemptions in policies, as well as their history of paying out actual claims for incidents*

Companies will benefit greatly from cyber insurance if they are informed about their security risks, educated on the variety of policies available and aware of the coverage they need.

Selecting legal partners

From a legal standpoint, there are several nuanced characteristics that should be considered. Often companies look to their existing law firm relationships to also cover a cyber security incident, which may mean not getting the level of counsel needed to manage a complex incident. Here are a few considerations to keep in mind:

- *Law firms should have both previous experience managing data breach litigation and have established relationships with local regulators such as the state Attorney General*
- *A good legal partner should have experience that goes beyond simply helping with formal legal notification. They should be able to serve as an overall breach coach with a strong understanding of what's needed from the technical investigations, as well as the potential implications of legal decisions on trust and reputation*
- *They should be able to provide insights about the latest developments in case law, which informs the counsel they provide across the board*
- *They should be able to connect you with other external experts ahead of an incident that can assist in the other major areas of a response*

[16] 2017 Cost of a Data Breach Study: Global Analysis, Ponemon Institute & IBM, 2017
[17] Fourth Annual Study: Is Your Company Ready for a Big Data Breach? Ponemon Institute, 2016

Creating your plan

Incorporating PR and communications

It's also important to ensure that communications is incorporated into the broader incident response process and there is a clearly documented plan for how your organization will make key communications decisions, the channels you will use to get out the message and what to say.

Here are some of the key elements that can help strengthen this capacity:

- ***Enlist a representative:*** *Ensure a communications representative is part of your core incident response team and is included in legal and forensics discussions*
- ***Map out your process:*** *Document a detailed process for developing and approving internal and external communications that includes a well-defined approval hierarchy*
- ***Cover all audiences:*** *Ensure your plan accounts for communicating to your employees, customers, regulators and business partners*
- ***Prepare templated materials****: Prepare draft communications materials with content placeholders including holding statements for a variety of incident types, a public Q&A document to address questions from customers, investors and media, a letter to customers from company leadership and an internal memo to employees*
- ***Test your communications process:*** *Create a tabletop simulation for the key executives to gauge your ability to manage communications challenges such as media leaks, customer complaints, questions from employees and inquiries from state attorneys general*

Managing international breaches

While organizations are generally more prepared to manage a data breach than in previous years, responding to an international incident that occurs or impacts customers overseas remains a challenge. In fact, the Ponemon Institute found that almost half (49 percent) of organizations in the United States have security solutions that are outdated and inadequate to comply with a global data breach. Consequentially, an even smaller fraction have *the right* security technologies to protect information assets and critical infrastructure in all overseas locations.[18]

Our statistics show that a worrying number of UK businesses which hold personal customer data abroad are not familiar enough with EU GDPR legislation. Nearly half admit they are only 'fairly familiar' with the laws, its responsibilities, while two in five say the same about their global notification procedures. While quite a large proportion are not familiar with any of the required procedures a worryingly high proportion are also not bearing in mind the varied preparation they need in place with legal, insurers, multilingual expertise aligned to the jurisdiction in which they are trading, ranging from a quarter (25%) to a third (33%).

Failing to notify a breach in accordance with the requirement of EU GDPR could result in a fine of 4 percent of an organization's global annual turnover or 20 million Euros, whichever is the greater.

Only 35% of organizations report they can manage cultural differences or expectations around privacy and data security across all regions of the world.[20]

[18, 19, 20] Data Protection Risks & Regulations in the Global Economy, Ponemon Institute, 2017

Creating your plan

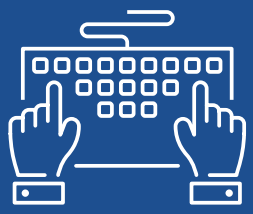
Managing international breaches (continued)

"With individuals expecting the very best experiences and reassurances there is no room for misplaced sentiments. As we move towards May 2018 and GDPR regulation, those who prepare now will be confident that they have the ability to reassure and respond competently and continue to maintain fruitful relationships with their customers." Jim Steven, Head of Data Breach Response, Experian UK.

