DATA BREACH RESPONSE GUIDE

By Experian® Data Breach Resolution

2015-2016 Edition

FOREWORD

It has been quite a year for data breaches, to say the least. A number of 'mega' breaches have changed the way companies approach data security and how consumers react to organizations that have exposed their personal information, forever.

This evolution can be viewed as a good thing as the threat of a breach has always been present, just put on the back burner among other technology and security priorities.

Now that the issue is front and center for businesses and consumers, companies are forced to face it head on and prepare accordingly knowing it is a major reputational risk along with, potentially, huge financial fallout.

We have seen preparedness levels certainly increase as a Ponemon Institute study in 2014 showed 73 percent of companies have a response plan in place and 48 percent increased investments in security technologies. However, what we also found is that while there is greater awareness and preparation for a breach, companies are not practiced. They are not implementing security trainings for employees or performing breach plan evaluations and drills on an ongoing basis, which is necessary to ensure a smooth response. Yet, the study findings showed that 77 percent of respondents believe more drills would help them be more prepared. This is why we updated our guide this year to include an entire section about practicing the response plan.

For those who are just getting started or need to audit their existing plan, we have covered preparedness from soup to nuts here as well. We want this guide to be a useful tool for every organization looking to improve their security posture because the potential for a data breach is not going away so the sooner an organization gets ready the better.

Sincerely,
Michael Bruemmer
Vice President
Experian Data Breach Resolution

TABLE OF CONTENTS

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.

INTRODUCTION

SINCE 2005, MORE THAN 786 MILLION RECORDS HAVE BEEN COMPROMISED AS THE RESULT OF A DATA BREACH.*

It's certainly no longer a secret that large-scale data breaches are happening with regularity, and at a higher frequency. Businesses across the globe recognize that, today, no company is safe.

According to a report published by the Identity Theft Resource Center (ITRC), there were 783 reported data breaches in 2014 across all industries, which impacted more than 85 million consumer records. This year, as of July 28, 2015, there have already been 450 recorded data breaches, with more than 135 million exposed records – far more than all of last year.*

The average cost of a data breach is also on the rise. According to its annual Cost of a Data Breach Study, the Ponemon Institute found that the average consolidated total cost of a data breach is $3.8 million, which represents a 23 percent increase since 2013.**

It goes without saying that, with statistics such as these, 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 – and those who have – this Guide illustrates how to best create, implement and refine a comprehensive data breach response plan for the security challenges that lie ahead.

Identity Theft Resource Center: 2015 Data Breach Category Summary

Report Date: 9/1/2015

Totals for Category:	# of Breaches	% of Breaches	# of Records	% of Records
Banking/Credit/Financial	51	9.6%	411,569	0.3%
Business	212	39.8%	915,671	0.7%
Educational	45	8.4%	740,700	0.5%
Government/Military	40	7.5%	28,194,728	20.1%
Medical/Healthcare	185	34.7%	109,744,263	78.4%
Totals for All Categories:	**533**	**100%**	**140,006,931**	**100%**

Total Breaches: **533** | Records Exposed: **140,006,931**
2015 Breaches Identified by the ITRC as of: **9/1/2015**

*Identity Theft Resource Center, 2015, **2015 Cost of a Data Breach Study: Global Analysis, Ponemon Institute & IBM, 2015

COMMUNICATING TO THE C-SUITE

COMMUNICATING TO THE C-SUITE

THE SUCCESS OF ANY DATA BREACH RESPONSE PLAN BEGINS WITH CLOSE INVOLVEMENT FROM THE EXECUTIVE TEAM.

Without engagement and support from board-level executives, developing and maintaining an effective plan can pose a significant challenge for any organization.

However, by illustrating some of the severe implications of a data breach – such as heavy costs and damage to a company's reputation and brand – managers can gain the support at the highest levels of the organization in fairly short order.

