

Data Breach Response Guide

8TH Edition

2022-2023



Presented by Experian® Data Breach Resolution



Meet the Experts



**Has your company experienced
a data breach?**



Contact us now!

1-866-751-1323

databreachinfo@experian.com



Michael Bruemmer

Vice President,
Global Data Breach and
Consumer Protection



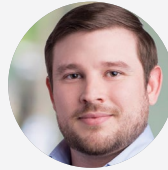
Apiyo Obala

Account Director and Team Lead



Allen Burzen

Business Development Manager,
Breach Business Development



Christopher Mims

Support Readiness Coordinator



Michael Morelli

Director,
Breach Business Development



Kyle Walker

Account Manager



Ozzie Fonseca

Senior Director,
Breach Business Development



Ryan Coyne

Business Development Manager,
Breach Business Development



Meet the Experts



**Has your company experienced
a data breach?**



Contact us now!

1-866-751-1323

databreachinfo@experian.com



Adam Castilleja

Support Readiness Manager



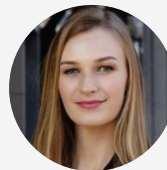
Carrie Craft

Client Engagement Manager



Alex Kheyson

Client Relations Specialist Lead



Mercedes Bellcase

Client Engagement Team Lead



Anel Linsenbardt

Senior Client Engagement Manager



Saba Tahir

Client Engagement Manager



Armando Valdez

Client Engagement Manager

Foreword

For decades, the world has been on a steady and not-so-slow path of innovation and daily adoption toward what some might call digital domination. In this world, almost everything is done and undone with a screen touch, keystroke, password, or PIN. This world is a reality now.

We are all more digitally connected than ever before. While this connectivity allows for new technological capabilities, it also creates constant vulnerabilities for businesses, governments, and consumers that cost lost time, relationships, and financial and reputational damage.

The New Normal

As we navigate the new way of living, working, and handling the unpredictability of COVID-19 and its wide range of impacts, now is not the time to ease up on data breach preparedness.

The [2022 Experian Data Breach Forecast](#) identifies five predictions to keep an eye on. For starters, natural disasters and global crises will continue to drive more donations to aid organizations. In response, both donors and people in distressing situations will see increased phishing attempts masked as charitable giving. This [Perfect Storm](#) prediction, complicated by the continuation of broken and unreliable global supply chains, will make sourcing essential emergency goods difficult – another vulnerability that hackers will look to exploit.

The Cyberdemic 2.0: Institutions Adapt, Individuals Remain the Weak Link prediction highlights how cybercriminals will continue to take advantage of new work and lifestyle changes produced by the pandemic, including reliance on telehealth and remote work. Some of the changes may be permanent aspects of daily life, creating arguably mixed consequences. While many institutions will have successfully adapted and developed new security protocols, many individuals – many working remotely indefinitely – will likely be the weak security link in these new digital systems.

Many industries should be on the lookout for threats in 2022, including [Gambling and Infrastructure](#). The Infrastructure and Investment Jobs Act poses unique threats, which are detailed in the Industry perspective section of this guide. As for gambling, as more states legalize online sports betting, phishing scams will target the growing ranks of online gamblers, particularly new entrants. The large pool of money flowing from gamblers to online casinos will be a tempting target. Scammers will also target fantasy sports sites, whether through phishing attempts or outright hacks.

Aside from the above predictions, [ransomware](#) keeps CIOs, CEOs, and data breach response teams up at night. Ransomware attacks have become more aggressive domestically than globally, accounting for 30%

of all cyberattacks in 2020, more than double the global rate of just 14%¹. The financial stakes are high too. In 2021, the [average total cost of a ransomware breach was \\$4.62 million](#)², with 46% of ransoms ringing up at more than \$100,000³.

At Experian, we handle more than 50,000+ breaches a year and know that [7 of 10 breaches involve ransomware](#), which takes about 20% more time to begin breach notification.⁴ While ransomware payments are trending downward – 53% paid in 2021, from 62% paid in 2020 – the attacks are still a rising threat⁵.

Limit Your Liability

With cybercrime on track to cost the world [\\$10.5 Trillion annually](#) by 2025⁶, securing proper insurance will become even more essential. In 2022, [premiums are expected to rise 30-50% depending on the industry](#), with healthcare and medical service providers potentially experiencing a triple-digit uptick⁷. The stakes for not holding a policy could make recovering from a breach severely problematic.

In addition, the burden of proof will shift to companies in 2022, as policyholders will need to provide proper documentation proving that insureds were following policy controls before their breaches to process their claims. Since only about one-third of companies have cyber insurance, we could see a rush for many companies to secure cybersecurity counsel after their breach, creating delays and added stress to an already burdensome situation.

The latest data shows that only [56% of companies have a Business Continuity plan](#), and just 59% have a Crisis Management plan⁸.

At Experian, we know that preparation is paramount when it comes to a cyberattack. We're continuing to expand our product offerings, keep our eyes and ears on the lookout for rising threats and trends, and use our years of experience to support our partners when they need us most.



Michael Bruemmer

Vice President,
Global Data Breach and
Consumer Protection

¹ Verizon 2021 Data Breach Investigations Report

² IBM & Ponemon 2021 Cost of a Data Breach Report

^{3-5, 7-8} Experian and Ponemon. 2022. Ninth Annual Study: Is Your Company Ready for a Big Data Breach?