Given the GDPR essentially creates a worldwide notification protocol, it's important that multinational companies understand and address the new requirements, and think beyond the mandated regulations to necessary actions such as coordinating a global response, engaging with stakeholders and keeping consumers notified. Thinking through a response plan is crucial to not only compliance, but also protecting consumers and brand reputation.

The following are steps your organization can take immediately to better prepare for an international data breach:

- ***Coordinate a multinational response team:*** *This team of internal support and third-party vendors – lawyers, communications specialists, a data breach resolution provider and forensic experts – can help serve as "boots-on-the-ground," ensuring local laws and customs are followed. To guarantee a quick response, these partners should be identified during the planning process*
- ***Prepare for increased stakeholder engagement:*** *With new international regulations come new groups of stakeholders that companies must engage. It is imperative that companies know who these key stakeholders are and work to build relationships as appropriate. The GDPR requires organizations to notify their Data Protection Authority (DPA) within 72-hours of discovering the breach, making it critical that companies are coordinating what this notification looks like well ahead of a breach. Additionally, reaching out to regulators early can reduce scrutiny and help streamline the process*
- ***Organize consumer notification and support:*** *One of the biggest challenges companies face when responding to an international data breach is notifying consumers and setting up call centers in multiple languages. The GDPR's 72-hour notification rule makes it crucial that organizations are prepared to notify and address consumer concerns in a timely fashion. This means ensuring impacted parties receive notifications in the correct language as well as access to a secure, multilingual call center for their questions. Another consideration for consumer support that a company should address during the planning process is whether they will offer identity protection services to affected consumers. While not mandated, these services can help quell the fears of those impacted by the breach and ultimately help improve a company's reputation post-breach*



Engage with the right resources

both domestic and abroad, as early as possible

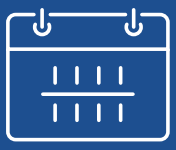
Practicing your plan

Practicing your plan

Conduct response exercises at least twice per year

Once your breach response team has been established and your response plan finalized, department-specific training should trickle down to all corners of the company from the data breach response team. Unfortunately, for many companies, there is a significant gap between completing a breach preparedness plan and practicing the elements of the plan itself.

To ensure all departments are aligned with breach response requirements and plan implementation, practice and test your preparedness plan in all areas of operation, and perform regular reviews to ensure you're ready.



Establish a schedule involving all departments

to practice implementation on a regular basis.

Responsibility of your team

Make sure everyone on your data breach response team understands his or her specific responsibilities – both in preparing for and responding to a breach. Each and every member of the team has a duty to apply prevention and preparedness best practices to his/her own department.

Activities should include:

- *Working with employees to integrate smart data security efforts into their daily work habits*
- *Developing data security and mobile device policies, updating them regularly and communicating them to all business associates*
- *Investing in the proper cyber security software, encryption devices and firewall protection*
- *Updating security measures regularly*
- *Limiting the type of both hard and electronic data employees can access based on their job requirements*
- *Establishing a method of reporting for employees who notice that others aren't following the proper security measures*
- *Conducting employee security training/re-training at least once a year*

Practicing your plan

Implementing a simulation exercise

The data breach response plan should not just be a binder that sits on a shelf. To be effective, plans must be practiced. While security awareness has increased and the majority of companies have a response plan in place, they are still not being practiced adequately. Almost one-third of organizations still do not practice their plans, yet cite this action (specifically "conducting more fire drills") as the number one way their data breach response plans could become more effective.[21]

