Data Breach Response Guide

By Experian® Data Breach Resolution

2018-2019 Edition

Foreword

Data breaches are on the rise: in 2017, 5,207[1] incidents were reported worldwide, and 1,579[2] originated in the U.S. alone. Given this environment, it's critical for businesses and consumers alike to take cyber security seriously.

Every day, organizations continue to battle sophisticated cybercriminals who continuously evolve their tactics and techniques to access and profit from valuable, sensitive information. Regardless of your organization's size, the threat of a data breach continues to increase. While the number of data breaches making headlines seems to have quieted in comparison to last year's avalanche of highly-publicized events, this decrease doesn't equate to a safer cyber environment. Instead, it suggests cybercriminals are growing more advanced in their ability to access sensitive materials undetected.

Ensuring you have the right people and processes in place before an attack occurs can make a significant difference in how an attack impacts your company's operations, reputation and bottom line. When your organization experiences a data breach, time is of the essence. The longer it takes for your organization to respond after an attack, the bigger the hit to your company's reputation and customers' loyalty. By acting swiftly and strategically, your company can get back to business as usual.

There is room for growth when it comes to preparing for a breach. Despite the increased risks around of a breach and the emphasis these risks put on preparation, Experian's 2017 Annual Data Breach Preparedness Study found just 19 percent of employees thought their organization's data breach response plan was highly effective. Additionally, only 31 percent of respondents were confident in their organization's ability to recognize and minimize spear phishing incidents, while even fewer (21 percent) were confident in their organization's ability to deal with ransomware. With a growing number of organizations have a data breach response plan in place (88 percent),[3] it's clear that the majority of companies want to be prepared but understanding the infusing industry best practices is critical for an effective plan.

It's vital for organizations to take the initiative and prepare for the inevitable. Regardless of where your organization falls on the preparedness scale, there's never been a more important time to boost your efforts.

The likelihood of a data breach will only continue to climb, but the measures you put in place today can greatly minimize the damage and disruption to your organization. This guide is intended to be a useful tool and resource for any organization looking to improve its cyber security and preparedness efforts. Data breach preparedness is no longer optional in our current threat landscape – your customers, reputation and future demand you take steps to formulate a concrete response plan today.

Sincerely,
Michael Bruemmer
Vice President
Experian Data Breach Resolution

[1] 2017 Year End Data Breach Quick View Report, Risk Based Security, 2018
[2] ITRC Data Breach Report 2017, Identity Theft Resource Center, 2017
[3] Fifth Annual Study: Is Your Company Ready for a Big Data Breach? Ponemon Institute, 2018

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.*

When a company experiences a data breach, the effects are felt far beyond the walls of the tech and security teams.

From legal to customer service to the executive team, every employee should be aware of and prepared to participate in a robust data breach response plan. Last year, the Identity Theft Resource Center (ITRC) reported the number of U.S. data breach incidents hit a new record high of 1,579, which is a drastic upturn (44.7 percent) from 2016. This year, as of July 2, there have been 688 data breaches exposing more than 22 million records.[4]

With data breaches becoming a regular occurrence, response plans are a critical component of any business's cyber security strategy. For companies who are just starting to think about developing a plan or for those looking to update current practices, this guide illustrates what a comprehensive data breach response plan should look like and how to implement one in a way that meets the security challenges that lie ahead.

Since 2005, more than 1,104,625,430 records have been compromised as the result of a data breach.[4]

Identity Theft Resource Center: 2018 Data Breach Category Summary

Report Date: 7/2/2018

Totals for Category:	# of Breaches	% of Breaches	# of Records	% of Records
Banking/Credit/Financial	84	12.6%	1,705,354	7.6%
Business	309	46.3%	15,213,588	67.9%
Educational	45	6.7%	642,270	2.9%
Government/Military	49	7.3%	1,598,501	7.1%
Medical/Healthcare	181	27.1%	3,248,545	14.5%
Totals for All Categories:	**668**	**100.0%**	**22,408,258**	**100.0%**

Total Breaches: **668** | Records Exposed: **22,407,258**

2018 Breaches Identified by the ITRC as of: **7/2/2018**

[4] 2018 Data Breach Stats, Identity Theft Resource Center

Keeping Pace with Cybercriminals

Ransomware

Ransomware is the top variety of malicious software, found in 39 percent of cases where malware was identified.[5]

The world of cybersecurity is ever-changing.

