Data Breach Response Guide

2020-2021 Edition

By Experian® Data Breach Resolution

Foreword

The COVID-19 outbreak has upended business and life as usual. Consumers habits and attitudes toward shopping and working online are changing, and companies' work-from-home policies may never be the same.[1] Perhaps it's no surprise that cybercrime may look a little different as well.

During the first nine months of 2020, there was a 30% decrease in the number of data breaches reported compared to the prior year.[1] However, that shouldn't be misinterpreted as a sign that you can rest easy. The pandemic pulled attention and resources elsewhere, and the actual number could be similar to prior years even if there have been delays in discovery and reporting.[2]

Additionally, cyberattacks are increasing as previously compromised information gets put to use for ransomware, phishing and brute force attacks. In some cases, cybercriminals deliberately targeted individuals, organizations and municipalities that are already strained by the pandemic.[3,4]

Even before the pandemic hit, the Experian and Ponemon Seventh Annual Data Breach Preparedness Study found only 20% of respondents were very confident in their ability to deal with ransomware, and only 23% of respondents were confident about their ability to minimize spear-phishing incidents.[5]

Unfortunately, a remote workforce doesn't make responding easier. Among companies that asked staff to work from home, 76% said it would take longer to identify and contain a data breach — 70% also predicted an increase in data breach costs. On average, a remote workforce may increase the cost of a data breach by $136,974.[6]

The coronavirus-fueled acceleration of the digital transformation also means companies collect and store more business and customer information in the cloud or in web applications. Data breaches might be down, but the number of records compromised is skyrocketing.

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.

The good news is that more organizations than ever before are instituting data breach response plans. Leadership understands the importance of being prepared for and responding to a data breach, especially as governments create and expand regulations, and consumers become increasingly concerned about their data.

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 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 cybersecurity 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.

Michael Bruemmer
Vice President
Experian Data Breach Resolution

[1] Identity Theft Resource Center. 2020. Q3 Data Breach Analysis and Key Takeaways
[2] RiskBased Security. 2020. Mid Year Data Breach QuickView Report
[3] INTERPOL. 2020, April 4. Cybercriminals targeting critical healthcare institutions with ransomware
[4] Forbes. 2020, March 21. FBI Coronavirus Warning: 'Significant Spike' In COVID-19 Scams Targeting These Three States
[5] Experian and Ponemon. 2020. Seventh Annual Study: Is Your Company Ready for a Big Data Breach?
[6] IBM and Ponemon. 2020. Cost of a Data Breach Report

Table of Contents

Foreword 2

Introduction 4

Industry Perspective 6

- Financial Services 6
- Healthcare 7
- Small and Medium-Sized Businesses 7

Keeping Pace with Cybercriminals 8

Engaging the C-Suite 10

Why do Consumer Response Plans Fail? 11

- Lack of Preparedness and Planning 11

Creating Your Plan 12

- Start With a Bullet-Proof Response Team 12
- Engage Your External Partners 14
- Understand the Impact of Influencers 15
- What to Look for in a Breach Response Partner 15
- Additional Considerations 16
- Selecting Legal Partners 16
- Selecting a Breach Response Provider 17
- Incorporating Crisis Communications 17
- Managing International Breaches 18

Practicing Your Plan 20

- Conduct Response Exercises Routinely 20
- Implementing a Drill Exercise 21
- Developing Your Drill 22
- Developing Injects 22
- Quiz: How Prepared Are You 23

Responding to a Data Breach 24

- The First 24-hours 24
- Next Steps 25
- Managing Communications and Protecting Your Reputation 26
- Protecting Legal Privilege 27
- Taking Care of Your Consumers 28

Auditing Your Plan 30

- How the Pandemic Impacts Your Response Plan 31
- Areas to Focus On 31
- Preparedness Audit Checklist 32

Experian® Reserved Response™ 33

- A Proactive Approach 31
- Guaranteed and Scalable 31

Helpful Resources 34

Introduction

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

Data breaches are no longer just a cybersecurity issue, but also a business operations issue. Every employee should be aware of and prepared to participate in a robust data breach response plan because a data breach creates havoc well beyond the initial intrusion.