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

17%	Senior executives currently not aware of whether or not their organization had suffered a data breach in the last year*	77%	Suggested more firedrills to practice data breach response would help them be more prepared*
43%	Organizations that indicate they do not have training and awareness programs for employees and other stakeholders who have access to sensitive or confidential personal information*	40 Billion	U.S. company losses from unauthorized use of computers by employees last year*
59%	Security incidents in the last year caused by employees and employee negligence, yet they remain the least reported issue*	$217	The average cost for each compromised record containing sensitive and confidential information increased with the total average cost rising to $6.5 million***
69%	Indicated additional funding as a major need to improve response activity*	$184-$330 Million	Average loss in brand value, depending on the information lost as a result of the breach**
70%	Executives who want more oversight and participation from board members, the chairman and CEO when it comes to data breach preparedness*	1 Year	Average time to restore an organization's reputation after records containing confidential customer information are lost or stolen**

*Is Your Company Ready for a Data Breach?, Ponemon Institute, 2015
**Reputation Impact of a Data Breach Study, Ponemon Institute, 2011, ***2015 Cost of a Data Breach Study, Ponemon Institute, 2015

CREATING YOUR PLAN

CREATING YOUR PLAN

ASSEMBLE YOUR BREACH RESPONSE TEAM TO ENSURE END-TO-END PREPAREDNESS.

Start With a Bullet-Proof Breach Response Team

A data breach can take a heavy toll on any business – large or small. Having a breach preparedness plan 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.

When you discover a data breach, it is not the time to decide who will be responsible for leading and managing the incident. It's critical to assemble your response team before you need them. This group will play an important role in coordinating efforts between your company's various departments.

Your internal breach response team should include the following:

Incident Lead

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

- Manage and coordinate your company's overall response efforts and team
- 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

Public Relations

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

- Identify the best communications strategy and tactics to announce the breach to media and stakeholders
- Track and analyze media coverage and quickly respond to any negative press during a breach

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

Start With a Bullet-Proof Breach Response Team (Cont'd)

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

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

Information Technology (IT)

IT and security teams will likely lead the way in catching and stopping a data breach, as well as:

- 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

SECURE EXTERNAL PARTNERS EARLY SO THEY ARE READY WHEN YOU NEED THEM.

Engage Your External Partners

Identifying partners and securing pre-breach agreement contracts with them beforehand is crucial – not only to help you be prepared but also so you won't be slowed with cost negotiations in the middle of your response. As expected, 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 those who have no relationships with influencers, which can lead to significant risk when managing a breach.

What is a Pre-Breach Agreement?

It's a contract with a partner, executed before a data breach occurs, that establishes the relationship so the partner is ready to take action the moment you need them.

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 and comprehensive fraud resolution, and secure call center services

Forensics

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

- Advise your organization with 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

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 to best position the incident to key audiences and help manage media questions related to the issue

Legal Counsel

While many organizations already have in-house legal counsel, it's important to seek outside help with specialized skills in data breach response. Legal partners should preferably have an established relationship with local regulatory entities such as the state attorney general to help bridge the gap when communicating with them following a breach. Further, they should have an understanding 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 Attorney Generals/Regulators

It is important to establish relationships early with state attorney generals and other regulatory entities to streamline the response process and timeline in the event of a breach. 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. Be sure to collect appropriate contact information now so you can act quickly when needed. This includes local and state bodies and the FBI. They will:

- Look for evidence that a crime has been committed
- Sometimes be the one to inform the company that they have had a breach unbeknownst to the company prior

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 a breach may initially seem small as to the amount of data and/or people affected, after the investigation it can be discovered to be much larger.

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.

Consider Cyber Insurance

Given the flurry of new state and federal regulations governing how and when customers must be notified of a breach, the risk of reputational damage from a mishandled breach is significant. With comprehensive cyber insurance coverage from a reputable provider, organizations can properly prepare themselves for a potentially damaging breach event.

Last year, we predicted that this component of corporate security would grow significantly. In one of the few reports out about cyber insurance, a 2013 Ponemon Institute study showed that roughly 30 percent of respondents had cyber insurance coverage. In the same study, another 30 percent said they would be adding coverage over the next 12 months.* While this trend should not be interpreted as companies waving the white flag at protecting against security threats, it does demonstrate the need to think beyond the traditional technology-centric “castle and moat” strategy.