New threats appear on a daily basis and cybercriminals continuously escalate their techniques and capabilities. If you're finding it difficult to keep up with the ever-evolving threat landscape, you're not alone – seven out of 10 organizations report their security risk increased significantly last year.[6]

Tactics and Techniques

While developments in artificial intelligence (AI) and machine learning (ML) enable cybersecurity professionals to predict and identify potential threats, these technologies present a double-edged sword as more and more hackers leverage them to create more sophisticated attacks. With the help of AI and ML, cybercriminals can enhance traditional hacking techniques like phishing scams or malware attacks.

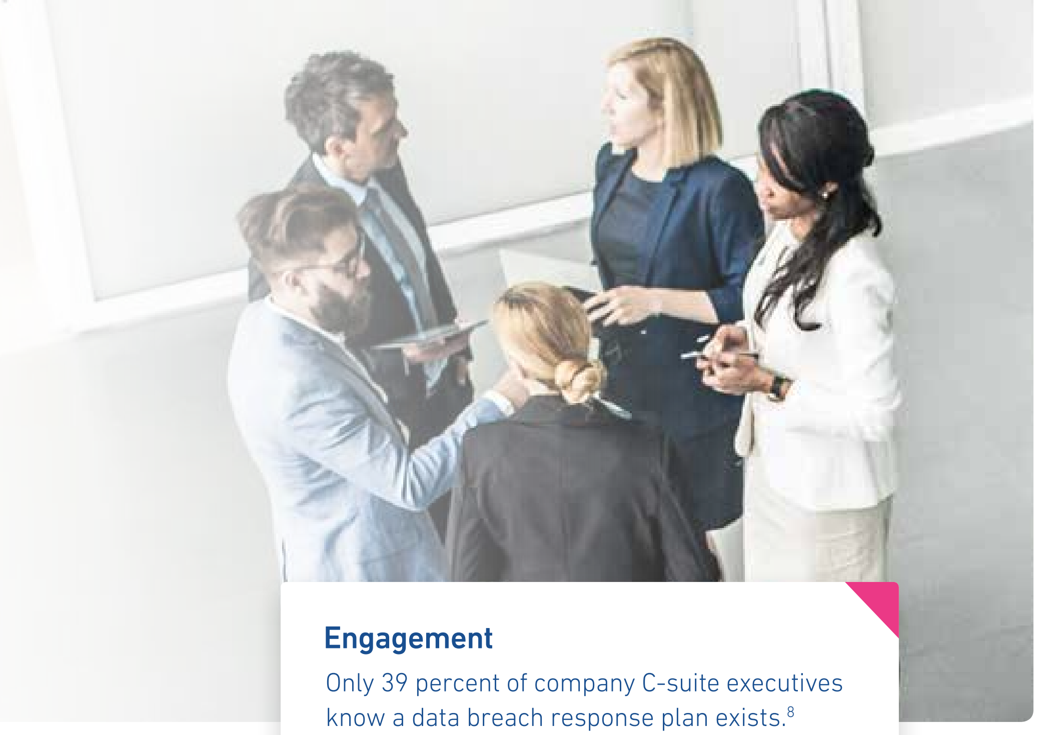
For example, cybercriminals could use AI and ML to make fake emails look more authentic and deploy them faster than ever before, causing more extensive damage to a broader group of people. Cybercriminals are also taking advantage of the rise of Bitcoin, which has given way to a new kind of threat-cryptomining malware. Whether in the form of drive-by mining attacks or scams used to access cryptowallets, cybercriminals are taking every opportunity to exploit the rising value and popularity of cryptocurrencies.

While cryptomining is becoming increasingly popular, cybercriminals still depend heavily on tried and true hacking methods, such as malware and spear phishing, which continue to grow in scale and sophistication. Recently, we've also seen an uptick in fileless attacks, which avoid the use of malicious executables and are more successful at bypassing security measures than traditional, file-based attacks. In fact, fileless attacks are 10 times more likely to succeed than file-based attacks.[7]

While anticipating the next approach cybercriminals will take is nearly impossible, we can look to previous and current trends to get an idea of what to expect in the months and years to come. It's important to remember that while technology advances security measures, cybercriminals can also harness it with malicious intent. Any data breach preparedness program should be updated regularly to accommodate threat changes and risks.