Enlist an outside facilitator

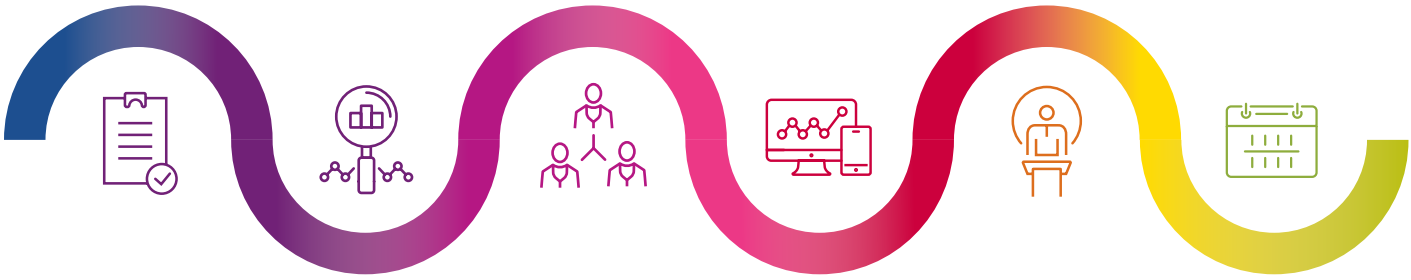
Have someone outside the organization act as a moderator and run the drill so that the team can focus on the activity.

Include everyone

Include all team members – both internal and external at headquarters and across the globe – who will be involved in responding to a data breach.

Debrief after the exercise

The team should review and discuss the lessons from the session and what to improve upon.



Schedule a healthy amount of time

Give yourself plenty of time (4 hours) to conduct the exercise and discuss the challenges experienced.

Test multiple scenarios

Address as many "what if" questions you can think of and run through different types of situations that could take place before, during and after a data breach.

Conduct drills every SIX months

Make sure to keep on top of the latest changes internally and externally with regular simulation exercises.

Who to involve:

- *C-Level Executives (CEOs, CIOs, CISOs, other chief executives and board of directors)*
- *IT*
- *Legal*
- *Public Relations*
- *Human Resources*
- *Risk & Compliance*
- *Customer Service*
- *Outside Partners (legal counsel, public relations firm, data breach resolution provider, cyber insurers)*

[21] Fourth Annual Study: Is Your Company Ready for a Big Data Breach? Ponemon Institute, 2016

Practicing your plan

Developing your simulation

Ideally you will want to dedicate a half-day for a simulation exercise so that you may address multiple different scenarios that your organization may face. These scenarios should be pertinent to your industry, the type of data you collect and the way your IT infrastructure is set up. However, each need not be 100 percent realistic and can allow for a degree of imagination because a true response will likely take weeks, not hours. Companies will still have the desired outcome of honing response skills and testing key decision-making protocol.

Sample scenarios:

- *The FBI contacts your company. They suspect that a user on the dark web is in possession of usernames and passwords of your customers and are selling them to the highest bidder. They recommend investigating the matter and suggest it's only a matter of time before the press find the posts*
- *A hacktivist organization sends your company a note claiming to be in possession of PII (names, addresses, DOB and SSNs) of your customers. They threaten to release the data unless the company meets its specific demands*
- *A company vendor that handles customer data notifies you that they suspect a breach that may have included compromise of your data. They are not divulging any information, citing a forensics investigation and advice from their legal counsel*
- *Employees are complaining that they received a 5071-C letter from the IRS suggesting that someone may have filed a fraudulent tax return in their name, or similarly, an "executive" email that requests their personal information. These alerts could be due to the potential exposure of W-2 records to attackers, otherwise a likely successful phishing scam*
- *Your organization is targeted with ransomware that takes a critical business system offline*

Developing injects

The cornerstone to every simulation is the use of "injects" to provide more information about the incident to participants and require that they react to new developments that take place over the course of the drill. These injects often force participants to make decisions or think of required response team members in different functions to take new actions. When designing an effective response drill, it is essential that there are injects designed to engage all part of the response team.

Possible injects can include:

- *A media inquiry from a reporter claiming to have information about the incident and planning to write on a tight deadline*
- *A letter from a state Attorney General threatening an investigation into the incident if he/she does not receive a detailed accounting*
- *Forensics updates informing the IT teams of additional details on impacted systems and lost information*
- *Mock angry emails from customers or employees about the incident*

Practicing your plan

QUIZ: How prepared are you?