⁶ Cybersecurity Ventures, Cybercrime Magazine. "Cybercrime To Cost The World \$10.5 Trillion Annually By 2025", November 2020



Table of Contents

Foreword	4	Practicing Your Plan	24
Introduction	6	Conduct Routine Response Exercises	24
Industry Perspective	8	Developing a Response Drill	25
Healthcare	8	Developing Injects	25
Financial Services	9	Implementing a Response Drill	26
Small and Medium-Sized Businesses	9	Preparedness Checklist	27
Government and Infrastructure	10	Auditing Your Plan	28
Education	10	Quarterly Audit Questions	28
The Rise of Ransomware	12	Preparedness Audit Checklist	29
Why Consumer Responses Fail	14	Focus Areas	30
Lack of Preparedness and Planning	14	Responding to a Data Breach	31
Creating Your Plan	15	The First 24	31
Start With a Strong Response Team	15	Next Steps	32
Convincing the C-Suite	17	Managing Communications and Protecting Your Reputation	33
Engage Your External Partners	18	Protecting Legal Privilege	34
Understanding Influencers Impact on a Breach Response	19	Taking Care of Your Customers	35
Recruit the Right Breach Resolution Partner	19	Managing Your Crisis Response	37
Cyber Insurance Considerations	20	Experian Reserved Response™	38
Choosing a Legal Partner: A Checklist	20	Our Take Charge Technique	38
Breach Response Provider Review	21	Guaranteed and Scalable	38
Crisis Communications Capabilities	21	Resources	39
The Global Standard	22		

© 2020 Experian Information Solutions, Inc. All rights reserved. Experian and the marks used herein are service marks or registered trademarks of Experian Information Solutions, Inc. Other product and company names mentioned herein may be the trademarks of their respective owners.

Legal Notice: The information you obtain herein is not, nor intended to be, legal advice. We try to provide quality information but make no claims, promises or guarantees about the accuracy, completeness or adequacy of the information contained. As legal advice must be tailored to the specific circumstances of each case and laws are constantly changing, nothing provided herein should be used as a substitute for the advice of competent legal counsel.

Introduction

Stay ready. In today's fast-paced world, where cybercriminals can compromise your organization at every level in a second, staying prepared for a data breach is critical.

From the C-Suite to the call center, every employee in your organization must have breach risks on their radar and understand their role in your data breach response plan. The days of data breach preparedness falling squarely on the shoulders of cybersecurity and IT teams are over.

2021 broke data breach records. Again.

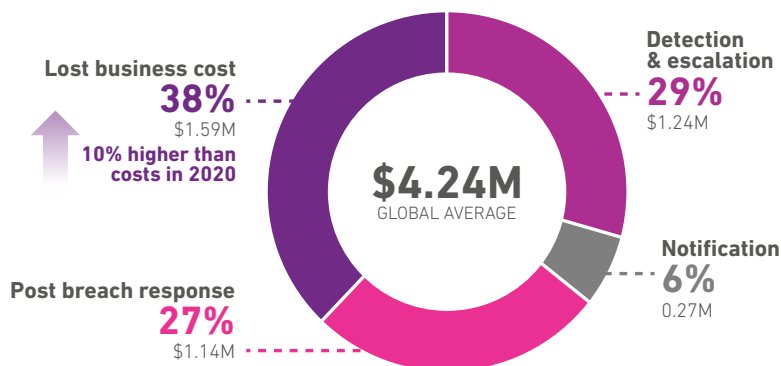
More than 18.8 billion records were exposed across nearly 1800 breaches in the first six months⁹. By year's end, the final reported incident number rose to almost 1,900, surpassing 2020's record by 68% (1,108 breaches) and beating the all-time 2017 high of 1,506 breaches by 23%¹⁰.

Consumers, employees, and businesses are exchanging more data than ever. While this creates ease and speed, it also leads to financial loss and a loss of trust.

What's more, though almost 23% of businesses disagree that they are effectively preparing for post-breach backlash and loss of trust, and 18% are unsure, consumers are clear on where they stand.

Consider this: **33% of consumers say fraud is the number one reason they leave a business**, followed by 32% who depart because of a breach, even if the incident didn't involve PII or other sensitive information. For consumers, data breach preparedness is not just about having a plan but quickly activating it¹².

Average total cost of a data breach in 2021¹¹



Consumer confidence is key.

Your consumers want assurances that your cybersecurity plan is prioritizing protecting the data they entrust you with so that when a breach happens, you have a plan in place to protect it.

A recent Experian Data Breach report revealed that **if you experience a breach, consumers want to know about it within 24 hours** if it is a financial sector breach and within days for a government agency and healthcare industry breach¹³.

The study also found that 90% of consumers are more forgiving of companies with a response plan before the breach. In comparison, **nearly 70% of survey respondents said they would stop doing business with a company** that had a poor consumer response¹⁴.



\$4.24 million

The average cost of a data breach, up from \$3.86 million.

-IBM & Ponemon 2021 Cost of a Data Breach Report

⁹ RiskBased Security, 2021 Mid-Year Data Breach Quick View Report

¹⁰ Identity Theft Resource Center (ITRC) 2021 Annual Report

¹¹ IBM & Ponemon 2021 Cost of a Data Breach Report

¹² Experian and Ponemon. 2022. Ninth Annual Study: Is Your Company Ready for a Big Data Breach?

¹³⁻¹⁴ Experian. 2019. Data Breach Consumer Survey

Data breaches are here to stay. Quick response and immediately providing your consumers with credit monitoring and identity theft protection services and expert call agents to address their fears, questions, or concerns about their stolen PII will foster confidence, trust, and loyalty.