[5] 2018 Data Breach Investigations Report, Verizon, 2018
[6] 2017 Cost of Data Breach Study, Ponemon Institute, 2017
[7] The 2017 State of Endpoint Security Risk, Ponemon Institute, 2018

Engaging the C-Suite



Engagement

Only 39 percent of company C-suite executives know a data breach response plan exists.[8]

The involvement of the executive team greatly determines the success of a data breach response plan.

Lack of leadership engagement in the creation and implementation of a response plan can cause organizations significant challenges in creating a culture of cyber security.

Despite the importance of their involvement, most boards of directors, chairmen and CEOs are not actively engaged and often avoid responsibility in data breach preparedness. Less than half of employees (48 percent) say C-suite executives are informed and knowledgeable about how their companies plan to respond to a data breach. Further, only 40 percent of organizations claim their boards understand their specific security threats.[9]

Organizations can help get buy-in and involvement from the C-suite by clearly illustrating the impact a data breach can have on a company's financial and reputational standing. When working to gain the support of your company's leadership, consider these data points:

$148:
The average cost per lost or stolen record[10]

145,927,550: Number of records compromised in 2017 due to employee negligence or error[11]

$14: Average cost savings per record with an incident response team[10]

$3.86 million:
The average cost of a data breach[12]

[8] Fifth Annual Study: Is Your Company Ready for a Big Data Breach? Ponemon Institute, 2018

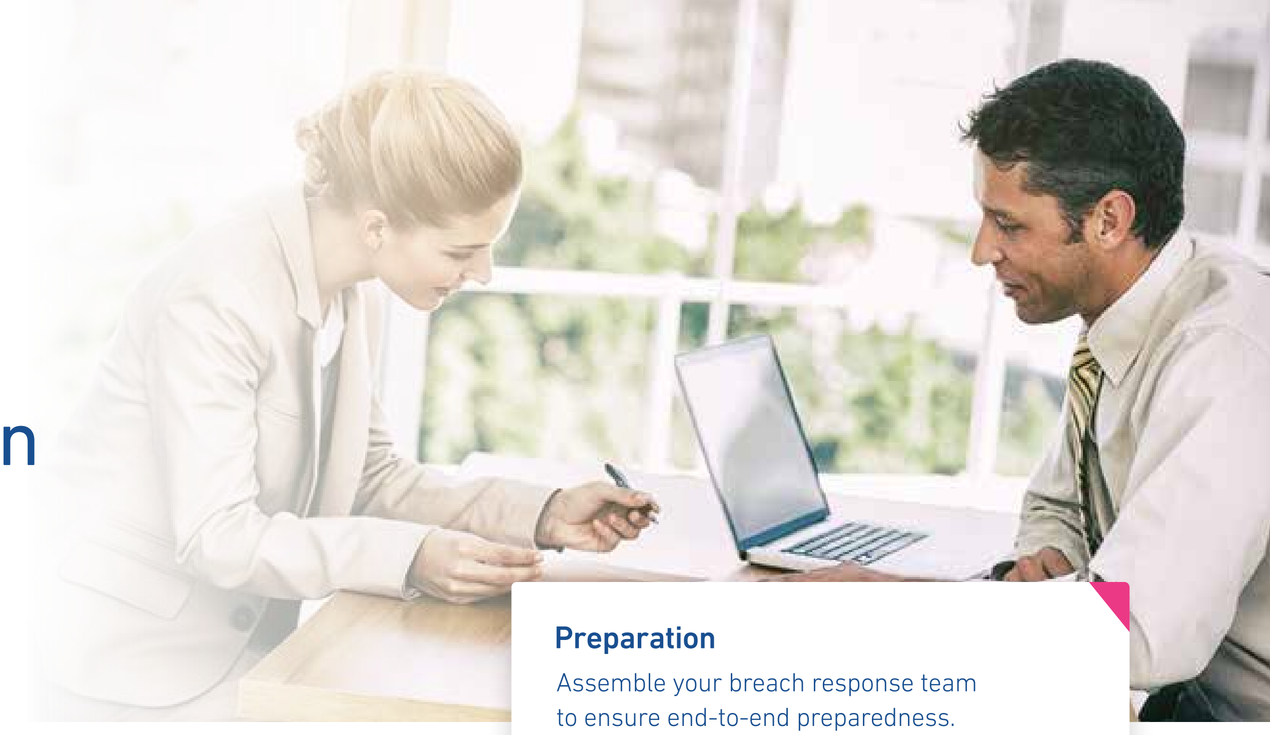
[9] 2018 Data Breach Investigations Report, Verizon, 2018