Here are some key questions to help you evaluate your level of preparedness. If you answer NO more than once or twice, you and your team should immediately address the gaps to get fully prepared.

RESPONSE PLANNING

- Do you have an internal response team assembled?
- If you have a preparedness plan in place, have you updated, audited and tested your plan in the last 12 months?

KEY PARTNERS

- Have you identified third-party vendors and signed contracts to engage in the case of a breach?
- Do you have a relationship with relevant state attorneys general to contact in the case of a breach and ensure you are following state guidelines?

NOTIFICATION AND PROTECTION

- Have you identified what your breach notification process would look like and have the proper contact lists for relevant stakeholders (customers, employees, etc.) in place to activate quickly in all locations of operation?
- Have you evaluated identity theft protection services to offer to affected parties if you experience a data breach?

SECURITY PLANNING

- Have you taken inventory of the types of information you store that could be exposed during a data breach?
- Do you have the technology and processes in place to conduct a thorough forensic investigation into a cyber security incident?

COMMUNICATIONS

- Have you developed a communications incident response plan including drafts of key media materials that will be useful during an incident (e.g. holding statements, Q&A covering likely questions, letter from company leadership)? Do these translate for all areas where consumer data is being collected?
- Have you media trained your spokespeople and executives specifically on security matters?

TRAINING AND AWARENESS

- Have you conducted a data breach crisis table top exercise or simulation to test how effectively your company would manage a major incident in the last 12 months? Did this exercise incorporate overseas locations?
- Have you conducted employee training to apply security best practices in the last 12 months?

Responding to a data breach

Responding to a data breach

Act fast

the first 24-hours following a breach are critical.

Acting swiftly and strategically following a data breach can help you regain your security, preserve evidence and protect your brand

Always collect, document and record as much information about the data breach and your response efforts as possible, including conversations with law enforcement and legal counsel.

The first 24-hours

When you discover a data breach, immediately contact your legal counsel for guidance on initiating these 10 critical steps:

1. **Record the moment of discovery:** Also mark the date and time your response efforts begin, i.e. when someone on the response team is alerted to the breach
2. **Alert and activate everyone:** Include everyone on the response team, including external resources, to begin executing your preparedness plan
3. **Secure the premises:** Ensure the area where the data breach occurred and surrounding areas are secure to help preserve evidence
4. **Stop additional data loss:** Take affected machines offline, but do not turn them off or start probing into the computer until your forensics team arrives
5. **Document everything:** Record who discovered the breach, who reported it, to whom was it reported, who else knows about it, what type of breach occurred, etc
6. **Interview involved parties:** Speak to those involved with discovering the breach and anyone else who may know about it – then document the results
7. **Review notification protocol:** Review those that touch on disseminating information about the breach for everyone involved in this early stage
8. **Assess priorities and risks:** Include those based on what you know about the breach. Bring in your forensics firm to begin an in-depth investigation
9. **Notify law enforcement:** Do this if merited, after consulting with legal counsel and upper management

Self-detection, a key first step to an effective response, is on the rise.

From 2016 to 2017, self-detected incidents increased from 52 percent to 64 percent.[22]

[22] Be Compromise Ready: Go Back to the Basics, 2017 Data Security Incident Response Report, BakerHostetler

Responding to a data breach

Next steps

After the first day, assess your progress to ensure your plan is on track. Then, continue with these steps:

STEP 1

IDENTIFY THE ROOT CAUSE

» *Ensure your forensics team removes hacker tools and address any other security gaps*

» *Document when and how the breach was contained*

STEP 2

ALERT YOUR EXTERNAL PARTNERS

» *Notify your partners and include them in the incident response moving forward*

» *Engage your data breach resolution vendor to handle notifications and set up a call center*

STEP 3

CONTINUE WORKING WITH FORENSICS

» *Determine if any countermeasures, such as encryption, were enabled during the breach*

» *Analyze all data sources to ascertain what information was compromised*

STEP 4

IDENTIFY LEGAL OBLIGATIONS

» *Revisit state and federal regulations that apply and then determine all entities that need to be notified*