Whether you are thinking about developing a plan for your organization or need to update your current practices, this guide will show you exactly what a comprehensive data breach response plan should look like and how to execute it to meet the cybersecurity challenges that lie ahead.

Data breach response preparedness is the only way forward. **Stay. Ready.**

The average amount of lost business data breaches cost companies in 2021¹⁵.

\$1.59M



Identity Theft Resource Center: 2021 End-of-Year Data Breach Report¹⁶

Compromise Type	Breaches/ Exposures	Victims	Cause #1 % of Volume	Cause #2 % of Volume	Cause #3 % of Volume
Cyberattacks	1,613	188,900,415	Phishing/BEC 33%	Ransomware 22%	Malware 98%
Human & System Errors	179	104,891,759	Correspondence 37%	Cloud Security Failure 30%	Lost device or document 7%
Physical Attacks	51	132,979	Device theft 33%	Document theft 18%	Improper disposal 10%

¹⁵ IBM & Ponemon 2021 Cost of a Data Breach Report

¹⁶ Identity Theft Resource Center. 2020. 2021 End-of-Year Data Breach Report



Industry Perspective



Healthcare

The healthcare industry continues to be a top target for hackers. According to the Department of Health and Human Services, the sector suffered a **record 713 data breaches in 2021**, exposing nearly 50 million records¹⁷. To add insult to injury, hospitals, service providers, and practitioners are getting hit with massive bills to fix the damage, with the average **healthcare breach costing just over \$9 million**, the highest of all industries¹⁸.

While COVID-19 scams played a significant role in the breach increase, hacker SaaS platforms also made it easier for less-skilled bad actors to strike healthcare systems using data as currency. Personal Health Information (PHI) commands higher prices on the dark web and black market than financial-related data, such as credit card numbers or Personally Identifiable Information (PII) like Social Security numbers, with PII selling for as little as \$1 and **PHI going for \$363 per record**¹⁹.

2021's Largest Healthcare Breaches

- Florida Health Kids
- 20/20 Eye Care Network
- Forefront Dermatology

TOTAL AFFECTED INDIVIDUALS:

>8MM²⁰

¹⁷ U.S. Department of Health and Human Services Office for Civil Rights

¹⁸ IBM & Ponemon 2021 Cost of a Data Breach Report

¹⁹ Infosec Institute HIPPA Breach Reporting Tool

²⁰ GovInfoSecurity HIPPA Journal



Financial Services

The financial services industry is a top target for cyberattacks, facing tens of thousands of incidents daily. In 2021, the banking industry saw an astronomical **1,318% increase in ransomware attacks** in the first half of 2021²¹. The uptick has caused financial organizations to go on high alert, with 70% of financial organizations ranking cybersecurity as their biggest concern²². Since financial firms rely heavily on third-party vendors to introduce innovations, leverage cloud services, and delegate tasks, raising concerns about data breach security and confidential data access they have and the consequences those relationships create.

According to Security Today, financial firms **fall victim to data breaches almost 300 times more** frequently than other industries. Financial services firms are disproportionately the target for data breaches because of the far-reaching impact and profit that hackers stand to gain if their security breach is successful. And by all accounts, they have been successful, with the **average cost of a data breach in 2021 debiting nearly \$6 million** from financial firms²³.

While bad external actors cause many breaches, that's only about half of the story. In 2020, **44% of financial data breaches were activated by internal actors**²⁴. Although mainly the result of accidental actions, such as sending emails to wrong contacts (55%), error-based activities also accounted for 13% of all breaches that year²⁵.

"Third-party attacks are rising. Internal planning is step one, but don't forget to create an external breach response plan for vendors who handle or house sensitive data."

- Chris Mims
Support Readiness Coordinator



Small and Medium-Sized Businesses

Like global corporations, SMBs also experience frequent cyberattacks. However, unlike larger companies, underfunding and understaffing play a more significant role in how SMBs handle an incident.

Although **43% of cyber attacks target small businesses**, SMBs have fewer resources to plan for and respond to an attack. They are also more likely to have their cyber security infrastructure infiltrated²⁶.

On average, a small business with less than 500 employees spends **\$7.68 million per incident**²⁷. While a ransomware attack could mean a short period of disruption for a large organization, for an SMB, it could mean total devastation.

2020 SMB Cyber Attack Facts

1,037 incidents, 263 with confirmed data disclosure²⁸

DATA TYPES COMPROMISED:

- **Credentials (44%)**
- **Personal (39%)**
- **Other (34%)**
- **Medical (17%)**



²¹ Trend Micro Report. "Attacks Surge in 1H 2021 as Trend Micro Blocks 41 Cyber Threats, September 2021"

²² Conference of State Bank Supervisors. "Community Banker Concerns Shift to Funding," October 2019

²³⁻²⁵ Verizon 2021 Data Breach Investigations Report

²⁶⁻²⁷ Cybint Solutions. "15 Alarming Cyber Security Facts and Stats," December 2020

²⁸ Verizon 2021 Data Breach Investigations Report



Government and Infrastructure

As perhaps the most significant legislation introduced and passed in 2021, the U.S. Infrastructure Investment and Jobs Act law will provide **\$550 billion** for new federal infrastructure investments through 2025. As the funds to rebuild our nation's roads and bridges and expand access to high-speed internet get distributed, hackers will undoubtedly increase their activities to detect and exploit network vulnerabilities involved in these transactions.