More data is available than ever before, so while there may be fewer data breaches, the amount of data at risk of compromise is greater than ever before. Over 27 billion records were exposed in the first six months of 2020, more than double the 12 billion exposed during all of 2019. The vast majority of these exposed records came from three data breaches, which were all the result of misconfigured databases and services. But even if you set those large events aside, the average number of records exposed per breach is increasing.[8]

With a rising threat to PII and an increased risk of consumer identity theft caused by data breaches, the response plan is a critical component to a business's cybersecurity strategy. Your customers care about their data, and they expect you to safeguard the information they share with you. Of course, they don't ever want to hear that their PII was part of a data breach, but if it does happen, how you respond makes a huge difference in whether your customers return or do their business elsewhere.

Lost business from operational downtime, customer turnover and increased acquisition costs due to a hurt reputation accounts for about 40% of the cost of a data breach. And while 61% of total data breach costs are incurred during the first 12 months, you'll be feeling the financial impact of a data breach for years to come.[9]

Experian's 2019 Data Breach Consumer Survey Report revealed that if you are breached, consumers want to know about it quickly – within 24 hours if the data breach was in the financial sector, for example, and within days for breaches in government agencies and the healthcare industry.[10] The only way to respond that quickly is by having a response plan already in place.

How important is that response plan to consumers? The study found 90% of consumers are more forgiving of companies that had a response plan in place prior to the breach, while nearly 70% of survey respondents said they would stop doing business with a company that had a poor consumer response.

95%

Since the pandemic, 95% of CISOs plan to integrate cyber risks with overall enterprise risk management.[7]

[7] PwC. 2020. Digital Trust Insights Pulse Survey
[8] RiskBased Security. 2020. Mid Year Data Breach QuickView Report
[9] IBM and Ponemon. 2020. Cost of a Data Breach Report
[10] Experian. 2019. Data Breach Consumer Survey

$1.52M

In 2019, data breaches cost companies an average of $1.52 million in lost business.[11]

The threat of identity theft is stressful. Your quick response gives your customers peace of mind that you are on top of the breach and its aftermath. However, it isn't just a quick response. They want you to reach out to them directly and inform them. They want to know how you are going to help them protect themselves and they want to know if you provide credit monitoring and identity theft protection services. They want to be able to talk to a real person within the company who can answer any questions or concerns. Again, having a data breach response plan means you are prepared to take care of your customers' needs *immediately*. It's not just a good business move for your company, but a good thing to do to protect consumers.

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.

Identity Theft Resource Center: 2019 End-of-Year Data Breach Report[12]

Report Date: 1/8/2020

Industry	# of Breaches	% of Breaches	# of Sensitive Records Expose	% of Sensitive Records	# of Non-Sensitive Records Exposed	% of Non-Sensitive Records Exposed
Banking/Credit/Financial	108	7.33%	100,621,770	61.10%	20,000	0.003%
Educational	113	7.67%	2,252,439	1.37%	23,103	0.003%
Medical/Healthcare	525	35.64%	39,378,157	23.91%	1,852	0.000%
Business	644	43.72%	18,824,975	11.43%	705,106,352	99.990%
Government/Military	83	5.63%	3,606,114	2.19%	22,747	0.003%
Totals for All Categories:	**1,473**	**100.0%**	**164,683,455**	**100.0%**	**705,174,054**	**100.0%**

Total Breaches: **1,473** | Records Exposed: **164,683,455**

Breaches Identified by the ITRC as of: **1/8/2020**

[11] IBM and Ponemon. 2020. Cost of a Data Breach Report

[12] Identity Theft Resource Center. 2020. 2019 End-of-Year Data Breach Report

Industry Perspective

Financial Services

Financial services firms have been prime targets of cybercriminals for years, in part because of the valuable data that they maintain. The coronavirus pandemic may have also incited a surge in new cyberattacks. From February to April 2020, there was a 238% increase in cyberattacks against financial services firms. In particular, ransomware attacks increased by 900%.[13]

The Identity Theft Resource Center reports that banking/credit/financial firms experienced fewer breaches in 2019 than other industries. However, banking/credit/financial data breaches accounted for over 60% of all exposed sensitive records for the year.[14]

Data breaches can also be particularly expensive in financial service. In 2019, the average cost was $5.85 million, or about $2 million higher than the overall average data breach cost.

