

Data Breach Response Guide

By Experian® Data Breach Resolution
2014-2015 Edition



Experienced Trusted Comprehensive



Foreword

According to a recent data breach preparedness study by the Ponemon Institute, much has changed in the world of data breaches in the past year – some are positive, others a bit more challenging. It's no secret that, according to the study, many more companies suffered a data breach in 2013 versus the year before. To date, nearly half of organizations have experienced at least one breach incident that impacted personal records – an increase of 10% from 2013 – and 17% were unsure if they had been victimized.

Fortunately, more companies are answering the call by taking basic steps to prepare themselves for the increasing likelihood of a breach. A majority of them (73%) now have a data breach response plan in place and nearly half have notched up their investment in security technologies in the past 12 months.

Still, it's clear that businesses need to do more than simply checking the box of establishing an incident response plan. They need to take action to test their plans, practice them regularly, and improve their plan on a continual basis. In other words, they can't afford to just let it sit on a shelf. Case in point, most of the study's respondents (78%) haven't or don't regularly update their data breach response plan to account for changing threats or their own evolving company processes.

In short, vigilance is key. The more organizations can do to prepare themselves – by developing and maintaining a comprehensive data breach response plan – the better off they will be in the months and years to come. This Guide is designed to help them do just that.

Sincerely,

Michael Bruemmer

Vice President, Experian Data Breach Resolution



© 2014 Experian Information Solutions, Inc. All rights reserved. Experian and the marks used herein are service marks or registered trademarks of Experian Information Solutions, Inc. Other product and company names mentioned herein may be the trademarks of their respective owners.

Table of Contents

Understanding Data Breaches	4
The Evolving Landscape	5
The Data Breach Response Plan	6
Prepare	
Creating Your Plan	7
Implement	
Responding to a Data Breach	9
Notifying Data Breach Victims	12
Managing Communications	15
Managing Global Breaches	17
Improve	
Auditing Your Plan	18
Selecting the Right Resolution Partner	20
Helpful Resources	22
Appendix	23



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.

Understanding Data Breaches

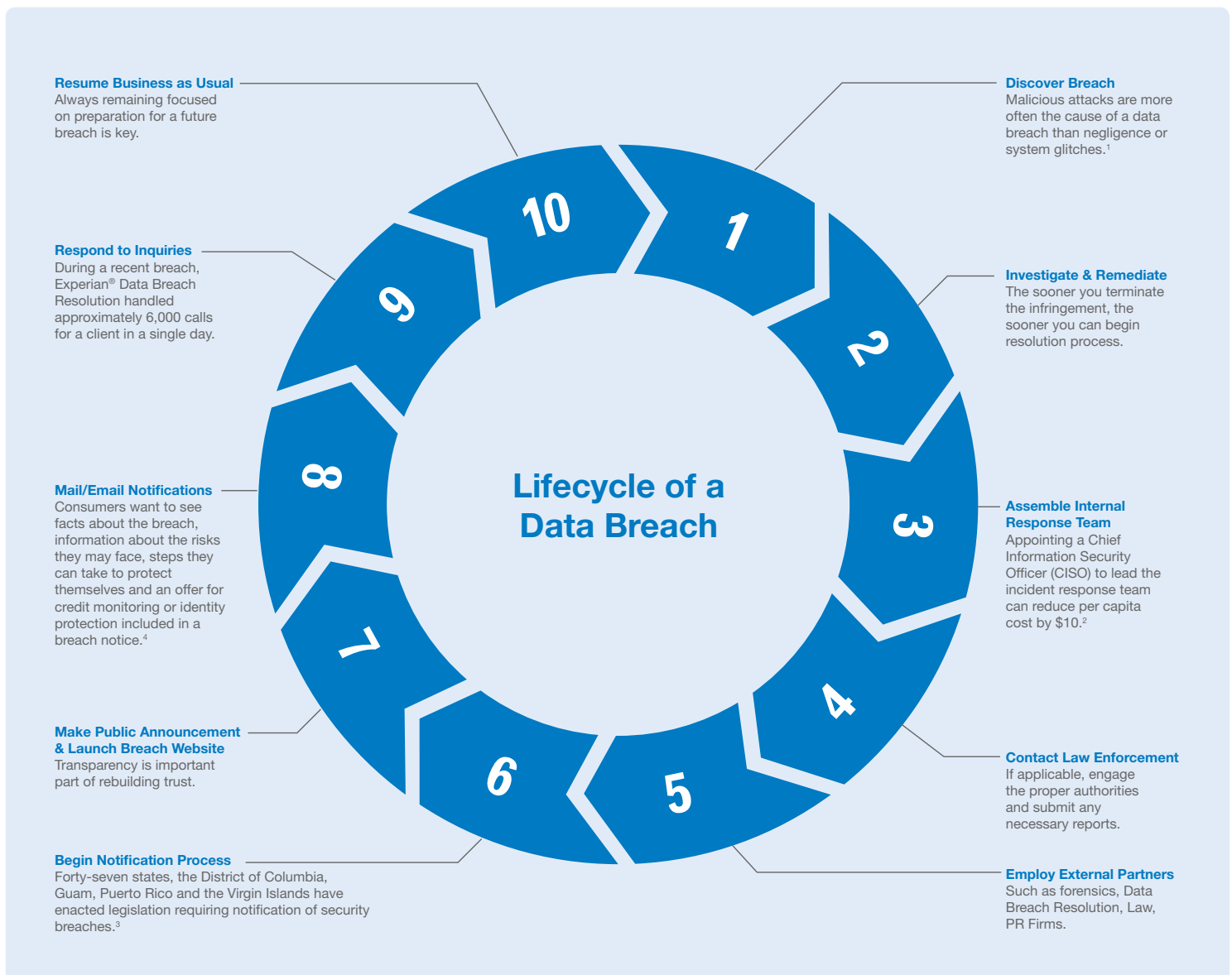
The Purpose of this Guide

Experian's Data Breach Response Guide is designed to provide organizations with information, insight and tools to help them better understand the growing data breach epidemic, defend against data breaches and, if and when they encounter one, safely navigate the resolution process.