From the 2021 Colonial Pipeline hack—which shut down the primary conduit for oil along the U.S. Eastern Seaboard to the JBS Foods, Kia Motors, San Diego Hospital System, and Clearwater, Florida water treatment plant incident—it's clear that more infrastructure and government-related attacks are ahead. While the Colonial Pipeline eventually paid a ransom to the criminal ring, The DarkSide, to restore gas flow, it's also clear that either geopolitical gain, money, or plain and simple malice will continue to fuel the motivation for more attacks.

In 2022, the Mining, Quarrying and Oil and Gas Extraction and Utilities vertical endured 546 incidents²⁹. Of those incidents, 355 had confirmed data disclosure data types compromised: Credentials (94%), Personal (7%), Internal (3%), Other (3%) (breaches)³⁰.

Public sector data breaches cost an average of \$1.93 million³¹.

While "low cost" compared to other sectors, that figure is still problematic. Government agencies collect and store vast and diverse citizen data, from passport information to social services data. Many, if not most, rely on outdated computer systems for data security, making them easier targets for cybercriminals³².

As the infrastructure activity moves forward, both government agencies and infrastructure leaders, both public and private, must tighten up loose ends and fix network holes before a data breach undermines its positive economic impact on the country.



Education

Over the last few years, with the COVID-19-related shift to remote learning and reliance on technology, the educational sector, rich in PII, saw a rise in vulnerabilities and more frequent and sophisticated cybercrime. According to the K-12 Cybersecurity Resource Center, **there were more than 400 publicly-disclosed school incidents in 2020 alone³³** – and that number is likely much higher due to the varying reporting requirements that schools and districts operate within. One explosive incident occurred in March 2021 with Buffalo, NY Public Schools, where hackers shut down classes for days, stole sensitive student and employee information and destroyed vital school records. **The attack result: a \$10 million payout³⁴.**

In response to the growing rise in ransomware and data breaches in the K-12 educational sector, in the fall of 2021, the Biden Administration passed the K-12 Cybersecurity Act of 2021 to study the cybersecurity risks that elementary and secondary schools face and establish recommendations to respond.

The average cost of an education sector data breach hit \$3.79 million in 2020, according to the IBM & Ponemon 2020 Cost of a Data Breach Report.



²⁹⁻³⁰ Verizon 2021 Data Breach Investigations Report

³¹ IBM & Ponemon 2021 Cost of a Data Breach Report

³² Security Intelligence

³³ K-12 Cybersecurity Resource Center. "The State of K-12 Cybersecurity: 2020 Year in Review, K-12 Cybersecurity Resource Center and the K12 Security Information Exchange, March 2021

³⁴ Buffalo Public Schools. MSSP Alert, A CyberRisk Alliance Resource, March 2021

³⁵ Since 2005, according to Comparitech

Top Industries by Number of Compromises³⁶

Industry	Number of Compromises	Victims
Healthcare	330	28,045,658
Financial Services	279	19,745,846
Manufacturing & Utilities	222	49,775,124
Professional Services	184	22,697,765
Education	125	1,680,300
Retail	102	7,186,143

2021 Data Breach Download³⁶



Total Data
Compromises:

1,862



Victims:

293M



Records
Exposed:

18B



³⁶ Identity Theft Resource Center: 2021 End-of-Year Data Breach Report



The Rise of Ransomware

What is Ransomware?

Ransomware happens when cybercriminals take over an organization's computer network with malware. Once control is assumed, the criminals demand a ransom to restore the victim's encrypted data access.

Ransomware 2.0

According to cybersecurity experts, ransomware is now a chief threat with room to increase. High-profile criminal ransomware rings like DarkSide, REvil, and BlackMatter show no signs of letting up on their attacks. In 2021, 47% of organizations experienced a ransomware attack, and the Kronos, Colonial Pipeline, JBS, and Kaseya attacks made headlines, causing widespread disruption and cost millions³⁷. According to reporting, the Colonial Pipeline and JBS collectively paid more than \$15 million to resolve their ransomware attacks³⁸⁻³⁹.

Ransomware Facts

Upping the Extortion Ante

Nowadays, it's not enough for cybercriminals to hold an organization's data hostage for a single ransom payment. Criminals have taken to layering their strategy with double and triple extortion demands. With double extortion, hackers threaten to release sensitive data to the public to ratchet up an organization's pressure to pay. With triple extortion, thieves use the power of proof to get paid, leveraging a successful ransomware attack on a company to extort one of its business partners.

- **\$4.62 million:** the average total cost of a ransomware breach⁴⁰.
- **59%:** breach events involving ransomware serviced by Experian.
- In 2021, a business was hit by a ransomware attack **every 11 seconds**, up from around 40 seconds in 2016⁴¹.
- 50% of breaches occurred because of **third-party supply chain partners**⁴².

Ransomware-as-a-service (RaaS)

Influenced by the increase in remote work with RaaS, bad actors are also launching successful attacks by purchasing ready-made ransomware tools created by a skilled developer. A recent, real-world example: the RaaS platform DarkSide attacking the Colonial Pipeline.

Threat Vectors

As hackers get even bolder with structuring their attacks and payment demands, organizations from all industries must know where they rank on the attack vulnerability scale. According to a 2021 Ponemon Institute study, the following industries should be on high alert⁴²:

- **IT Infrastructure Attacks 41%**
- **Endpoints 35%**
- **Nation-State Attacks 34%**
- **Physical Infrastructure Attacks 28%**
- **Cloud 25%**
- **Online gaming 19%**
- **Mobile Devices 15%**

^{37, 42} Experian and Ponemon. 2022. Ninth Annual Study: Is Your Company Ready for a Big Data Breach?