In general, the faster you can identify and contain a breach, the lower the overall cost. However, the financial services sector also had the shortest average data breach lifecycle (the time from identification to containment) at 233 days — 47 days faster than the overall average.[15]

[13] VMWare Carbon Black. 2020. Modern Bank Heists 3.0

[14] Identity Theft Resource Center. 2020. 2019 End of Year Data Breach Report

[15] IBM and Ponemon. 2020. Cost of a Data Breach Report

Healthcare

The healthcare industry is made up of hospitals, practitioners and service providers, many of whom maintain valuable personal records. In 2019, the healthcare industry experienced the second-highest number of data breaches (behind "business"), accounting for about 36% of all incidents.[16] The second-place spot held steady in the first half of 2020, and as the coronavirus spread in early 2020, cybercriminals changed their messaging and looked for ways to use COVID-19 to their advantage.

In April 2020, INTERPOL warned of an increase in ransomware attacks targeting hospitals, medical service centers and other organizations involved in coronavirus response efforts.[17] There has also been an increase in nation-state actors using COVID-19-themed messages in cyberattacks against healthcare and humanitarian aid organizations, as well as academic and commercial groups that are working on a vaccine.[18]

In addition to being a prime target, the healthcare industry also incurs the highest costs related to data breaches — and has done so for the last 10 years. In 2019, the average cost was $7.13 million, a 10.5% increase from the previous year.[19] The average data breach lifecycle in the healthcare sector was 329 days, 49 days longer than the overall average and 96 days longer than in the financial sector.

Small and Medium-Sized Businesses

The threat of data breaches impacts every organization, large and small. In the aftermath of a data breach, companies must deal with financial loss, hefty fines, a reputational hit and customers leaving. A data breach is devastating to the large enterprise, but for a smaller company, it is too often a blow from which the business will never recover.

While the average cost of a data breach has fallen for the smallest companies (down to $2.35 million for companies with fewer than 500 employees), data breaches continue to have disproportionately higher relative to the number of employees when compared to large firms. Medium-sized organizations saw an increase in average data breach costs compared to last year.[19]

In recent years, data breaches have also become more prevalent for SMBs, and cyberattacks are more targeted. In 2019, 63% of SMBs reported experiencing a data breach during the previous 12 months, up from 58% and 54% in prior years' surveys. And 69% say they agree or strongly agree that cyberattacks are becoming more targeted (up from 62% and 60% in prior years).[20]

Some SMBs may falsely believe they aren't targets if they don't keep customers' or clients' sensitive information, such as payment data. However, stolen usernames and passwords can be valuable for credential stuffing — when hackers use compromised information to attempt to access other sites. Credential stuffing is on the rise, a trend that may continue as people sign up for new services but fail to use different credentials for each account.[18]

[16] Identity Theft Resource Center. 2020. 2019 End-of-Year Data Breach Report

[17] INTERPOL. 2020, April 4. Cybercriminals targeting critical healthcare institutions with ransomware

[18] Microsoft. 2020. Digital Defense Report

[19] IBM and Ponemon. 2020. Cost of a Data Breach Report

[20] Keeper Security and Ponemon. 2019. Global State of Cybersecurity in Small and Medium-Sized Businesses

Keeping Pace with Cybercriminals

The world of cybersecurity is ever-changing.

Cybercriminals excel at staying one step ahead of business cybersecurity systems. Many of their attack vectors remain consistent – phishing and stolen credentials have been two out of the top three for five years running, according to the 2020 Verizon Data Breach Investigations Report (DBIR).[22] However, criminals and state actors are also finding new ways to infiltrate corporate networks.

Ransomware

From 2018 to 2019, the average ransom payment increased by 90% — from $28,920 to $302,539. The largest ransom paid in 2019 was $5.6 million.[21]

Taking Advantage of Changes in Business Operations

Cyberattacks are moving away from some of the old familiar methods to a more modern approach. Or better put, cybercriminals go to where the action is.