This Guide offers an overview of the current data breach landscape, including current legal and technological developments, as well as information on why it's important to have an incident response plan, and how to create, implement and improve it.

You will discover what you need to do in the first 24 hours after a data breach, how to notify your customers, patients or employees, why communicating with the media is so important, and suggested steps for creating, implementing and improving a data breach response plan.

So please, take time to review this guide, and if you don't have an incident response plan, use this resource to help you create one. It could mean the difference between a breach that causes a brief disruption and one that causes a major meltdown.



¹ 2011 Cost of a Data Breach Study: United States, Symantec Corp. and Ponemon Institute.

² 2011 Cost of a Data Breach Study: United States, Symantec Corp. and Ponemon Institute.

³ Congressional Research Service Report for Congress, 2012

⁴ Consumer Study on Data Breach

The Evolving Landscape

Legal Issues

The current regulatory framework in the United States does not provide for a national uniform data breach notification standard. Instead, businesses are guided by a patchwork of existing laws in 47 states, the District of Columbia, Puerto Rico and the Virgin Islands. In fact, only three states do not have such laws. They are Alabama, New Mexico and South Dakota. In addition to the existing body of state laws, two sector-specific Federal laws — HIPPA and GLBA — govern breaches of health related and financial data. The Federal Trade Commission has also used its authority under Section 5 of the FTC Act to take enforcement actions related to data security. This regulatory structure makes compliance complex, and creates an incentive for a company to have a breach notification strategy and plan in place before a breach occurs.

A National Breach Notification Law?

Congress continues to debate and move toward enactment of a national data breach standard to replace the patchwork of state and sectoral laws, but progress has been slowed for various reasons. In fact, data breach was top of mind for policymakers during a series of Congressional hearings throughout the year and more than seven breach notification bills were proposed and considered during Committee hearings. However, despite the apparent increase in support for a data breach bill, lawmakers continue to have trouble avoiding pitfalls that plagued past efforts to pass a national breach notification law. In particular, this can be attributed to a lack of consensus on specific issues related to the pre-emption of state laws, the types of personal information that, if breached, would trigger notification, jurisdictional issues among Congressional committees, and attempts to conflate data breach

legislation with other more contentious issues — like general consumer privacy or data broker regulation.

Technology Considerations

The evolution of certain technologies is also shaping the world of data breaches, both in terms of how they impact the scope of a breach and how they help organizations protect themselves from damage. Two of the more prominent developments are the emerging threat posed by cloud technologies and the growth of encryption technologies.

The Global Cloud

The data breaches of tomorrow are likely to be global in nature, adding significant complexity to the data breach response process. With the rise of cloud computing, significant quantities of sensitive data now travel across national borders in the blink of an eye. Large data centers host data from citizens all over the world. Yet, while these data flows are global, the data breach laws and cultural norms for responding to an incident are local. This makes responding properly to a large breach a significant compliance challenge.

Notifying individuals and providing some form of identity protection in multiple countries may be increasingly complicated. With the European Union likely to pass more stringent regulations, the frequency of reported international data breaches is likely to explode in the near future. The biggest challenge for companies will be keeping up with each country's regulations and maintaining compliance with all of them.

Encryption is Critical

While encrypting internal and traveling data may be expensive and time-consuming,



it's clearly a worthwhile undertaking for organizations, especially in light of increasing data breaches and federal government scrutiny. Organizations should also keep up with IT security and install the latest software to protect their systems, but technology alone is not the answer. Numerous breaches are, in fact, caused by insiders. In these cases, an employee purposely steals sensitive consumer data or carelessly opens a link and infects his or her company's systems. As a result, it is always a good practice to establish procedures for safeguarding consumer data and limiting access to that data to staff members who truly need it to perform their job effectively.

The Data Breach Response Plan



Why Create a Response Plan?

According to a survey conducted by the [Ponemon Institute](#), the average total cost of data breaches for U.S. companies grew to \$5.9 million in 2014 from \$5.4 million the previous year. Similarly, the average cost for each stolen or lost record rose to \$201. Of course, when millions of records are involved, some breaches end up costing much more than that. That's why it's critical to be prepared for the worst.

In the end, a data breach can take a heavy toll on companies of all sizes. Having a breach preparedness plan in place can help you act quickly if one is encountered by your organization, which can help you prevent further data loss, and avoid significant fines and costly customer backlash.



Look to C-level executives to make data breach preparedness a continuing priority for the entire company.

Incident Preparedness

After a data breach has been discovered is not the time to decide how you're going to respond or who will be responsible for addressing the many challenges it poses. It's critical to develop your response plan and build your response team well before you need them.