» *Ensure all notifications occur within any mandated timeframes*

STEP 5

REPORT TO UPPER MANAGEMENT

» *Generate reports that include all the facts about the breach, as well as the steps and resources needed to resolve it*

» *Create a high-level overview of priorities and progress, as well as problems and risks*

STEP 6

IDENTIFY CONFLICTING INITIATIVES

» *Determine if any upcoming business initiatives may interfere or clash with response efforts*

» *Decide whether to postpone these efforts and for how long*

STEP 7

EVALUATE RESPONSE AND EDUCATE EMPLOYEES

Once an incident is resolved, evaluate how effectively your company managed its response and make any necessary improvements to your preparedness plan. Taking time to reflect and make these adjustments will ensure a smoother response in the future. Use the incident as an opportunity to retrain employees not only in their specific response roles when a breach occurs, but also in their own security & privacy practices. For instance, recent Ponemon reports found that only 26 percent of companies conduct security training courses annually[23] and 60 percent of companies do not require employees to retake courses, missing an opportunity to emphasize security best practices.[24]

[23] Fourth Annual Study: Is Your Company Ready for a Big Data Breach? Ponemon Institute, 2016
[24] Managing Insider Risk Through Training & Culture, Ponemon Institute, 2016

Responding to a data breach

Managing communications & protecting reputation

Along with the direct financial impact of security incidents, the potential loss of reputation and customer loyalty pose a major risk to organizations. As such, it is essential that companies are prepared with the right communication strategies and understand best practices well ahead of an incident.

Managing communications during a data incident

While early planning is essential to successfully managing a security incident, organizations must keep in mind data security incidents always include unexpected twists and are very fluid. Amidst the accompanying swirl of rumors and misinformation surrounding an incident, companies must understand that investigating a data breach and communicating facts properly takes time.

Although incident response planning is not one-size-fits all, the following are key principles to live by:

» *Assume that news of the incident will be leaked before your organization has all the details, and have a plan in place to address questions early in the process*

» *Focus initial holding statements on steps being taken to investigate the issue and resist speculating on details about the breach prior to a forensics investigation*

» *If your organization is committed to providing identity protection if an incident is confirmed, consider mentioning that in the statement*

» *Establish traditional and social media monitoring to detect leaks and understand how your incident is being framed by external stakeholders*

» *When more information is available, establish a consumer-centric website regarding the incident that provides details about what happened and steps individuals can take to protect themselves*

» *Communicate with the appropriate regulators early and transparently to avoid potential scrutiny*

» *Ensure front line employees have the information they need to communicate to their customers and make sure they know to route any media requests directly to the incident response team*

Responding to a data breach

Protecting legal privilege

The likelihood of class action lawsuits following a breach is at an all-time high. It's almost like clockwork. A company discloses a data breach, and within days, there are class action lawsuits filed. Given the risk of litigation is very high, it is essential to take steps to protect legal privilege of the response process.

While you should consult your outside counsel when deciding the approach to maintaining privilege, the following are good general rules:

- *Ensure that all written materials, including emails are marked "privileged and confidential" and that someone from the legal department is included on the distribution*
- *All contracts for external partners should be arranged through outside counsel so that their work is part of the course of providing legal counsel to your organization*
- *Be thoughtful about what information you are documenting or is being put in writing versus what should be discussed in-person or on a call*

It's important that your general counsel

send out guidelines for protecting privilege

at the very start of the incident as the initial forensics investigation starts.

Responding to a data breach

Taking care of your consumers

Typically, when required by law to notify affected individuals of a data breach, companies have 60 days to do so. However, depending on a variety of circumstances (such as locations affected), you may have even less time as the countdown starts the moment a breach is discovered. In 2016, the average time from discovery until notification was 41 days.[25] A separate 2017 study found that in the case of international data breaches, the notification timeline is even worse with 57 percent of impacted companies taking at least two months to notify victims.[26] With the EU's GDPR in place, this will simply not be an option moving forward.

Not all breaches require a notification.

If your data was encrypted or an unauthorized employee accidentally accessed but didn't misuse the data, you may not need to notify.