[10] The 2017 State of Endpoint Security Risk, Ponemon Institute, 2018

[11] 2017 Annual Data Breach Year-End Review, ITRC, 2017

[12] 2018 Cost of a Data Breach Study: Global Overview, Ponemon Institute, 2018

Creating Your Plan



Preparation

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

Start with a bullet-proof response team

Regardless of the size of your organization, a data breach can have a significant impact on your business. Having a response plan and team in place can help you prevent further data loss in the event of a breach and avoid significant fines and harm to your reputation.

If you're waiting until the actual discovery of a breach to decide who will be responsible for leading and managing the incident, you're already too late. A response team should be assembled well in advance and involve the coordination of multiple departments. The following internal members, external partners and influencers should play critical roles in your response plan:

Customer Care

- Assists in or crafts phone scripts
- Logs call volume and top questions and concerns

Executive Leaders

- Ensures executive management supports team decisions
- Maintains a line of communication to the board of directors and other stakeholders such as investors

Incident Lead

- Determines when the full response team should be activated
- Manages and coordinates your company's overall response team and efforts, including establishing clear ownership of priority tasks
- Acts as an intermediary between C-level executives and other team members to report progress and problems, and as the liaison to external partners
- Ensures proper documentation of incident response processes and procedures

Information Technology

- Identifies the top security risks your company should incorporate into its incident response plan
- Trains personnel in data breach response, including securing the premises, safely taking infected machines offline and preserving evidence
- Works with a forensics firm to identify compromised data and delete hacker tools without jeopardizing evidence and progress

Legal

- Determines how to notify affected individuals, the media, law enforcement, government agencies and other third parties
- Establishes relationships with any necessary external legal counsel before a breach occurs
- Signs off on all written materials related to the incident

Public Relations

- Determines the best notification and crisis management tactics before a breach ever occurs
- Tracks and analyzes media coverage and quickly responds to any negative press during a breach
- Crafts consumer-facing materials related to an incident (website copy, media statements, etc.)

HR

- Develops internal communications to inform current and former employees
- Organizes internal meetings or webcasts for employees to ask questions

Engage your external partners:

Communications

Communications partners should have experience helping companies manage highly-publicized security issues and demonstrate an understanding of the technical and legal nuances of managing a data breach.

- Develops all public-facing materials needed during an incident
- Provides counsel on how best to position the incident to crucial audiences
- Helps to manage media questions

Forensics

Forensics partners have the skills to translate technical investigations of a data breach into enterprise risk implications for decision makers within the organization.

- Advises your organization on how to stop data loss, secure evidence and prevent further harm
- Preserves evidence and manages the chain of custody, minimizing the chance of altering, destroying or rendering evidence inadmissible in court

Data Breach Resolution Provider

A data breach resolution partner offers various services and extensive expertise in preparing for and managing a breach.

- Handles all aspects of account management and notification including drafting, printing and deployment (they should also have an address verification service)
- Provides a proven identity theft protection product, comprehensive fraud resolution and secure call center services

Legal Counsel

Legal partners should have an established relationship with local regulatory entities, such as the state Attorney General, to help bridge the gap during post-breach communication.

- Indicates what to disclose to avoid creating unneeded litigation risks based on the latest developments in case law
- Ensures anything recorded or documented by your organization balances the need for transparency and detail without creating unnecessary legal risk

Influencers

State Attorneys General and Regulators

It is important to establish relationships early with your state attorney general and other regulatory entities to streamline the response process and timeline in the event of a breach. Because the majority of state notification laws now require companies to notify regulators upon discovering a breach, it's best if they are familiar with your organization ahead of an issue. To be prepared, you should maintain a contact list and know state-specific timeframe requirements for notification. Additionally, it's important to keep abreast of new stipulations as requirements evolve.