For example, the rapid shift to remote work opens up companies to new vulnerabilities. Chief information security officers (CISOs) were asked about the incidence of attacks related to COVID-19. Over half say they've seen and expect an increase in risk from the use of non-enterprise devices or software due to remote work. About 60% have also seen and expect an increase in phishing attacks.[23]

Social engineering scams (including, but not limited, to phishing) often make use of timely events, and the coronavirus is no exception. Scammers and hackers may pose as an authority figure, such as a government official, international health organization, doctor or scientist and use fear or false hope as a hook. Securing devices may also be more difficult for companies when employees are working offsite, particularly for organizations that have never had a remote workforce before. Kivu, a global cybersecurity consultancy, expects an increase in unsecured remote desktop protocol traffic (a preferred vector for ransomware attacks) and companies struggling with employees mixing work and personal devices.[24]

[21] BakerHostetler. 2020. Data Security Incident Response Report

[22] Verizon. 2020. Data Breach Investigations Report

[23] PwC. 2020. Digital Trust Insights Pulse Survey

[24] KIVU. 2020. Threat Intelligence Reports March 2020

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.

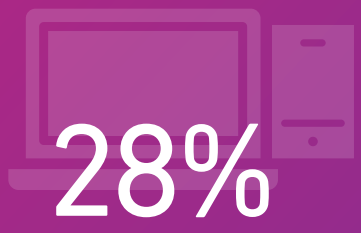
Cybercriminals still depend heavily on tried-and-true hacking methods, such as malware attacks and phishing scams. In addition to incorporating current trends and fears, cybercriminals could use AI and ML to make fake emails look more authentic and deploy them faster than ever before, causing more extensive damage to a broader group of people.

There's also been a trend in cybercriminals using popular cloud, email delivery and file-sharing services in addition to compromised web hosting infrastructures to launch phishing campaigns. The campaigns are frequently changed in an attempt to avoid detection, and a variety of phishing delivery methods may be put into use, including SMS texting, social media and video games.

Attacks are becoming more sophisticated as cybercriminals use a multi-step approach, starting with researching a target company to identify high-value targets before attempting to compromise business email accounts.[26] The increase in sophistication and targeting extends to cases that involve ransomware, which continues to be a growing threat to individuals and businesses.

The use of internet of things (IoT) devices in the workplace has been a growing concern for several years. In 2019, only 23% of organizations said they were highly or fully prepared (7+ out of 10) to deal with an IoT-based attack, and only 23% had a data breach response plan that included guidance on how to deal with such an incident.[27] This may be a particularly important area of focus in the future. Already, in the first half of 2020, there was an approximate 35% increase in attack volume on IoT devices.[26]

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.



28%

of employees admit to using personal devices for work-related activity more than their work-issued devices.[25]

[25] Malwarebytes.2020. Enduring from home COVID-19's impact on business security

[26] Microsoft. 2020. Digital Defense Report

[27] Experian and Ponemon. 2020. Seventh Annual Study: Is Your Compnay Ready for a Big Data Breach?

Engaging the C-Suite

Engagement

79% of organizations believe increased participation and oversight from senior executives could make their data breach response plan more effective.[28]

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 cybersecurity.

Despite the importance of their involvement, many boards of directors, chairmen and CEOs are not actively engaged and often avoid responsibility in data breach preparedness.

A little more than half of surveyed organizations (55%) say C-suite executives are informed and knowledgeable about how their companies plan to respond to a data breach. However, only 40% claim their boards have the same level of knowledge.[28]

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 2019 data points:

- **63%** of organizations experienced a data breach that resulted in the loss or theft of over 1,000 records with sensitive or confidential material.[29]
- **$302,539:** Average ransom payment[30]
- **80%** of data breaches included customer records with PII.[29]
- **$146:** Average cost per lost record[29]
- **$3.86 million:** Global average cost of a data breach[29]
- **207 days:** Average amount of time it takes to identify a data breach[29]
- **$8.64 million:** Average cost for US organizations[28]
- **$2 million:** Average savings from having an established incident response team with a tested response plan[29]

[28] Experian and Ponemon. 2020. Seventh Annual Study: Is Your Company Ready for a Big Data Breach?
[29] IBM and Ponemon. 2020. Cost of a Data Breach Report
[30] BakerHostetler. 2020. Data Security Incident Response Report

Why do Consumer Response Plans Fail?