Notification

It is your responsibility to determine the deadlines for notification according to state law. To help minimize that stress, determine how you'll handle notifications before a breach occurs.

There are a host of challenges that may impact your notification process. The following are just a few:

- *Certain state laws and federal regulations shrink the timeline to 30 or 45 days, leaving you little time to verify addresses, send out notification letters and set up a call center*
- *Some states mandate specific content for you to include in your notification letters. Make sure you know what they are*
- *Notification may be delayed if law enforcement believes it would interfere with an ongoing investigation*
- *Multiple state and global laws may apply to a data breach depending on where the affected individuals reside, as opposed to where the business is located*
- *If some affected individuals live in a state or country that mandates notification and others live in a state or country that doesn't, you should notify everyone*
- *Be aware that some recipients will think the notification letter itself is a form of scam*

Identity theft protection

Consumers will expect a remedy from the breached organization; a 2014 study found that 63 percent of affected victims want identity theft protection,[27] and these numbers are likely rising. From 2015 to 2016, the percentage of individuals redeeming complimentary credit monitoring and identity theft protection after a breach increased from 10 percent to 26 percent.[28] While there are many identity protection and credit monitoring providers in the marketplace, some of these providers are only proficient in one area of the full identity protection spectrum. When selecting a protection product for the affected breach population, organizations should have a strong understanding of the various product features and capabilities.

A comprehensive protection product should, at a minimum, include access to:

- *Consumer credit reports*
- *Credit monitoring*
- *Social security number (SSN) monitoring*
- *Dark web and internet records scanning and alerts*
- *Fraud resolution services*
- *Identity theft insurance*

What is the difference between identity theft protection and credit monitoring services?

Identity protection includes credit monitoring, along with several other methods for finding stolen information and resolving potential issues. Credit monitoring is a major component of identity protection because it can detect and notify key financial changes, including new account openings, delinquencies and address changes. Identity protection takes this a step further by providing other types of monitoring.

[25, 28] Be Compromise Ready: Go Back to the Basics, 2017 Data Security Incident Response Report, BakerHostetler. [26] Data Protection Risks & Regulations in the Global Economy, Ponemon Institute, 2017. [27] Aftermath of a Mega Data Breach: Consumer Sentiment, Ponemon Institute, 2014

Auditing your plan

Auditing your plan

Once you've created your preparedness plan, you've cleared one of the biggest hurdles in positioning your organization for success.

Still, your plan will always work best if it's current and up to date. Every quarter, make it a priority to audit and test your plan. Think about the different scenarios that could occur and whether your plan would help address each one, including an internal breach, external attack, accidental data sharing and loss or theft of a physical device. Also, continue to update your plan based on new, unforeseen threats that may emerge in the months and years ahead.

Update, audit and test your plan

every quarter to ensure a successful response.

Areas to focus on

Here are just a few key elements that should be on your radar during a preparedness plan audit.

Call center

Preparing your call center representatives when a data loss incident arises or onboarding external resources to help manage the high volume of calls is critical. When a breach is discovered, the last thing you should do is hide from or alienate your consumers. Instead, be readily available to answer their questions in order to reinforce the value of your brand and your commitment to their continued security.

Whether you use internal or external resources, you should be able to:

- ***Swiftly pull together training materials:*** *Informed and empathetic call center representatives can make a positive impact on your brand during a crisis*
- ***Scale the call center component:*** *You need to be able to adapt to any type of breach, large or small*
- ***Conduct ongoing crisis training for your call center:*** *Make sure your representatives are thoroughly trained to handle sensitive information and emotional callers*
- ***Test, test some more and test again:*** *Conduct regular test calls to ensure the call center is ready to handle incident-related calls*

Vendor negotiations

Since many companies are victimized by data security breaches at the hands of their vendors (15 percent of network attacks in 2016 succeeded due to vendor "wrongdoing"[29]), take extra caution to select vendors that have appropriate security measures in place for the data they will process. Then, take it a step further by contractually obligating your vendors to maintain sufficient data safeguards and assessing their performance in meeting contract requirements on a regular basis.