³⁸ Bloomberg News Hackers Breached Colonial Pipeline Using Compromised Password. June 2021

³⁹ The Wall Street Journal JBS Paid \$11 Million to Resolve Ransomware Attack. June 2021

⁴⁰ IBM & Ponemon 2021 Cost of a Data Breach Report

⁴¹ Cybersecurity Ventures, Cybercrime to Cost the World \$10.5 Trillion Annually by 2025

Tactics and Techniques Update

Our last report touched on how artificial intelligence (AI) and machine learning (ML) present unique concerns for cybersecurity professionals. On the one hand, the technology helps the cybersecurity community predict and identify potential threats. On the other hand, it creates a challenge because hackers use it to create more sophisticated attacks, including launching malware attacks and phishing scams. With AI and ML, hackers create more authentic-looking emails, deploy them faster, impact more people, and cause more damage.

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.

While there's no way to anticipate what cybercriminals will do next to disrupt businesses and consumers' security, historical and current trends can help both audiences increase their awareness, preparedness, response, and recovery efforts.

What's changed.

62% 

of IT Managers' **most significant concern** was employees accidentally exposing data, such as by using "shadow IT" tools⁴³.

62% 

of businesses are **still struggling** to find the right cybersecurity tools to support employees at home⁴³.

Top Cybersecurity Concerns⁴³:

39% Phishing/clicking on a malicious link initiated by employees

63% Exposing data or information accidentally, (possibly by using shadow it tools or software/tool...)

34% Ransomware

32% Hackers gaining access to proprietary information

52% Cloud collaboration tools may not provide adequate cybersecurity (Zoom call concerns)



25+

The number of malicious email techniques hackers are using **in addition to** phishing scams⁴⁵.

CONSUMERS' DEVICE USAGE IS CHANGING⁴⁴

How has the pandemic changed your habits?

42%

I now **only** use my work-issued devices for work

28%

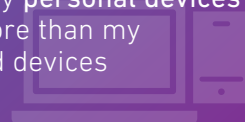
I now **sometimes** use my personal devices for work

20%

I now use my personal and work devices to the **same degree**

10%

I now use my **personal devices** for work more than my work-issued devices



⁴³⁻⁴⁴ Malwarebytes.2021. Still Enduring from Home

⁴⁵ Microsoft. 2021. Digital Defense Report



Why Consumer Responses Fail



Lack of preparedness and planning

No budget

From firewalls, IDs, and tokenization to vulnerability assessments and MFA, most global companies have invested considerable resources into IT security to prevent a data breach. However, even the most walled-off and secure companies can get hacked, and they often do.

To be prepared, your team must answer tough questions.



How much has my company allocated or invested in guaranteed customer response resources?



Have we put aside enough money to ensure our readiness program will deliver the speed, quality, and scale we need?



Are we ready to deliver on our customer response requirements, including Notification, Call Center Agents, and Identity Protection and Restoration Services?

Real-world failure:

An educational system client with over 60 campuses and 2 million employees created a plan but never tested it. After the breach, it was time to execute customer communication, but some campuses realized they had no response budget. While the system still managed to respond, the lack of funding delayed the response by about six weeks instead of responding in days.

Unprepared for customer response

Across emails, social media, and phone calls, a data breach creates a massive communications channel demand from affected consumers. They want details from a real person about what happened and what you're doing to mitigate their identity theft risk. Ask your team: Do we have the resources to handle a worst-case scenario call center spike?

Lack of speed

Regulatory and compliance bodies, including the New York Department of Financial Services (NYDFS) Cybersecurity Regulation, European Union General Data Protection Regulation (GDPR), and the California Consumer Privacy Act (CCPA), require swift action. Is your company ready to comply with the required speed of notification, which is 72 hours in some cases?

No guaranteed SLAs

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.

Untested plan

You've probably evaluated the number of consumers and clients you need to notify and identified your message delivery system, such as first-class mail, email, and substitute notice website, but have you pressure-tested your notification plan—prepared notification letters, tested the secure transfer of files to a mail house, and completed a live call center agent drill?

Unknown customer impact

Companies of all sizes collect and store large amounts of data internally and externally. For a quick response, your team must know precisely where the company's data is and have an accurate accounting of consumer records to notify and support them when a breach occurs.

Real-world failure:

A hospital system was unsure how many consumers were impacted by their breach. The estimates were between 50,000 and 2 million. It discovered it was 1.2 million, then found a new problem: determining the system impact. Since the system didn't keep clean data records, the response team didn't know what PII was affected. The response was clunky and took more time than necessary.

Pro Tip: Basic annual data analysis and knowing details about their data, including storage location and records of internal and external contacts with access privileges, would have prevented a big headache.



Creating Your Plan

Preparation

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

Start With a Strong Response Team.

A data breach can significantly impact businesses of any size. Having a ready-to-go response plan and team in place can help prevent further data loss if a breach happens and also avoid significant fines and harm to your reputation.

Don't wait to discover a breach to decide who will lead the breach management process.

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

- Establishes relationships with necessary external legal counsel before a breach occurs
- Determines when to notify and activate the response team
- Manages and coordinates the company's overall response team efforts, including establishing clear ownership of priority tasks
- Acts as liaison between C-level executives, other team members, and external partners and reports progress and problems
- Ensures proper documentation of incident response processes and procedures
- Coordinates with legal team to understand regulatory notice requirements
- Determines how to notify impacted individuals, the media, law enforcement, government agencies, and other third parties
- Signs off on all incident written materials

CUSTOMER CARE

- Assists in or writes phone scripts
- Logs call volume and top questions and concerns
- Develops and fulfills notifications
- Provides 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.)