Lack of preparedness and planning

Annual budget for guaranteed customer response resources and maintaining customer response readiness is $0

Like most global companies, you have likely invested heavily in IT security to ensure a data breach does not occur – firewalls, IDS, tokenization, MFA, security services, vulnerability assessments, penetration testing, etc. But we all know that even the most prepared/most secure companies often get hacked. Given that reality, ask yourself the tough questions:

- How much has my company budgeted or actually invested in guaranteed customer response resources?
- Have we invested in a comprehensive readiness program to ensure a successful response at speed, quality and scale?
- Are we proactively prepared to deliver on our customer data breach response requirements of – Notification, Support (agents) and Protection (ID Protection and Restoration Services)?

There is no estimate for the number of customer calls, emails, or messages expected

A data breach creates a huge spike in demand for information from your customers whose data may have been affected. This wave comes in the form of emails, social media activity and especially phone calls. When people believe their precious identity info has been compromised, they want to speak with a real human who can help them understand (1) what has happened and (2) what is being done to mitigate their risk. Every large data breach has validated this fact. How many calls, emails and/or messages would you expect in the worst case?

The notification plan has never been tested by a live drill

You've probably evaluated the number of customers/clients you need to notify and how you would do this (first class mail, email, substitute notice website, etc.). However, have you pressure tested your notification plan (actually prepared the verbiage in the notification letters and tested the secure transfer of files to a mail house) with a live drill talking with a live call center agent?

The maximum number of customers that could be breached is unknown

Given data archive plans, multiple data centers, cloud service providers and other business realities many companies proclaim, "We have data everywhere!" How accurate is your current "count" of the number of customer records that would need to be notified and supported in the event of a data breach?"

The availability of the staff expected to service those queries is not guaranteed

Many companies have internal call center resources or know where to go on the outside for call center help should an event occur. Be sure to ask what the guarantees and service-level agreements (SLAs) look like for the resources you have reserved to handle the wave of customer queries should you experience a large data breach.

Speed is critical – 72-hour notification regulations with massive fines

The New York Department of Financial Services (NYDFS) Cybersecurity Regulation, European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) have very sharp teeth. How prepared are you to comply with the required speed of notification – 72 hours in some cases?

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:

INCIDENT LEAD

- Determines when the full response team should be activated
- Manages and coordinates the 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
- Coordinates with legal to understand regulatory notice requirements
- 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

CUSTOMER CARE

- Assists in or crafts phone scripts
- Logs call volume and top questions and concerns
- Crafts and fulfills notifications
- Provides a dedicated Call Center

C-SUITE

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

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
- The recommended U.S. Department of Commerce National Institute of Standards and Technology Cybersecurity Framework breaks down functions into five core areas: Identify, Protect, Detect, Respond and Recover

HR

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

PUBLIC RELATIONS AND/OR CORPORATE COMMUNICATIONS

- 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.)

Engage your external partners:

CRISIS 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 and comprehensive fraud resolution services
- Offers an enhanced call center experience with high-capacity systems that can securely route calls, staff who are experienced handling data breach-related questions and 24/7 availability
- Guarantees its offering with SLAs and penalties if it doesn't deliver

LEGAL COUNSEL

Legal partners should have an established relationship with local regulatory entities, such as the state attorneys 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

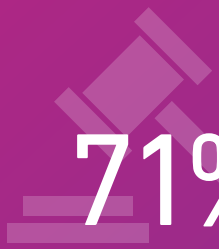
Understand the Impact of Influencers on a Breach Response

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 cybersecurity 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.



71%

of data breach response plans include procedures for communicating with state attorneys general and regulators. However, only 14% of organizations have met with law enforcement and/or state regulators in preparation.[31]

What to Look for in a Breach Response 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. **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.

4. **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.

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.

[31] Experian and Ponemon. 2020. Seventh Annual Study: Is Your Company Ready for a Big Data Breach?