Make sure your vendors:

- *Maintain a written security program that covers your company's data*
- *Only use your customer data for the sole purpose of providing the contracted services*
- *Promptly inform you of any potential security incidents involving company data*
- *Comply with all applicable data security laws*
- *Return or appropriately destroy company data at the end of the contract*

[29] Be Compromise Ready: Go Back to the Basics, 2017 Data Security Incident Response Report, BakerHostetler

Auditing your plan

Preparedness Audit Checklist

Auditing your preparedness plan helps ensure it stays current and useful. Here are several recommended steps for conducting an audit, but we recommend you tailor your audit process to fit the scope of your company's unique response plan.

UPDATE YOUR TEAM CONTACT LIST

- Check that contact information for internal and external members of your breach response team is current and remove anyone who is no longer linked to your organization
- Provide the updated list to the appropriate parties

VERIFY YOUR PLAN IS COMPREHENSIVE

- Update your plan - as needed - to account for any major company changes, such as recently established lines of business, departments or data management policies
- Verify each response team member and department understands his/her role during a data breach

DOUBLE CHECK YOUR VENDOR CONTRACTS

- Ensure you have valid contracts on file with your forensics firm, data breach resolution provider and other vendors
- Verify your vendors and contracts still match the scope of your business

REVIEW NOTIFICATION GUIDELINES

- Ensure the notification portion of your response plan takes into account the latest legislation and update your notification letters, if needed
- Ensure your contact information is up to date for the attorneys, government agencies or media you will need to notify following a breach

REVIEW WHO CAN ACCESS YOUR DATA

- Assess whether third parties are meeting your data protection standards and ensure they are up to date on any new legislation
- Healthcare entities should ensure business associate agreements (BAAs) are in place to meet Health Insurance Portability and Accountability Act (HIPAA) requirements

EVALUATE IT SECURITY

- Ensure proper data access controls are in place
- Verify that company-wide automation of operating system and software updates are installing properly and backup tapes are stored securely

REVIEW STAFF SECURITY AWARENESS

- Ensure everyone on staff is up to date on proper data protection procedures, including what data, documents and emails to keep and what to securely discard
- Verify employees are actively keeping mobile devices and laptops secure onsite and offsite and changing passwords every three months

Helpful resources

Helpful links

Better Business Bureau/Data Security
www.bbb.org/data-security

Data Breach Today
www.databreachtoday.com/resources

Department of Health and Human Services
www.hhs.gov

Federal Trade Commission
www.ftc.gov/idtheft

Identity Theft Resource Center
www.identitytheft.org

InfraGard
www.infragard.org

International Association of Privacy Professionals
www.privacyassociation.org

Medical Identity Fraud Alliance
www.medidfraud.org

National Conference of State Legislatures
www.ncsl.org

Online Trust Alliance
www.otalliance.org

Experian links

Experian Data Breach Resolution
www.Experian.com/DataBreach

Online Resource Center
www.Experian.com/databreachresources

Perspectives Newsletter
www.Experian.com/DataBreachNews

Blog
www.Experian.com/DBBlog

LinkedIn
www.linkedin.com/company/data-breach-resolution

Twitter
www.Twitter.com/Experian_DBR

ABOUT EXPERIAN DATA BREACH RESOLUTION

Experian Data Breach Resolution, powered by the nation's largest credit reporting agency, is a leader in helping businesses plan for and mitigate consumer risk following data breach incidents. With more than a decade of experience, Experian Data Breach Resolution has successfully serviced some of the largest and highest-profile breaches in history. The group offers swift and effective incident management, notification, call center support, and reporting services while serving millions of affected consumers with proven credit and identity protection products. Experian Data Breach Resolution is active with the International Association of Privacy Professionals, the Health Care Compliance Association, the American Health Lawyers Association, the Ponemon Institute RIM Council, and InfraGard and is a founding member of the Medical Identity Fraud Alliance. For more information, visit experian.com/databreach.