Law Enforcement

Some breaches require involvement from law enforcement. Meeting with your local FBI cyber security officer ahead of a breach to establish a relationship will serve you well when managing an active incident. Be sure to collect appropriate contact information early on so you can act fast when the time comes and inquire about an up-front meeting. During an incident, law enforcement can help look for evidence a crime has been committed and, in some cases, be the first to discover a breach has occurred.

Sixty-nine percent of data breach response plans include procedures for communicating with state attorneys general and regulators.[13]

What to Look for in a Partner

While the right external partners may vary depending on your organization, we've identified five important considerations when vetting for your response team:

1. **Understanding of Security and Privacy**
   Regardless of their line of business, partners should have a background supporting different types of data breaches, along with comprehensive knowledge of the entire breach life cycle.

2. **Strategic Insights - Can They Answer and Handle "What If" Scenarios?**
   Partners should provide compelling insights, counsel and relevant tools before, during and after an incident to help your organization better navigate the response and prevent future incidents.

3. **Ability to Scale**
   Select partners who can scale to your organization's size and potential need during an incident. While the impact may seem small, upon closer investigation, it may be broader than previously thought.

4. **Relationship with Regulators**
   If possible, data breach partners – particularly legal firms – should have established relationships with government stakeholders and regulators. Organizations with 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 a partner's global knowledge base and service capabilities, including awareness of breach laws in different countries or the ability to implement multilingual call centers.

A pre-breach agreement is a contract with a partner executed before a data breach occurs to establish the relationship and ensure the partner is ready when you need them.

[13] Fifth Annual Study: Is Your Company Ready for a Big Data Breach? Ponemon Institute, 2018

Additional Considerations

Modern cyber insurance policies offer several other valuable resources to companies, including access to leading attorneys, forensics investigators, data breach resolution providers and communications firms to help navigate complex incidents. Further, many policies offer additional valuable services ahead of an incident, such as access to risk management tools and pre-breach consultations with response experts.

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

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

Despite the substantial financial risk organizations face when it comes to data breaches, only half of companies have cyber insurance to help cover them when an incident occurs.[14]

Selecting Legal Partners

Companies often look to their existing law firms to cover a cyber security incident, which may keep them from getting the level of counsel needed to manage such a complex event. Here are a few considerations to keep in mind:

- » Law firms should have previous experience managing data breach litigation and established relationships with local regulators such as the state attorney general.
- » A good legal partner should have experience beyond formal legal notification. They should also serve as an overall breach coach with a strong understanding of technical investigations, as well as the potential implications legal decisions can have on trust and reputation.
- » Legal partners should provide insights about the latest developments in case law, which informs their counsel, and connect you with additional external experts ahead of an incident to assist in other significant areas of a response.

[14] 2018 Cost of a Data Breach Study: Global Overview, Ponemon Institute, 2018

Incorporating PR and Communications

It's important the communications team plays a role in the broader incident response process. Make sure there is a documented plan for how your organization will make critical communications decisions, what channels you will use, and what you will say.

Below are some key elements to help strengthen these efforts:

- **Enlist a Representative:** Ensure a communications representative is part of your core incident response team and included in legal and forensics discussions.
- **Map Out Your Process:** Create a detailed process for developing and approving internal and external communications, including a well-defined approval hierarchy.
- **Cover All Audiences:** Confirm your plan accounts for communicating with your employees, customers, regulators and business partners.
- **Prepare Templated Materials:** Prepare draft materials with content placeholders including:
  - Holding statements for a variety of incident types
  - Public Q&A document to address customers, investors and media
  - Letter to customers from company leadership
  - Internal employee memo
- **Test Your Communications Process:** Create a tabletop simulation for executives to gauge your ability to manage communications challenges such as media leaks, customer complaints, questions from employees and inquiries from state attorneys general.

Managing International Breaches

As data breaches become more global in scale, organizations must be prepared to handle incidents impacting customers overseas. Your organization and data breach partner need to be aware of the many complexities that go into managing incidents throughout different parts of the world. Not only do international breaches involve different languages and cultures, but they also involve increasingly diverse notification laws.