What are the benefits of cyber insurance? For one, companies with insurance often have a stronger security posture. Plus, a breach event is often smoother operationally for them because a pre-breach plan is already in place. When a plan is in place and successfully executed, the average cost of the response can be up to 25 percent lower.

What Breach Expenses Does it Cover?

In general, it can cover the notification costs to data breach victims, legal costs and forensics and investigative costs. It may also include identity protection and credit monitoring services for breach victims. While this is a good benefit of the coverage and wise investment by the organization because it will help protect the company’s reputation and rebuild the relationship with their customers.

Selecting Legal Partners

From a legal standpoint there are several nuanced characteristics that should be taken into account. These are a few considerations to keep in mind:

» Law firms that have both previous experience managing data breach litigation and that have established relationships with local regulators such as the state attorneys general are ideal

» They should be able to provide insights about the latest developments in case law, which should inform the counsel involved across the board

» 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.

*Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age, Ponemon Institute, 2013

Incorporating PR and Communications

It's also important to ensure that communications is incorporated into the broader incident response process. 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.

Key Elements

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
- **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
- **Cover all audiences –** Ensure your Plan accounts for communicating to your employees, customers, regulators and business partners
- **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 attorney generals

ENGAGE WITH THE RIGHT RESOURCES, BOTH DOMESTIC AND ABROAD, AS EARLY AS POSSIBLE.

Handling Global Breaches

It’s clear that more U.S. organizations are now better prepared for a data breach than in previous years. However, many still don’t understand the sensitivities of responding to a breach that occurs overseas. As the economy becomes more globalized, the odds of experiencing an international data breach are now higher than ever. According to a recent survey by PricewaterhouseCoopers, the total number of security breaches worldwide rose to nearly 43 million in 2014, an increase of 48 percent over the prior year.

Preparing for an international incident, which can be far more complex than a domestic breach, is essential. A global breach can involve multiple languages, varying notification laws and, most importantly, a variety of diverse cultures and differing views of privacy, as evidenced by the European Union pushing for stricter standards.

Prepare Your Organization

The following are ways to prepare if your organization has an international footprint:

- Develop a roster of attorneys in your countries who are familiar with existing local breach notification laws
- Consider the need to engage a local public relations consultant should a breach occur
- Assess if you need local call centers who are familiar with local sentiment regarding privacy issues
- Ensure your notification partner can handle multi-language letters

PRACTICING YOUR PLAN

PRACTICING YOUR PLAN

ESTABLISH A SCHEDULE INVOLVING ALL DEPARTMENTS TO PRACTICE ON A REGULAR BASIS.

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 completion of 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, and perform regular reviews to ensure you're ready.

Responsibility of Your Team

Make sure everyone on your data breach response team understands their 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 that are updated regularly and communicated to all business associates
- Investing in the proper cyber security software, encryption devices and firewall protection
- Updating these security measures regularly
- Limiting the type of both hard and electronic data someone 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/retraining at least once a year

PRACTICING YOUR PLAN

Implementing a Simulation Exercise

The incident response plan should not just be a binder that sits on a shelf. Conducting a breach simulation exercise is an effective way to replicate the challenges of a breach. In doing so, you can quickly expose areas of weakness or gaps in your playbook that should be addressed. Where to start?

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

Schedule a healthy amount of time

Give yourself plenty of time (2-4 hours) to conduct the exercise and discuss the challenges experienced

Include everyone

Include all team members – both internal and external – who will be involved in responding to a data breach

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

Debrief after the exercise

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

Conduct drills every 6 months

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

Who Should Be Involved:

» CIO, CISO or other chief executives

» IT

» Legal

» Public Relations

» Human Resources

» Risk & Compliance

» Customer Service

» Outside partners (legal counsel, public relations firm, data breach resolution provider)

SAMPLE EXERCISE

Developing a Training Module

If you're able to dedicate a half-day for a training exercise, it's ideal to address two different scenarios. Both should be pertinent to your industry and the type of data your company stores. However, each need not be 100% realistic and can allow for a degree of imagination. They will still hone response skills while giving participants the opportunity to be creative.