“We see many teams meeting for the first time when we kick off the breach response, and with The Great Resignation that’s becoming more common.”



- Anel Linsenbardt

Senior Client Engagement Manager



Convincing the C-Suite

Executive-level participation plays a significant role in the success of a data breach response plan.

Creating and executing a response plan without leadership buy-in makes it challenging to establish a cybersecurity-first culture. Even though their involvement can add tremendous value, many C-Suite leaders and board members often avoid engaging in data breach preparedness discussions and planning.

Case in point: Only 54% of surveyed U.S. organizations say C-suite executives and board of directors are informed and knowledgeable about how their companies plan to respond to a data breach⁴⁷.

To raise awareness and get support, cybersecurity, legal, communications, and other relevant organizational leaders must drive home the financial and reputational stakes involved if there's a failed or insufficient data breach response.

Collaboration

85% of U.S. organizations believe increased senior executive participation and oversight could make their data breach response plan more effective⁴⁶.

Use this data to get your C-Suite on board:



70% of U.S. organizations experienced a data breach that resulted in the loss or theft of over 1,000 records with sensitive or confidential material in the last two years⁴⁸



\$570,000:
Average ransom payment in 2021⁴⁹



44% of data breaches included customer records with PII⁵⁰



\$161:
Average cost per lost record⁵¹



\$4.24 million:
Global average cost of a data breach⁵²



287 days:
Average amount of time it takes to identify a data breach⁵³



\$9.05 million:
Average cost for US organizations⁵⁴



\$2.46MM:
average savings from having an established incident response team with a tested response plan⁵⁵



Breaches where remote work was a factor cost an average of **\$1.07MM or 24% higher**⁵⁶



39%:
More than one-third of executives feel they could lose their jobs over a successful ransomware attack⁵⁷

⁴⁶⁻⁴⁸ Experian and Ponemon. 2022. Ninth Annual Study: Is Your Company Ready for a Big Data Breach?

⁴⁹ Info Security Group. "Average Ransomware Demands Surge by 518% in 2021," August 2021

⁵⁰⁻⁵⁶ IBM & Ponemon 2021 Cost of a Data Breach Report

⁵⁷ Mimecast "State of Ransomware Readiness: Facing the Reality Gap" Report, November 2021



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.



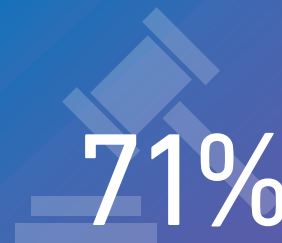
Understanding Influencers Impact on a Breach Response

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 law enforcement involvement. Establishing a relationship with your local FBI cybersecurity officer before a breach will serve you well when responding to an active incident. During an incident, law enforcement can explore evidence to determine if a crime occurred. In some cases, law enforcement discovers the breach before other parties.



71%

of data breach response plans globally, and 72% in the U.S. include procedures for communicating with state attorneys general and regulators. However, only 17% of organizations have met with law enforcement or state regulators in preparation effective⁵⁸.

Recruit The Right Breach Resolution Partner

Here are five critical qualifications to consider when hiring and evaluating your external response team:

1. Relevant Relationships

Partners should be certified, have detailed knowledge of the data breach life cycle, collaborative relationships with government stakeholders and regulators, including attorneys general, and experience supporting different data breach types.

2. Experience Handling “What If” Scenarios

Partners should provide compelling insights, counsel and relevant tools throughout the data breach life cycle to help execute a successful 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. 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.

5. Ability to Respond Quickly

Select partners that guarantee speed with SLAs to ensure that you have the fastest response.

⁵⁸ Experian and Ponemon. 2022. Ninth Annual Study: Is Your Company Ready for a Big Data Breach?



Cyber Insurance Considerations

There is a growing interest in and increasing need for businesses to acquire cyber insurance. However, insurance is becoming more expensive and challenging to obtain at the same time due to the rising response and resolution costs and the frequency of data breach occurrences.

Year of the Rate Increase

While there has been an increase in the availability of cyber insurance policies, companies are still playing catch up to secure it. In 2021, **53% of companies surveyed had a cyber insurance policy**, up from 49% of companies only a year before, according to the Experian and Ponemon Ninth Annual Data Breach Preparedness Study: Is Your Company Ready for a Big Data Breach?⁵⁹ Among companies not currently holding a policy, 71% said they had plans to purchase, an increase of 10% from the previous year, according to the study⁶⁰.

Shifting Burden of Proof

In 2022, cyber insurance requirements will take a hard right, with attestations becoming a thing of the past. This year, policyholders will need to explicitly prove, with proper documentation, that the breach controls they attest to have are actually in place. In other words, the burden of proof will fall on the company seeking cyber insurance, not the insurance company.

Rising Costs

Another 2022 trend: higher premiums (sector-dependent). For example, in some cases, the healthcare industry and Medical Service Providers will see triple-digit increases⁶².



Staying Insured

Keeping a policy will become more difficult in 2022. Organizations that cannot verify proper controls will not receive renewal, even in cases where the company has had a longstanding policy in place with a particular insurer. Also, since only about one-third of companies have cyber insurance, most will rush to hire cybersecurity counsel post-attack, creating more stress and delays since it can take months for large companies or those without backup, to determine the extent of the damage⁶³.