With the European Union's General Data Protection Regulation (GDPR) having gone into effect May 25 of this year, the threshold for notifying regulators and consumers of a possible data breach is lower than ever before. Companies must now notify authorities within 72 hours of becoming aware of an incident. Response plans should designate a specific individual or group to manage and anticipate potential international conflicts considering the varying degrees of compliance from one country to another.

Managing International Breaches (continued)

Your organization can take the following steps to better prepare for an international data breach

Coordinate a multinational response team: This team of internal support and third-party vendors – lawyers, communications specialists, a data breach resolution provider and forensic experts – can serve as your eyes and ears ensuring local laws and customs are followed. For a quick response, you should identify these partners during the planning process.

Prepare for increased stakeholder engagement: New international regulations bring new groups of stakeholders with which companies must engage. It is imperative your company can identify these key stakeholders and is prepared to build relationships as appropriate. The GDPR requires organizations to notify their Data Protection Authority (DPA) within 72-hours of discovering a breach. These stricter regulations make it critical for companies to coordinate and envision what this notification looks like before a breach even occurs. Additionally, reaching out early to regulators can reduce scrutiny and help streamline the process.

Organize consumer notification and support: One of the biggest challenges companies face when responding to an international data breach is activating multi-lingual consumer notifications and call centers. GDPR makes it even more crucial for organizations to notify and address consumer concerns promptly. This multi-faceted approach includes ensuring impacted parties receive notifications in the correct language as well as access to a secure, multilingual call center for their questions. Another consideration is whether or not your company will offer identity protection services to affected consumers. While not mandated, these services can help quell the fears of those impacted by the breach and ultimately help improve a company's reputation post-breach.

Preparing for an international data breach

1. Coordinate a multinational response team
2. Prepare for increased stakeholder engagement
3. Organize consumer notification and support

Practicing Your Plan

Practicing Response Plan

Of the 71% of organizations that practice their response plans, less than half (44%) practice them at least twice a year.[15]

Conduct Response Exercises Routinely

Once you've established your breach response team and finalized your plan, department-specific training should occur throughout the company. Unfortunately, for many companies, there is a significant gap between creating a breach preparedness plan and practicing its elements.

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

Responsibilities of Your Team

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

Activities should include:

» Conducting employee security training and re-training at least annually

» Working with employees to integrate smart data security efforts into their work habits

» Limiting the types of hard and electronic data employees can access based on their job requirements

» Establishing a method of reporting for employees who notice others not following proper security measures

» Developing and updating data security and mobile device policies regularly and communicating them to all business associates

» Investing in the appropriate cyber security software, encryption devices and firewall protection

» Updating security measures regularly

[15] Fifth Annual Study: Is Your Company Ready for a Big Data Breach? Ponemon Institute, 2018

Implementing a Simulation Exercise

Data breach response plans must repeatedly be practiced to not only be effective but to give your organization the chance to identify any missteps or areas of weakness. Despite security awareness increasing as well as the number of companies with a response plan in place, they are still not being practiced adequately.

Verify your organization is ready to carry-out your response plan by doing the following:

Enlist an outside facilitator

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

Schedule a healthy amount of time

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

Include everyone

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

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 learned from the session and upon what areas to improve.

Conduct drills every 6 months

Make sure to stay ahead of the latest changes internally and externally with regular simulation exercises.

Who to Involve:

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

Developing Your Simulation

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

Sample Scenarios

» The FBI contacts your company because they suspect a user on the dark web is in possession of your customers' usernames and passwords and selling them to the highest bidder. They recommend investigating the matter and conclude it's only a matter of time before the press becomes aware of the situation.

» Your company receives a note from a hacktivist organization claiming to be in possession of your customers' personal identifiable information (PII), including names, addresses, DOB and SSNs. They threaten to release the data unless the company meets its specific monetary and time demands.

» A company vendor who handles customer data suspects a breach may have compromised your data. However, they refuse to divulge any further information, citing a forensic investigation and advice from their legal counsel.