Your team will play an important role in coordinating efforts between your company's various departments, fulfilling two primary functions:

1. The immediate function is to develop the data breach response plan and prep the entire organization on proper protocol during a breach.
2. Then, if a breach does occur, the team will implement the response plan, engage the proper resources and track the efforts.

A Comprehensive Approach

Because a typical data breach involves a long list of moving parts, many of which need to be addressed simultaneously, it's best to establish a response plan that takes into account every scenario and responsibility that could come into play. This includes assembling a strong internal response team, interfacing with government or law enforcement agencies, notifying victims, communicating with the media, responding to customer inquiries and repairing customer loyalty.

Secure a Proven Breach Resolution Partner

The quickest – and often more effective – way to develop a breach response plan is to retain the services of a breach resolution partner. However, it's critical to choose yours wisely. Many data breach resolution providers specialize in a specific aspect of resolving a data breach, but only a few offer the breadth of services and proven expertise to address every point along the resolution lifecycle. To ensure yours is a truly comprehensive plan and response, do your due diligence and secure a resolution partner who can support all your needs.

A comprehensive data breach response plan includes a variety of specific elements and covers a wide range of disciplines. Still, a well-constructed data plan, no matter how comprehensive and detailed, is only as good as the team that's responsible for putting it into action.

Assemble Your Response Team

Assembling a complete team comprised of strong, capable representatives will go a long way toward ensuring an efficiently executed response. Your Breach Response Team should include the following constituents:

Incident Lead

Start by selecting your incident lead, which would typically come from an internal or external legal department or a Chief Privacy Officer. Your incident lead should be able to:

- 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.
- Identify key tasks, manage timelines and document every response effort from start to finish.
- Outline the budget and resources needed to respond to a breach.

- Ensure contact lists remain updated and team members are ready to respond.
- Analyze response efforts post-breach to better prepare for the next incident.



Your incident lead, as well as every response team member, needs a backup.

Here is a quick look at the other members you will want on your team and what their responsibilities might entail:

Executive Leaders

Include the company's key decision makers as advisors to your data breach response team to help ensure you have the needed leadership, backing and resources to properly develop and test your plan.



Creating Your Plan Continued

Information Technology & Security

Your IT and security teams will likely lead the way in catching and stopping a data breach but not necessarily in investigating it. You'll want someone from IT and/or security on your response team to:

- 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 & Privacy

Rely on internal and/or external legal, privacy and compliance experts to shape your data breach response and help minimize the risk of litigation and fines. Your legal representatives will need to:

- Determine how to notify affected individuals, the media, law enforcement, government agencies and other third parties, such as card holder issuers, if needed.
- Establish relationships with any necessary external counsel before a breach occurs.
- Review and stay up to date on both state and federal laws governing data breaches in your industry.



Outline a structure of internal reporting to ensure executives and everyone on the response team is up to date and on track during a data breach.

Public Relations

Depending on the size of the data breach and your industry, you may need to report the breach to the media and/or notify affected individuals. Your response team member from PR or communications will need to:

- Identify the best notification and crisis management tactics before a breach ever occurs.
- Handle any information leaks regarding a breach.
- Track and analyze media coverage and quickly respond to any negative press during a breach.

Customer Care & Human Resources

Data breaches may affect both your customers and your employees so appoint representatives from both customer service and HR to your response team to provide needed support. Your internal representatives should:


- Create simulation training for your customer service representatives that demonstrates how their roles would change during a data breach.
- Outline a plan for setting up a data breach hotline for customers and/or employees if a breach occurs. Determine in advance if you'll use internal or external resources.

Law Enforcement

Depending on the severity of a data breach, you may need to involve law enforcement. Take time to collect all of the appropriate contact information now so you can act quickly if a breach does occur.

- Identify which state and federal authorities, including the FBI and Secret Service, to contact in the event of a data breach involving criminal activity.
- During a breach, be sure everyone on the data breach response team is aware of any law enforcement directives so the investigation isn't interrupted.

Creating Your Plan Continued

 Clearly defined steps, timelines and checklists help keep everyone focused during the stress of a data breach.

Data Breach Resolution Provider

Contract with a data breach resolution partner in advance of a breach to benefit from their strategic expertise in preparing for a breach. Your provider should be able to:

- Assign you a dedicated account manager to handle escalations, tracking and reporting.
- Handle all aspects of notification, including drafting, printing and mailing letters and address verification.
- Offer proven identity protection and comprehensive fraud resolution, and secure call center services for all affected individuals.


Conduct Preparedness Training

In addition to a company-wide focus on data security and breach preparedness, department-specific training should trickle down from the data breach response team. Each member of the team has a responsibility to apply prevention and preparedness best practices to his/her own department.

- Work with employees to integrate smart data security efforts into their daily work habits.
- Develop data security and mobile device policies, update them regularly and communicate them to all business associates.
- Invest in the proper cyber security software, encryption devices and firewall protection. Update these security measures regularly.
- Limit the type of both hard and electronic data someone can access based on their job requirements.
- Establish a method of reporting for employees who notice that others aren't following the proper security measures.

- Conduct employee security training/re-training at least once a year.

While your data breach response team coordinates your preparedness and response efforts, everyone in your company plays a role in data security. Therefore everyone should be involved in data breach preparedness.