Choosing a Legal Partner: A Checklist

A data breach is a complicated issue that requires a legal team with cybersecurity experience. Use this checklist to judge your options and make sure you hire the right firm. Your partner should have:

- ☐ Experience that extends beyond legal notification
- ☐ Previous success managing data breaches
- ☐ Established relationships with state attorneys general and other relevant regulators
- ☐ Breach counsel and technical investigations knowledge
- ☐ Ability to deliver relevant case law insight
- ☐ External expert relationships to support your response team



^{59, 60} Experian and Ponemon. 2022. Ninth Annual Study: Is Your Company Ready for a Big Data Breach?

^{61, 62} Security InfoWatch, "The Future of Cyber Insurance: What to expect in 2022," December 2021

⁶³ Washington Post, "Ransomware claims are roiling an entire segment of the insurance industry," June 2021



Breach Response Provider Review

Your provider should guarantee:

- Resources and routine consumer-facing response readiness exercises
- Dedicated team and infrastructure to scale response with speed and quality
- Expert, best-practice-backed readiness advice developed from proven experience and success managing large and complicated responses
- Experience leading or participating in customer-facing breach response exercises focused on plan stress testing and gap identification
- Background in collaborating with internal and external cross-functional incident response teams to help create and execute a customer-facing breach plan, including operational notification details, customer support, and identity protection services
- Ability to back up the plan with robust notification, call center, and identity protection services

Crisis Communications Capabilities

From channel selection to spokespeople, a sound crisis communications process is critical to a successful response. Make sure your team is ready to respond.

For starters, add an internal and, if possible, an external communications contact to your team and ensure they are a part of all legal and forensic meetings. Next, **develop a thorough communications plan** and approval process to efficiently create multi-channel internal and external communications. Finally, include communications to notify and address your audience's concerns, including your employees, customers, regulators, and business partners.

Additional Communications Considerations:

Prepare Your Collateral: Create documents your team can efficiently distribute with quick tweaks, including specific incident statements, FAQs for consumers, investors, and media, as well as leadership messages to consumers and employees.



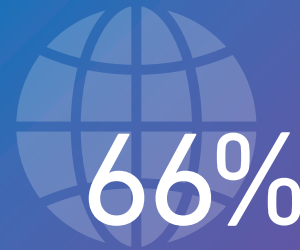


The Global Standard

Global data breaches require a well-coordinated response. With mandatory personal data breach laws on the books in 71 countries, 88⁶⁴, if you include countries with dependencies, managing the data breach consumer response in today's interdependent and interconnected world is becoming more regulated. Despite the growth of global data breaches, with **56% of U.S. companies reporting a global breach**, only 29% of companies say they are confident enough to deal with an international breach⁶⁵. And that's not all.

Accountability rules are also evolving, evidenced by the recent broadening of the definition of **Joint Controller**, which now states that two or more persons or entities are in charge of collecting and protecting consumer data and can be held responsible and face sanctions. The change is significant since **50% of global breaches in 2020 occurred because of supply chain third parties**⁶⁶, which exposed more organizations to increased risk.

On the compliance front, in 2021, GDPR saw an increase in non-compliance fines due to new challenges faced by companies, consent issues, the pandemic, and the growing remote workforce. Even a corporate giant like Amazon must comply. In the summer of 2021, the online retailer was hit with the largest **GDPR fine of \$887 million**, exceeding all previous penalties combined⁶⁷.



of incident response plans for U.S. businesses include processes for managing international breaches effective⁶⁸.

NEW PRIVACY LAWS

In 2021, China passed two new laws, the **Data Security Law** and the **Personal Information Protection Law**. DSL, which applies to data use and processing, outlines security requirements to safeguard data with sanctions, including fines and business revocation or suspension. It also requires prompt notifications of breaches and remedial measures with fine implications. Similar to GDPR, PIPL covers information processing of Chinese citizens, even when processed outside of the country.

⁶⁴ DLA Piper Global Data Protection Laws of the World Handbook

⁶⁵⁻⁶⁸ Experian and Ponemon. 2022. Ninth Annual Study: Is Your Company Ready for a Big Data Breach?



Data breaches don't have borders.

Take the following steps to better prepare for an international breach.

Step 1

Coordinate a global response team:

To execute a quick response, your planning team should include internal support, third-party partners, legal counsel, communications specialists, a data breach resolution provider, and a forensic expert.

Step 2

Prepare for increased stakeholder engagement:

New international regulations bring new stakeholder groups, which companies must engage. Your company must identify these key stakeholders and 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, contacting regulators early on can reduce scrutiny and help streamline the response process.

Step 3

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 promptly notify and address consumer concerns. This multi-faceted approach includes ensuring impacted parties receive notifications in the correct language and get access to a secure, multilingual call center. Another consideration is whether your company will offer identity protection services to affected consumers. While not mandated, these services can help address uncertainty and stress for those impacted by the breach and ultimately help improve a company's reputation post-breach.

Global Data Breach Preparation Basics

1. Assemble an expert, cross-functional internal and external response team
2. Increase your stakeholder engagement capacity
3. Ready your consumer notification and support process





Conduct Routine Response Exercises

Did you know?

84% of organizations say that their breach response plans could be more effective if they conducted more fire drills to practice⁶⁹.

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.

Team Responsibilities

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 their department.

EXERCISE ACTIVITIES:

- Conduct employee security training and retrain at least annually.
- Work with employees to integrate smart data security efforts into their work habits.
- Limit the types of hard and electronic data employees can access based on their job requirements.
- Update security measures regularly.
- Invest in the appropriate cybersecurity software, encryption devices and firewall protection.
- Establish a method of reporting security incidents to the incident team and for employees who notice others not following proper security measures.
- Develop and update data security and mobile device policies regularly and communicate them to all business associates.