Additional Considerations

Modern cyber insurance policies offer several other valuable resources to companies, including access to leading attorneys, forensic 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 costs 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.[32]

Selecting Legal Partners

Companies often look to their existing law firms to cover a cybersecurity 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 Counsel 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 response.

[32] Experian and Ponemon. 2020. Seventh Annual Study: Is Your Company Ready for a Big Data Breach?

Selecting a Breach Response Provider

A great breach response provider should have a program that guarantees:

- Breach response resources and pressure-tested readiness exercises to help the organization prepare for a successful customer-facing response
- The manpower and infrastructure guaranteed to respond at scale with speed and quality
- Expert readiness guidance based on the best practices developed from proven success and experience managing the largest and most complex data breach responses
- The ability to collaborate with internal and external incident response teams to help build a detailed customer-facing breach response plan that includes operational details for notification, customer support and identity protection services
- Robust notification, call center and identity protection services to back up the plan
- Participates or leads customer-facing breach response exercises designed to stress test the response plan and identify gaps

Incorporating Crisis 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 forensic 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 drill 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.

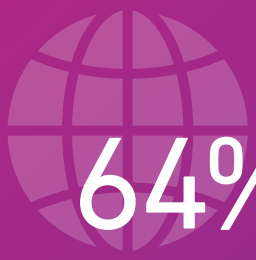
Managing International Breaches

Global data breaches are on the rise: 45% of companies report global data breaches, but only 34% say they are confident enough to deal with an international breach.[33] This isn't surprising, as more and more companies have a global outreach, even if it is no more than a website with a few international customers.

A data breach in your organization could have far-reaching implications. The increasing number of records compromised by data breaches has resulted in an increasing number of data privacy and protection laws. These new laws necessitate a data breach response plan that meets a variety of international regulations, but all address how data is collected and stored.

The best known of these regulations, and the one with the most impact, is the GDPR, which went into effect on May 25, 2018, and impacted every business with customers who are EU citizens. Companies with EU customers are now required to report a data breach within 72 hours of discovery or face large fines. China's data privacy laws are even stricter than GDPR and give the Chinese government the right to inspect how a company handles customer data. The Australia data privacy laws allow companies 30 calendar days to assess and report on the damage caused by a data breach.

These are just a few examples of the data privacy laws; at least 50 countries have laws that require companies to meet certain requirements in data protection and data breach reporting. 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.



64%

of incident response plans include processes for managing international data breaches.[33]

[33] Experian and Ponemon. 2020. Seventh Annual Study: Is Your Company Ready for a Big Data Breach?

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 partners – 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 multilingual 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 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 75% of organizations that practice their response plans, less than half (45%) practice them at least twice a year.[34]

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 retraining 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.
- Updating security measures regularly.
- Investing in the appropriate cybersecurity software, encryption devices and firewall protection.
- Establishing a method of reporting security incidents to the incident team and 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.

[34] Experian and Ponemon. 2020. Seventh Annual Study: Is Your Company Ready for a Big Data Breach?

Implementing a Drill 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:

Complete materials and workflows

Have your notification materials and workflows ready, so you can test their effectiveness during the drill.

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 action items, gaps and 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
- Privacy Information Security
- Outside Partners (legal counsel, public relations firm, data breach resolution provider and cyber insurers)

Developing Your Drill

Ideally, you will want to dedicate half a day to a drill exercise so that you can address multiple 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.

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.

74%

of organizations believe their data breach response plan could be more effective if they incorporated what they learned from previous breaches.[35]

- 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 drill 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 parts 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 they do not receive a detailed accounting.
- Forensics updates informing the IT teams of additional details on impacted systems and lost information.
- Mock angry emails or phone calls from customers or employees about the incident.

[35] Experian and Ponemon. 2020. Seventh Annual Study: Is Your Company Ready for a Big Data Breach?

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 plan and team assembled to execute it?
- ☐ If you have a preparedness plan in place, have you tested it in the last six months and audited it during the most?

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 cybersecurity incident?

TRAINING AND AWARENESS

- ☐ Have you conducted a data breach crisis tabletop exercise or drill 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?