 Practice and test your preparedness plan, and perform regular reviews to ensure you have everything covered.

Prepare for the Worst

Prepare for the worst so you can respond at your best. Make sure everyone on your data breach response team understands their specific responsibilities – both in preparing for and responding to a breach.

Responding to a Data Breach

IMPLEMENT

Acting quickly 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

Once you've discovered a data breach, respond quickly and don't panic. Immediately contact your legal counsel for guidance on initiating these 10 critical steps:

- Record the date and time when the breach was discovered, as well as the current date and time when response efforts begin, i.e. when someone on the response team is alerted to the breach.**
- Alert and activate everyone on the response team, including external resources, to begin executing your preparedness plan.**
- Secure the premises** around the area where the data breach occurred to help preserve evidence.
- 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.
- Document everything** known thus far about the breach: Who discovered it, who reported it, to whom was it reported, who else knows about it, what type of breach occurred, what was stolen, how was it stolen, what systems are affected, what devices are missing, etc.
- Interview those involved** in discovering the breach and anyone else who may know about it. Document your investigation.
- Review protocols** regarding disseminating information about the breach for everyone involved in this early stage.
- Assess priorities and risks** based on what you know about the breach.
- Bring in your forensics firm** to begin an in-depth investigation.
- Notify law enforcement**, if needed, after consulting with legal counsel and upper management.

 In a recent survey, 38% of respondents felt their organization is prepared to respond to a data breach.¹

¹ "Second Annual Study on Data Breach Preparedness," Ponemon Institute, 2014

Responding to a Data Breach Continued



Any data breach could lead to litigation. Work closely with your legal and compliance experts to analyze risks and ways to mitigate them, such as proper documentation and notification.

Next Steps

Once you have completed the 10 initial steps, take inventory of your progress to ensure your preparedness plan is on track. Then, continue with these next steps:

Fix the Issue that Caused the Breach

- Rely on your forensics team to delete hacker tools.
- Determine if you have other security gaps or risks and address them.
- Put clean machines online in place of affected ones.
- Ensure the same type of breach cannot happen again.
- Document when and how the breach was contained.

Continue Working with Forensics

- Determine if any countermeasures, such as encryption, were enabled when the compromise occurred.
- Analyze backup, preserved or reconstructed data sources.
- Ascertain the number of suspected people affected and the type of information that was compromised.
- Begin to align compromised data with customer names and addresses for notification.

Identify Legal Obligations

- Revisit state and federal regulations governing your industry and the type of data lost.
- Determine all entities that need to be notified, i.e. customers, employees, the media, government agencies, regulation boards, etc.
- Ensure all notifications occur within any mandated timeframes.

Report to Upper Management

- Compile daily breach reports for upper management.
- The first report should include all of 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.

Responding to a Data Breach Continued

💡 Never send sensitive information, such as SSNs, unnecessarily to vendors supporting the breach.



Identify Conflicting Initiatives

- Make the response team and executives aware of any upcoming business initiatives that may interfere or clash with response efforts.
- Decide whether to postpone these efforts and for how long so you can focus your efforts on the breach.

Alert Your Data Breach Resolution Vendor

- Contact your pre-selected vendor to choose business services for your company and protection products for individuals affected in the breach.
- Determine how many activation codes you will need for the protection products based on the number of affected individuals.
- Draft and sign a data breach resolution agreement if you do not have a pre-breach agreement in place.
- Engage your vendor to handle notifications (learn more in the next section: Notifying Databreach Victims) and set up a call center so affected individuals have access to customer service representatives trained on the breach.
- Work closely with your account manager to review incident reporting and metrics.

Keep Your Response Efforts on Track

Resolving a data breach requires a coordinated effort between your response team members, executives, external resources, law enforcement, forensic firm and data breach resolution vendor. Staying organized and documenting every step and decision should be a top priority. Act quickly to minimize the damage but don't lose sight of your priorities or of the needs of affected individuals.

Notifying Data Breach Victims

IMPLEMENT

Typically, businesses have 60 days to notify affected individuals of a data breach when notification is required by law. However depending on varying circumstances, you may have even less time. The countdown starts the moment a breach is discovered.

Notification Challenges

Your legal counsel should determine if the following challenges – as well as any others – may impact your notification process:

- Certain state laws and federal regulations shrink the timeline to 30 or 45 days, meaning there's no time to waste in verifying addresses; writing, printing and mailing notification letters; and setting up a call center and other services for affected individuals.
- Some states mandate specific content for you to include in your notification letters. This can include toll-free numbers and addresses for the three major credit bureaus, the Federal Trade Commission and a state's attorney general.
- Notification may be delayed if law enforcement believes it would interfere with an ongoing investigation.
- Multiple state laws may apply to one data breach because jurisdiction depends on where the affected individuals reside, not 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 so you're not singled out for showing inequality.
- Keep in mind that some recipients will think the notification letter itself is a form of scam.

Mishandling notifications can lead to severe consequences, including fines and other unbudgeted expenses. It could also tarnish your brand reputation and customer loyalty, leading to potential revenue loss.

Organizations can improve the outcome of a data breach if they contract with external resources ahead of time. That way, if a breach does occur, you would already have a forensics partner, a privacy attorney and a breach notification partner ready to hit the ground running.