» Employees are complaining about receiving a 5071-C letter from the IRS suggesting someone may have filed a fraudulent tax return in their name, or similarly, an "executive" email that requests their personal information. These alerts could be due to the potential exposure of W-2 records to attackers, otherwise a likely successful phishing scam.

Developing Injects

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

Possible injects can include:

» A media inquiry from a reporter claiming to have information about the incident and planning to write on a tight deadline

» A letter from a state attorney general threatening an investigation into the incident if he/she does not receive a detailed accounting

» Forensics updates informing the IT teams of additional details on impacted systems and lost information

» Mock angry emails from customers or employees about the incident

Quiz: How Prepared Are You?

Here are some 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.

□ 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 in preparation for a breach?

» Do you have a relationship with relevant state attorneys general to contact and ensure you are following state guidelines?

□ Notification and Protection

» Have you identified what your breach notification process would look like and do you have the proper contact lists for relevant stakeholders (customers, employees, etc.) in place to activate quickly in all locations of operation?

» Have you evaluated identity theft protection services to offer to affected parties if you experience a data breach?

□ Security Planning

» Have you taken inventory of the types of information you store that could be exposed during a data breach?

» Do you have the technology and processes in place to conduct a thorough forensic investigation into a cyber security incident?

□ Communications

» Have you developed a communications incident response plan including drafts of key media materials that will be useful during an incident (e.g. holding statements, Q&A covering possible questions, letter from company leadership)? Do these translate to all areas where consumer data is collected?

» Have your spokespeople and executives been explicitly media-trained 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 significant incident in the last 12 months? Did this exercise incorporate overseas locations?

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

Responding to a Data Breach

Breach Discovery

65% of breaches are discovered internally.[16]

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

The first 24-hours:

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 and to whom they reported it, who else knows about it and what type of breach occurred.
6. **Interview involved parties**: Speak to those involved with discovering the breach and anyone else who may know about it – then document the results.
7. **Review notification protocol**: Review those that touch on disseminating information about the breach for everyone involved in this early stage.
8. **Assess priorities and risks**: Include those based on what you know about the breach and bring in your forensics firm to begin an in-depth investigation.
9. **Notify law enforcement**: Do this if merited, after consulting with legal counsel and upper management.

[16] 2018 Data Security Incident Response Report, Baker Hostetler, 2018

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 Cause

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

» *Document when and how you contained the breach.*

STEP 2

Alert Your External Partners

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

» *Engage your data breach resolution vendor in handling notifications and set up a call center.*

STEP 3

Continue Working with Forensics

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

» *Analyze all data sources to ascertain the compromised information.*

STEP 4

Identify Legal Obligations

» *Revisit state and federal regulations that apply and then determine all entities to notify.*

» *Ensure all notifications occur within any mandated timeframes.*

STEP 5

Report to Upper Management

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

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

STEP 6

Identify Conflicting Initiatives

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

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

STEP 7

Evaluate Response and Educate Employees

Once you resolve an incident, evaluate how effectively your company managed its response, and make any necessary improvements to your preparedness plan. Taking time to reflect and make these adjustments will ensure a smoother response in the future. Use the incident as an opportunity to retrain employees not only in their specific response roles when a breach occurs but also in their security and privacy practices.

Managing Communications and Protecting Your Reputation

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

While early planning is essential to manage a security incident successfully, organizations must always expect the unexpected. While data breaches often cause a windfall of misinformation and confusion, it's important to remember that correctly investigating a data breach and communicating facts takes time.

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

Assume news of the incident will leak before your organization has all the details and have a plan in place to address questions early in the process.

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

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

Establish traditional and social media monitoring to detect leaks and understand how external stakeholders are framing the incident.

Focus initial holding statements on steps being taken to investigate the issue and resist speculating on details about the breach before a forensic investigation.

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

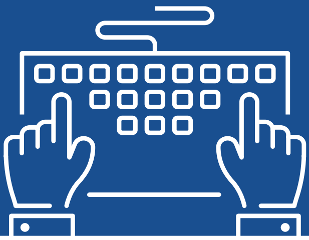
Ensure front-line employees have the information they need to communicate to their customers and make sure they know to route any media requests directly to the incident response team.