KEY PARTNERS

- ☐ Have you identified third-party partners and signed contracts in preparation for a breach? Do those contracts have guaranteed response timelines?
- ☐ 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 based on the data you hold if you experience a data breach?

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, a 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?

Responding to a Data Breach

Breach Discovery

78% of breaches are discovered internally.[36]

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, 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 protocols that touch on disseminating information about the breach for everyone involved in this early stage.
8. **Assess priorities and risks:** Set these 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.

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.

HOW A DATA BREACH UNFOLDS

- Data incident is discovered
- Outside legal counsel is engaged
- Forensics determines "who" and "what"
- "Go/No Go" for consumer response
- Public Relations crafts messaging
- Consumer notification (letter, email. website)
- 1-800 Call Center for FAQs/Enrollment
- Identity theft Protection/ Fraud Resolution

1. **DISCOVER**
2. **INFORM** (Company Incident Lead)
3. **ASSESS** (Forensics)
4. **GUIDE** (Breach Counsel)
5. **NOTIFY** (Breach Response Provider)

[36] BakerHostetler. 2020. Data Security Incident Response Report

Next Steps

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

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.

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.

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.

4 IDENTIFY LEGAL OBLIGATIONS

- [ ] Revisit state and federal regulations that apply and then determine which entities to notify.
- [ ] Ensure all notifications occur within any mandated timeframes.

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.

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.

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 in their specific response roles and 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.

Ensure frontline 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.

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.

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, with the EU's GDPR now fully in place and the addition of the CCPA, a lack of responsiveness is no longer an option. 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.

Even when there isn't a regulatory requirement to immediately notify customers, a quick response could be important. Today, over 70% of consumers expect to be notified of a data breach within 24 hours of a data breach.[37] Additionally, about half of consumers say they're more likely to trust a company that reacts quickly and actively discloses a data breach to the public.[38]

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 (like CCPA) 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.

[37] Experian. 2019. Data Breach Consumer Survey
[38] McKinsey & Company. 2019. Survey of North American Consumers on Data Privacy and Protection

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

74%

of security professionals believe offering free identity theft protection and credit monitoring services is the best approach to keep customers and maintain brand reputation.[39]

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.

[39] Experian and Ponemon. 2020. Seventh Annual Study: Is Your Company Ready for a Big Data Breach?

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. Make it a priority to test the plan every six months, and audit it quarterly to keep contact information up to date and ensure new members of the incident team are familiar with the plan. 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.

How the Pandemic Impacts Your Response Plan

Your quarterly audit also gives you the opportunity to update your plan based on new, unforeseen threats that may emerge in the months and years ahead. For instance, with the pandemic in mind, consider:

- Have you updated your communication workflows and conducted an end-to-end response drill based on the current work environment?
- Are you certain that your organization and vendors have the capacity to respond to an industry-wide event?
- Will your breach response provider continue to guarantee response times?

Continue to ask probing questions and updating the plan based on how your organization and industry is responding to the pandemic.

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

Many companies face data security breaches at the hands of their vendors, and it's important to select vendors that have appropriate security measures in place for the data they will process. Then, take it a step further by contractually obligating your vendors to maintain sufficient data safeguards and assessing their performance in meeting contract requirements on a regular basis.

Make sure your vendors:

- Maintain a written security program that covers your company's data.
- Only use your customer data 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.
- Document their own breach response plan.

Preparedness Audit Checklist

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

UPDATE YOUR TEAM CONTACT LIST

- [ ] 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.

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.

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.

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.

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.
- [ ] Implement annual security awareness training especially for phishing and spear-phishing attacks.

EVALUATE IT SECURITY

- [ ] Ensure proper data access controls are in place.
- [ ] Verify company-wide automation of operating systems and software updates are installed.

Experian® Reserved Response

Experian® Reserved Response program is the industry's first and only program that guarantees the manpower, infrastructure and response readiness that your company needs with service level agreements (SLAs). The agreements are backed by penalties if we don't follow through, but we've handled thousands of high-profile data breaches in nearly every industry without missing one SLA.