Successful 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. Lining up a data breach resolution provider in advance can help shave off both time and stress from your response efforts. In many cases, you can even save money by signing a contract with a provider before a breach happens to you.

💡 What you say, how you say it and when you say it are all important elements of data breach notification.



What Your Breach Resolution Partner Should Do

Above all, your data breach resolution provider should make security a top priority throughout the notification process. Unlike standard direct mail production, data breach notification requires critical service and quality assurance elements to ensure compliance. Look for one vendor that can seamlessly handle notifications from beginning to end and make a positive impact on your brand.

Account Management

Your vendor should assign an experienced account manager to your breach to help streamline and simplify the notification process. Your account manager should know the ins and outs of your breach, your priorities and your

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.

Notifying Data Breach Victims Continued

deadlines. That can only happen if you have an assigned, dedicated account manager. Otherwise you'll waste valuable time working with a different account manager every time you call.

Critical Notification Services

A full-service data breach resolution vendor should offer a range of options, as well as strict security standards, to fit your business needs and the scope of your breach. These include the following:

Comprehensive letter management

- Templates for you to customize to your company and breach
- Management of multiple letter versions based on state regulations, affected individuals (employee vs. consumer audience), etc.
- Four-color or black-and-white letters
- Professional printing with your company logo and electronic signature



Notification letters may contain sensitive data and require secure handling through every stage of drafting, printing and mailing.

Address validation & delivery

- Return mail management to securely handle and discard any returned notification letters

- Certified address cleansing confirmed against USPS standards
- Coding accuracy support system – address standardization
- Delivery point validation – validate address exists
- Locatable address conversion system – update address
- National change of address verified by the US Postal Service
- Deceased and criminal identification to minimize unnecessary mailings
- First-class postage

Quality assurance for printing and fulfillment

- Dedicated quality assurance personnel
- Robust integration controls to ensure 100% produced and mailed
- Tier-1 data security protocols along with a secure/restricted access production area
- Ongoing training and certification of personnel
- 24/7 camera monitoring with secure digital archiving

Reporting for compliance

- Daily inventory reporting
 - Initial mailings
 - Address changes
 - Undeliverable and returned letters
- Electronic letter copies for proof of notification
- US Postal Service postal delivery report

As dictated by state law, a notification letter should include:

- ▶ Clear language, not industry jargon, that the average person could understand.
- ▶ A toll-free phone number for individuals wanting additional information.
- ▶ Details about the type of data lost and how it was lost, unless prohibited by law.
- ▶ Next steps to help affected individuals regain their security, such as signing up for a complimentary identity protection product.

Notifying Data Breach Victims Continued

Ten Steps: Working with a DB Resolution Partner

1. Vendor assigns a dedicated account manager and conducts kickoff meeting
2. Client selects products and services and signs a data breach resolution agreement
3. Vendor provides samples of notification letters and options for a variety of consumer protection products
4. Client provides final data files and letter materials
5. Vendor aligns affected individuals with addresses and generates applicable product activation codes
6. Vendor preps call center using incident-specific FAQs
7. Client and vendor jointly approve final letter
8. Vendor oversees mailing, delivery and re-mailing from secure fulfillment center
9. Vendor provides regular reporting and metrics to client to track engagement
10. Client identifies affected individuals, determines notification requirements & contacts vendor

💡 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. Be sure to seek and follow legal advice before deciding to forego notification.



Legal Notice: Always check with your legal counsel in order to identify the notification requirements for your specific incident.

Keys to Successfully Managing the Communications Impact of a Data Security Incident

BY [David Chamberlin](#) & [Leigh Nakanishi](#)

The rash of high-profile data breaches that have dominated the news in recent months worry a growing number of companies, as they should. Boards are now responding seriously to the issue, with a clear eye to the significant reputational risk that can have on the bottom line. The criminal activity shows no signs of abating, despite the heightened attention of policymakers and regulators. According to the [Symantec's Internet Security Threat Report 2014](#) (disclosure: Edelman client), 552 million identities were exposed in data-breach incidents across various sectors in 2013 and the average number of records exposed per breach is up more than 2.6 times from last year.

Despite the ugliness, some valuable learnings have resulted about how best to respond to the onslaught of media and customer attention a company faces during a major incident.

Lesson No. 1: Ensure communications is integrated into planning

Benjamin Franklin's famous maxim, "An ounce of prevention is worth a pound of cure," couldn't be more appropriate in business today. If companies haven't done the necessary preparation, they burn the time the team just doesn't have in the heat of the moment.

It's essential that communications is involved in all aspects of data breach planning to ensure proper alignment of this key function. Often companies will have

a technical incident response team and plan, but it is not closely integrated with the communications function within the organization, as it should be.

To truly get ahead, incident response teams should take the following steps to effectively integrate communications:

1. Develop a communications incident response process and plan that clearly outlines who will be responsible for developing and approving the key messages that will be communicated to media, as well as internal audiences.
2. Ensure that the communications plan

includes drafts of key media materials that will be useful during an incident. While the particular fact patterns of an incident will have a significant influence over final versions of communications documents, having an agreed upon place to start will help reduce churn and potential for mistakes. Documents you need to draft should include:

- Holding statements for media for a variety of breach scenarios
- Q&A covering likely questions from media, financial stakeholders and customers



Managing Communications Continued

- Letter from company leadership to be shared with customers
 - Key messages document
 - Customer web portal to post information when available.
3. Conduct a data breach crisis communications simulation to test how effectively your breach will likely be managed.
 4. Media train key spokespeople on how they would likely respond to questions related to a security incident.
 5. Identify and vet an outside public relations firm with specific expertise in data breaches to be your partner during an incident.