Protecting Legal Privilege

The increasing likelihood of breach also increases the possibility that your company will face some form of litigation. Because the risk of litigation is exceptionally high, it is essential to take steps to protect the legal privilege of the response process.

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

Ensure that all written materials, including emails, are marked “privileged & confidential” and that you include someone from the legal department on the distribution.



All contracts for external partners should be arranged through outside counsel so their work is part of the course of providing legal counsel to your organization.

Be thoughtful about what information you are documenting or is being put in writing versus what should be discussed in-person or on a call.

Taking Care of Your Customers

Typically, companies have 60 days to notify affected individuals of a data breach as required by law. However, depending on a variety of circumstances (such as locations affected), you may have even less time as the countdown starts the moment you discover a breach. In 2017, the average time from discovery until notification was 38 days.[17] A separate 2017 study found that in the case of international data breaches, the notification timeline is even worse with 57 percent of impacted companies taking at least two months to notify victims.[18] With the EU's GDPR now fully in place, this lack of responsiveness is no longer an option.

Notification

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

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

- Certain state laws and federal regulations may 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.
- Law enforcement may require you to delay notification if they believe it would interfere with an ongoing investigation.
- Multiple state and global laws may apply to a data breach depending on where the affected individuals reside, as opposed to the location of the business.
- If some affected individuals live in a state or country that mandates notification and others live in a state or country that doesn't, you should notify everyone.
- Be aware that some recipients will think the notification letter itself is some form of a scam.

Identity Theft Protection

While there are many identity protection and credit monitoring providers in the marketplace, some are only skilled in a particular area of the full identity protection spectrum. When selecting a protection product for the affected breach population, organizations should have a solid understanding of the various product features and capabilities.

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

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

> Seventy-two percent of security professionals believe offering free identity theft protection and credit monitoring services is the best approach to keep customers and maintain brand reputation.[19]

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

Identity protection includes credit monitoring, along with several other methods for finding stolen information and resolving potential issues. Credit monitoring is a significant component of identity protection because it can detect and alert individuals to financial changes, including new account openings, delinquencies and address changes. Identity protection takes this a step further by providing other types of monitoring, including information compromised on the dark web.

[17] 2018 Data Security Incident Response Report, Baker Hostetler, 2018

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

[19] Fifth Annual Study: Is Your Company Ready for a Big Data Breach? Ponemon Institute, 2018

Auditing Your Plan

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

Still, your plan will always work best if it's current and up to date, so make it a priority every quarter to audit and test it. Think also 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. Additionally, you should continue to update your plan based on new, unforeseen threats that may emerge in the months and years ahead.

Areas to Focus On:

Call Center

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

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

- Swiftly pull together training materials: Informed and empathetic call center representatives can make a positive impact on your brand during a crisis.
- Scale the call center component: You need to be able to adapt to any 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 breach-related calls.

Vendor Negotiations

Since many companies face data security breaches at the hands of their vendors (vendors or service providers caused 16 percent of breaches in 2017)[20], select vendors who 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 to provide 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

[20] 2018 Data Security Incident Response Report, Baker Hostetler, 2018

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

» Confirm contact information for internal and external members of your breach response team is current and remove anyone no longer linked to your organization.

» Provide the updated list to the appropriate parties.

□ Verify Your Plan is Comprehensive

» Update your plan to account for any significant 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 accounts for the latest legislation and update your notification letters if needed.

» Ensure your contact information is up to date for the attorneys, government agencies or media you will need to notify following a breach.

□ Review Who Can Access Your Data

» Assess whether third parties are meeting your data protection standards and ensure they are up to date on any new legislation.

» Healthcare entities should guarantee that business associate agreements (BAAs) are in place to meet the Health Insurance Portability and Accountability Act (HIPAA) requirements.

□ Evaluate IT Security

» Ensure proper data access controls are in place.

» Verify company-wide automation of operating systems and software updates are installed, and backup tapes securely stored.

□ Review Staff Security Awareness

» Ensure 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 links

Federal Trade Commission
www.ftc.gov/idtheft

Identity Theft Resource Center
www.idtheftcenter.org

International Association of Privacy Professionals
www.iapp.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

Blog
www.Experian.com/DBBlog

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

Twitter
www.Twitter.com/Experian_DBR

Notes

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.