A Proactive Approach

Part of our — and your — success stems from the proactive nature of the program. The proprietary Experian process to become Response ReadyTM includes:

- Expert guidance based on the best practices developed from more than a decade of managing the largest and most complex data breach responses in history
- Collaboration with your internal and external incident response teams to build a customer-facing breach response plan that includes notification, support and identity protection services.
- Detailed response drills and simulations designed to stress test your plan and identify gaps. Annual planning exercises and simulations to keep your plan and team up to date.

When you do experience a data breach, having a tested plan in place can save your organization time and money. Through training, your staff can develop a muscle memory response, but you may also need additional resources to deal with the inevitable spike in communication.

$2M is the average organizations can save by having an established incident response team with an extensively tested response plan.[40]

Guaranteed and Scalable

With Experian® Reserved Response, you can reserve the guaranteed breach response manpower and infrastructure that's needed to execute a customer-facing response of any size. Your response could be up and running within as little as three days with guaranteed SLAs (rather than the up to five that competitors offer), and you'll benefit from:

- Preconfigured templates and workflows as part of your annual Response Ready program.
- A dedicated account manager to oversee the rapid response.
- 24-hour compliance review turn-around to ensure you won't miss notification requirements.
- Penalties for missing an SLA.
- Full-service notification services, including letter templates, custom messaging, address verification, printing and mailing.
- A 24/7 dedicated call center with a toll-free number and US-based agents.
- Multiple levels of data breach protection that you can provide to your customers and employees.
- Ongoing reporting of call centers, notification, enrollment, identity theft and fraud resolution metrics that you can use to keep key stakeholders and regulators informed.

When you do experience a data breach, having a tested plan in place can save your organization time and money. Through training, your staff can develop a muscle memory response, but you may also need additional resources to deal with the inevitable spike in communication.

[40] IBM and Ponemon. 2020. Cost of a Data Breach Report

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

NIST Cybersecurity Framework
www.nist.gov/cyberframework/csf-reference-tool

EXPERIAN LINKS

Experian Data Breach Resolution
www.Experian.com/DataBreach

Experian Reserved Response
www.experianpartnersolutions.com/reserved-response/

Blog
www.experian.com/blogs/data-breach/

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

Twitter
www.Twitter.com/Experian_DBR

REFERENCES

- BakerHostetler. 2020. Data Security Incident Response Report
  2020_DSIR_Report_(003).pdf
- Experian and Ponemon. 2020. Seventh Annual Study:
  Is Your Company Ready for a Big Data Breach?
  www.experian.com/Seventh Annual Study
- Experian. 2019. Data Breach Consumer Survey
- Forbes. 2020, March 21. FBI Coronavirus Warning: 'Significant Spike' In COVID-19 Scams Targeting These Three States
  www.forbes.com/FBI Coronavirus Warning
- IBM and Ponemon. 2020. Cost of a Data Breach Report
  www.ibm.com
- Identity Theft Resource Center. 2020. 2019 End-of-Year Data Breach Report
  www.idtheftcenter.org
- Identity Theft Resource Center. 2020. Q3 Data Breach Analysis and Key Takeaways
  notified.idtheftcenter.org
- INTERPOL. 2020, April 4. Cybercriminals targeting critical healthcare institutions with ransomware
  www.interpol.int
- Keeper Security and Ponemon. 2019. Global State of Cybersecurity in Small and Medium-Sized Businesses
  www.keeper.io
- KIVU. 2020. Threat Intelligence Reports March 2020
  kivuconsulting.com
- McKinsey & Company. 2019. Survey of North American Consumers on Data Privacy and Protection
  www.mckinsey.com
- Microsoft. 2020. Digital Defense Report
  www.microsoft.com
- PwC. 2020. Digital Trust Insights Pulse Survey
  www.pwc.com
- RiskBased Security. 2020. 2020 Mid Year Data Breach QuickView Report
  pages.riskbasedsecurity.com
- Verizon. 2020. Data Breach Investigations Report
  enterprise.verizon.com
- VMWare Carbon Black. 2020. Modern Bank Heists 3.0
  www.carbonblack.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 seventeen years 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 NetDiligence®, Advisen, and InfraGard.

For more information, visit **experian.com/databreach.**