Lesson No. 2: Be lean, yet integrated

Determine who's on the team – and the team leader with the authority to make decisions about press statements and media strategy – and keep it as small as possible. In most cases, the essential individuals are represented by the heads of IT, security, legal, communications, the business lead and, perhaps, the CEO. The same should be the rule for outside advisors. Doubling up on outside advisers or bringing in new players midstream will only hinder the response and distract you from keeping your customers as your primary concern.

Lesson No. 3: Be prepared for a fluid situation

Companies need to realize data security incidents always include twists. What they think they know invariably turns out later to be inaccurate and, if communicated, may cause significant legal liability issues. While rumors and misinformation will swirl, companies must understand investigating

a data breach and communicating about it properly takes time.

“In major breaches, it can take a month or two of round-the-clock work to answer: How did the attackers get in and when? What did they view? What did they steal? Are they still in there?” explains [Eric Friedberg](#), executive chairman of [Stroz Friedberg](#), a digital forensics firm. If you must communicate something, say what you know, acknowledge what you don't know and continue to keep people updated.

To deal with this, companies must be diligent to resist communicating numbers early in an investigation and be careful about claiming the issue is fully resolved too soon. While a company is likely to receive scrutiny in the media for taking longer to provide more details about an incident, this type of negative attention is easier to manage than communicating misinformation.

Lesson No. 4: Manage the message

Communicating the right messages at the proper points in the lifecycle of a breach will have a significant impact on how a breach is reported. While developing messages should not be one-size-fits all, the following are key principles to live by:

1. Focus initial messages on the steps being taken to investigate the issue and frame it as a criminal issue.
2. Think through what you push out and how to respond via social channels. There's no need to have a public debate in front of millions of followers.
3. Set up the appropriate media/social monitoring and listening posts to see how the breach is being covered.
4. Customers must be your north star, so make sure that you communicate with them clearly and effectively through traditional and digital channels.



5. However, don't neglect the wide variety of stakeholders interested in breaches including policymakers, regulators (state and federal) and industry stakeholders (eg. payment brands).

While taking these steps won't fix all of the problems, it will significantly lessen the pain once the issue surfaces and allow the company to focus on the problem at hand.

[David Chamberlin](#) is the executive vice president and general manager of [Edelman's Dallas office](#), and the leader of the firm's global [Data Security and Privacy team](#). [Leigh Nakanishi](#) is a vice president in [Edelman's Seattle office](#) and a senior data privacy and security strategist on the firm's global [Data Security and Privacy team](#).

Managing Global Breaches

IMPLEMENT

While more U.S. organizations may be better prepared for a data breach than in previous years, they may not know how to respond when a breach occurs overseas. As the economy becomes more globalized, the odds of experiencing an international data breach are now higher than ever. There were 2,164 global breaches reported in 2013 alone – exposing 822 million records, according to the Open Security Foundation and Risk Based Security.

For today's global organizations, 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.



Engage with the right resources ahead of time, both domestic and abroad.

Engaging Resources Abroad

When working in a foreign country, it is crucial for companies to secure an attorney who is familiar with existing local breach notification laws. An organization will benefit from expert counsel on not only the political climate surrounding privacy issues, but also current and proposed legislation in the affected region. Some countries have specific laws while others provide only suggested guidelines related to breaches.

Similarly, a company may also need to engage a local public relations consultant and nearby call centers who are familiar with local sentiment regarding privacy issues. Many countries don't have the "breach fatigue" that's growing in the U.S., so foreign residents may feel more alarmed in the event their information is compromised.

A local public relations or crisis management partner can properly advise an organization on how much information to release and when to release it to the public. Plus, local call centers can hire people who speak the native language and can relate better to residents. Securing these resources ahead of time enables companies to avoid the frantic scramble to find them when crisis hits.

Expect the Unexpected

Preparing for an international breach is similar to preparing for a natural disaster. Companies should brace for the worst case scenario and focus on protecting their most valuable asset – their customers.

Legal partners play an important role throughout the data breach incident response and, as more breaches cross borders, their global expertise will become even more crucial.

In the end, it all comes down to securing the right resources ahead of time that can help you navigate the complexities of a far-reaching breach, whether it's contained within domestic borders or bleeds overseas.



Once you've created your preparedness plan, you've cleared one of the major hurdles in setting up your organization for success if a data breach occurs. But your preparedness plan can only help you succeed if it's comprehensive and current. Each quarter, make it a priority to update, audit and test your plan. Consider 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.

Most Overlooked Details

Here's a glimpse of a few commonly overlooked details that should be on your radar during a preparedness plan audit.

Call Center

Getting your call center up to speed on a data loss incident or bringing external resources on board to help handle the high volume of calls is an important part of data breach preparedness. In the time following a data breach is not when you want to 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.