Possible general scenarios to start with can include:

- The FBI has contacted your company. They state that they suspect a user on the dark web is in possession of payment card data of your customers. They recommend investigating the matter.
- A blogger who writes about security posts a story that reliable sources have shared that there is personal identifiable information of your employees for sale on the dark web. Several news outlets are picking up on the news and posting stories.
- A company vendor that handles your customer data contacts your company that they suspect they have been breached and are investigating. They are not divulging any information, citing a forensics investigation and legal counsel.

? Questions

When addressing these situations, ask questions such as:

- Who are the first leaders to be notified?
- How would you classify the severity of this issue?
- Should you contact the local authorities?
- When do you notify the CEO and board?
- When would you activate the external partners?
- How will you respond to mainstream media inquiries?
- Do you consider reaching out to state and/or federal officials?

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 employees, customers, etc. in place to activate quickly?

» 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)?

» 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?

» Have you conducted employee training to apply security best practices in the last 12 months?

Experian®

RESPONDING TO A DATA BREACH

RESPONDING TO A DATA BREACH

ACT FAST. THE FIRST 24 HOURS FOLLOWING A BREACH ARE CRITICAL.

The First 24 Hours

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, who it was reported to, 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 protocols –** 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
9. **Bring in your forensics firm –** Begin an in-depth investigation
10. **Notify law enforcement –** Do this if needed, after consulting with legal counsel and upper management

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

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 3

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 4

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 5

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 6

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

Managing Communications & Protecting Reputation

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

While advance 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 about it 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 should an incident be confirmed, consider mentioning that in the statement
- Establish traditional and social media monitoring to detect a leak 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 people 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

While news of a data breach is likely to cause some damage to brand and corporate reputation, executing a strong communications plan can greatly reduce it.

By: Leigh Nakanishi is a vice president in Edelman's Seattle office and leader of the firm's global Data Security and Privacy team.

Taking Care of Your Consumers

Typically, when required by law to notify affected individuals of a data breach, they have 60 days to do it. However, depending on a variety of circumstances, you may have even less time as the countdown starts the moment a breach is discovered.

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.

Challenges:

» 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 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 that mandates notification and others live in a state that doesn't, you should notify everyone

» Be aware that some recipients will think the notification letter itself is a form of a scam

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.

Identity Theft Protection

Consumers expect a remedy from the breached organization with a 2014 study showing that 63 percent want identity theft protection.* While there are many identity protection and credit monitoring providers in the marketplace, some of these providers are only capable 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

» Fraud Resolution Services

» $1 Million Identity Theft Insurance

Customers that aren't provided all of these capabilities by the breached organization are often on their own to find out if their identity has been stolen or if someone has opened a new account in their name. The best way to know this activity has occurred in a timely fashion is with an identity protection product that monitors credit reports and alerts the individual if there is something new on their report.

What Is The Difference Between Identity Theft Protection and Credit Monitoring Services?

Identity theft protection should offer a number of different features which includes credit monitoring. It is an entire suite of services. Credit monitoring is one function that monitors an individual's credit report and sends alert notifications to that person if there is activity on their credit report.

*Aftermath of a Mega Data Breach: Consumer Sentiment, Ponemon Institute, 2014

Experian®

AUDITING YOUR PLAN

AUDITING YOUR PLAN

UPDATE, AUDIT AND TEST YOUR PLAN EVERY QUARTER TO ENSURE A SUCCESSFUL RESPONSE.

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 is 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.

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.

Activities Should Include:

- **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 of your response effort –** 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, 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

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 take into account 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 state 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

- Review how third parties are managing your data and if they 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 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.idtheftcenter.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

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

Blog
www.Experian.com/DBBlog

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.