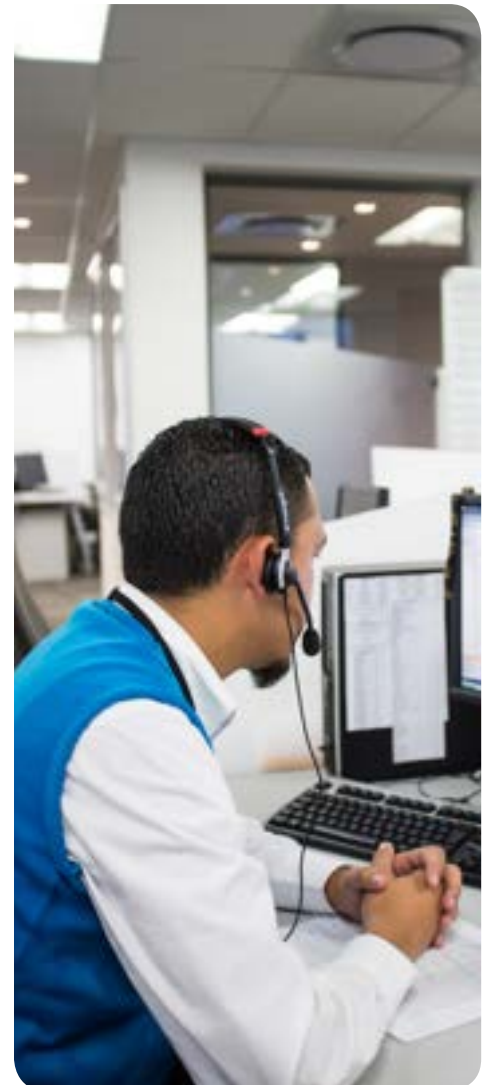
Always seek advice from legal and compliance when drawing up vendor contracts, especially ones involving data management or transfer.

Whether you plan to use internal or external resources, be sure you:

- Are prepared to swiftly pull together training materials, such as incident FAQs. Highly knowledgeable and emphatic call center representatives can make a positive impact on your brand during a crisis.
- Are able to scale the call center portion of your preparedness plan to fit any incident. In addition to identifying needed call center resources in advance of a breach, also create a call center script template specifically geared toward crisis management.
- Conduct ongoing crisis training for your regular call center, whether it's internal or external, so representatives are trained in handling sensitive information as well as emotional callers.
- Oversee several test calls to confirm the call center is ready to handle incident-related calls.

Vendor Negotiations

With companies being plagued by data security breaches at the hands of their



Auditing Your Plan Continued

vendors, take steps to ensure your company isn't headed down the same road. 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. Assess whether they are meeting the contract requirements on a regular basis.

In general, it makes sense for companies to require that vendors:

- Maintain a written security program that covers the company's data.
- Only use the company's customer data for the sole purpose of providing the contracted services.
- Promptly notify the company of any potential security incidents involving company data and cooperate with the company in addressing the incident.
- Comply with all applicable data security laws.
- Return or appropriately destroy company data at the end of the contract.



Audit your preparedness plan immediately after a data breach so you can clearly remember what went wrong and what went right.

Operational Challenges

So you've determined all of the steps and precautions you'll need to take if a data breach occurs. But, responding to one can take significant company resources. Does your preparedness plan address the operational challenges of managing a breach in conjunction with managing day-to-day business?

For example, if your head of security and/or IT is tied up with breach response, who oversees the department in the meantime? Answering questions like these truly helps to illustrate that data security, data breach preparedness and data breach response requires a true company-wide awareness and involvement.



As part of your preparedness plan, have every member of the response team prep their departments on what to expect and how to operate during data breach response. Everyone on staff should understand how their roles might change during a breach in order to maintain smooth operations.

Preparedness Audit Checklist

Auditing your preparedness plan helps ensure it stays current and useful. Here are several recommended steps you may want to take, but be sure to tailor your audit to fit the full scope of your company's individual response plan. Once you've created your preparedness plan, you've cleared one of the major hurdles in setting up your organization for success if a data breach occurs. But your preparedness plan can only help you succeed if it's comprehensive and current. Each quarter, make it a priority to update, audit and test your plan. Consider 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 the loss or theft of a physical device.

Auditing Your Plan Continued

- | | | |
|--------------------------|--|------------------|
| <input type="checkbox"/> | Update data breach response team contact list <ul style="list-style-type: none">• Check that contact information for internal and external members of your breach response team is current.• Remove anyone who is no longer with your company or with an external partner and add new department heads.• Re-distribute the updated list to the appropriate parties. | Quarterly |
| <input type="checkbox"/> | Verify your data breach response plan is comprehensive <ul style="list-style-type: none">• 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 its role during a data breach. Create example scenarios for your response team and departments to address. | Quarterly |
| <input type="checkbox"/> | Double check your vendor contracts <ul style="list-style-type: none">• 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. | Quarterly |
| <input type="checkbox"/> | Review notification guidelines <ul style="list-style-type: none">• Ensure the notification portion of your response plan takes into account the latest state legislation.• Update your notification letter templates, as needed, to reflect any new laws.• Verify your contacts are up to date for the attorneys, government agencies or media you will need to notify following a breach.• Healthcare entities need to ensure they have the proper Department of Health & Human Services contacts and reporting process in place. | Quarterly |
| <input type="checkbox"/> | Check up on third parties that have access to your data <ul style="list-style-type: none">• Review how third parties are managing your data and if they are meeting your data protection standards.• Ensure they are up to date on any new legislation that may affect you during a data breach.• Verify they understand the importance of notifying you immediately of a breach and working with you to resolve it.• Healthcare entities should ensure business associate agreements (BAAs) are in place to meet HIPAA requirements. | Quarterly |
| <input type="checkbox"/> | Evaluate IT Security <ul style="list-style-type: none">• Ensure proper data access controls are in place.• Verify that company-wide automation of operating system and software updates are installing properly.• Ensure automated monitoring of and reporting on systems for security gaps is up to date.• Verify that backup tapes are stored securely. | Quarterly |
| <input type="checkbox"/> | Review staff security awareness <ul style="list-style-type: none">• 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.• Review how to spot and report the signs of a data breach from within everyday working environments.• Verify employees are actively keeping mobile devices and laptops secure onsite and offsite and changing passwords every three months. | Yearly |

A data breach is a challenging experience which can have negative long-term effects for all parties involved. Your business may deal with loss of revenue from customer turnover and brand mistrust for an extended period of time. Plus, individuals affected by the data breach have a higher risk of experiencing identity theft, which may follow them for the rest of their lives, depending on the information that is compromised.

With comprehensive data breach resolution, businesses can protect their business interests and the personal identities of affected individuals all at once. This would address both your need for quick data breach resolution and your customers' demand for extended data breach protection to help you maintain your brand integrity and customer loyalty.

The Right Resources

Look for a partner that offers a turn-key approach that includes incident management, data breach notification and reporting, as well as identity protection and call center support for your customers.

Incident Management

The right resources and experience to keep your data breach resolution on track.

- Dedicated Account Manager
An assigned, experienced Account



Manager to help guide you through every aspect of your data breach resolution, and provide an implementation checklist so you know what to expect during each phase of the resolution process.

- Incident Response Education
The way you communicate internally and externally about a data breach can impact your brand integrity and resolution efforts. Your partner should train your key staff members on addressing the breach and preparing for situations that may arise.

Data Breach Notification

Your partner should help you act quickly to notify affected individuals within the timeframe of any federal data breach laws or state data breach laws pertaining to your unique incident.

- Effective Notification Letters
Request a notification letter template for you to customize and use to mail your choice of a four-color or black-and-white data breach notification letter, as well as resend any letters returned due to incorrect addresses.



Secure a data breach resolution partner that employs a truly comprehensive approach.

- Address Verification
Obtain current and appended addresses, as well as research addresses for incomplete records. This is an important step to help ensure you reach the right individuals in a timely manner.

Identity Protection Products

A data breach puts your customers at higher risk of identity theft. By offering them a protection product, you can help them maintain their security and continued peace of mind.

Selecting the Right Resolution Partner Continued

There are many identity protection and credit monitoring providers in the marketplace that a breached company may choose to work with. Some of these providers, however, are only capable in one area of the full identity protection spectrum. This means that you may be receiving a product that does not fully protect you.

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
- Internet Scanning

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 your credit report and alerts you if there is something new on your report.

Call Center Support

Call center services should serve the individuals affected by a data breach with the following.

- **Easy Enrollment**
A partner can assign a unique, toll-free number your customers can use to enroll in their protection product and develop scripting related to your specific incident to remind your customers that you are providing this protection product as a special precaution for them.
- **Daily Customer Service**
Customer service should be available seven days a week to ensure your customers have the identity protection support they need, and help escalate a case to a fraud resolution specialist when it's necessary.
- **Customized FAQs**
A partner should provide its Call Center with a list of FAQs regarding the data breach so their team can answer questions your customers might have regarding the incident. This eliminates the need for you to use internal resources for communicating with individuals affected by the breach.

Incident Reporting

Make sure your partner can provide the tracking and reporting you need to monitor your data breach resolution, report back to your key stakeholders and comply with state and federal regulations.

- **Escalation Reporting**
You will need timely updates on the status of any escalated concerns that your organization submits to Experian.
- **Notification Metrics**
Stay informed about the results of our data breach notification process, including the number of notices sent, received and returned.
- **Enrollment Metrics**
Request reports on enrollment numbers as individuals sign up for the identity protection product you have provided. Be sure the partner can track both online and offline enrollments.
- **Call Center Metrics**
You should track daily call volume, type of calls, speed of answer and other metrics so you can monitor the efficiency of the Call Center and your customers' use of the protection product.



Helpful Resources

Helpful Links

National Conference of State Legislatures

www.ncsl.org

Identity Theft Resource Center

www.idtheftcenter.org

Federal Trade Commission

www.ftc.gov/idtheft

Department of Health and Human Services

www.hhs.gov

Medical Identity Fraud Alliance

www.medidfraud.org

InfraGard

www.infragard.org

International Association of Privacy Professionals

www.privacyassociation.org

Online Trust Alliance

www.otalliance.org

Data Breach Today

www.databreachtoday.com/resources

Better Business Bureau/Data Security

www.bbb.org/data-security

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

Twitter

www.Twitter.com/Experian_DBR

Experian® Data Breach Resolution

☎ 866-751-1323

🌐 www.Experian.com/DataBreach

✉ databreachinfo@experian.com



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. In 2013, Experian Data Breach Resolution received the Customer Service Team of the Year award from the American Business Awards. 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 InfraGuard and is a founding member of the Medical Identity Fraud Alliance. For more information, visit databreachinfo@experian.com.

The word 'Experian' is a registered trademark in the EU and other countries and is owned by Experian Ltd. and / or its associated companies.