⁶⁹ Experian and Ponemon. 2022. Ninth Annual Study: Is Your Company Ready for a Big Data Breach?



Developing a Response Drill

Ideally, you should set aside at least four hours for your drill to run through multiple scenarios your organization may face. The scenarios should be pertinent to your industry, the type of data you collect and consider your IT infrastructure build. Since a real-world response will likely take weeks, not hours, you can allow for a degree of imagination during your drill. However, for context, here are four actual scenarios from recent years to give you an idea of how an exercise can play out.

Sample Scenarios

- The FBI contacts your company because they suspect a dark web user has your consumer's usernames and passwords. The user is selling the data to the highest bidder. The agency recommends investigating the matter and concludes it's only a matter of time before the press gets word of the situation.
- A hacktivist organization sends your company a note claiming to have personally identifiable information (PII) of your consumers, including names, addresses, DOB, and SSNs. They threaten to release the data if you don't meet their 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 log complaints about receiving a 5071-C letter from the IRS suggesting someone may have filed a fraudulent tax return in their names. Similarly, employees get an email from an "executive" requesting 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 if they do not receive a detailed account of the incident.
- Forensics updates informing the IT teams of additional details on impacted systems and lost information.
- Mock angry emails or phone calls from consumers or employees about the incident.



⁷⁰ Experian and Ponemon. 2022. Ninth Annual Study: Is Your Company Ready for a Big Data Breach?



Implementing a Response Drill

To be effective and give your organization a solid chance to identify gaps or weak spots, you must repeatedly practice your data breach response plan. Despite security awareness increasing as well as the number of companies with a response plan in place, they are still not being practiced adequately.

IS YOUR COMPANY'S RESPONSE PLAN READY TO GO? CHECK THE LIST BELOW.



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

Allow at least four hours to conduct the exercise, review action items, identify gaps and discuss challenges.



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:

- The C-Suite (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
- External Partners (Legal counsel, public relations, forensics firm and public relations firm, data breach resolution provider and cyber insurers)

“Even if you’ve created and practiced your breach response plan, it can become outdated in a matter of months. When it comes to testing your plan, be proactive.”



- **Apiyo Obala**
Account Director and Team Lead



Preparedness Checklist: Are You Ready?

Here are some questions to help you evaluate your level of preparedness. If you leave any box unchecked, gather your team immediately to address your gaps.

RESPONSE PLANNING

- ☐ Do you have an internal response plan and team assembled to execute it?
- ☐ If you currently have a preparedness plan, have you tested and audited in the last six months?

SECURITY PLANNING

- ☐ Have you inventoried the types of information you store that could be at risk for exposure 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

- ☐ In the last 12 months, have you conducted a data breach crisis tabletop exercise or drill to test how effectively your company would manage a significant incident? If so, did this exercise incorporate international 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 the contracts have guaranteed response timelines?
- ☐ Do you have a relationship with state attorneys general to contact to ensure state guidelines compliance?

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?



Auditing Your Plan

Creating a preparedness plan is one of the biggest challenges to positioning your organization for success. Clearing this step is mission-critical.

To ensure your plan is always ready to respond, make it a priority to:

- Audit it quarterly
- Test it every six months
- Share it with new incident team members as they onboard
- Keep the contact information current

Also, remember to run through as many incident scenarios as possible and evaluate how your plan would hold up to each one, including an internal breach, external attack, accidental data sharing, and loss or theft of a physical device.

Quarterly Audit Questions

Staying on top of your quarterly audit allows you to adjust your plan based on new and unexpected threats. Consider the following questions when updating your plan.

- Are your communications workflows ready to respond?
- Have you conducted an end-to-end response drill based on your current environment?
- Are you confident in your capacity and your vendor's ability to respond to an industry-wide event?
- Will your breach response provider continue to guarantee response times?

If your answers are anything other than a strong "yes," then continue planning and updating to ensure readiness.



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.



Focus Areas

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:

- Scale your call center: You need to be able to adapt to any breach, large or small.
- Conduct ongoing crisis training: Make sure your representatives are ready to handle sensitive information and emotional callers.
- Swiftly pull together training materials: Informed and empathetic call center representatives can positively impact your brand during a crisis.
- Test, test, and test again: Conduct daily to ensure your agents can handle breach-related calls.

VENDOR NEGOTIATIONS

Selecting vendors that have and follow appropriate data processing security measures must be a priority to help avoid vendor-triggered data breaches. Your team should also contractually obligate your vendors to maintain sufficient data safeguards and regularly assess their performance for added security and confidence.

Require your vendors to:

- Maintain a written security program covering your company's data
- Only use customer data for contracted services
- Immediately communicate 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 breach response plan



Responding to a Data Breach

Breach Discovery

Over 80% of socially engineered breaches are discovered by external parties⁷¹.

The first 24

What you do in the first 24 hours after a breach is critical



Record: Document the moment of discovery, the date and time your response efforts begin, i.e., when the first member of your response team receives breach notification, and what type of breach occurred.



Alert and activate: To launch your preparedness plan, notify your entire internal and external response team and law enforcement if your legal team and C-Suite advises.



Secure: To help preserve and protect evidence, secure the data breach site and its surrounding areas.



Stop and unplug: To prevent additional data loss, take affected machines offline, but do not turn them off or start probing into the computer until your forensic team arrives.



Interview and Document: Every detail matters. In collaboration with your legal team, always collect, document, and record all available information about your data breach and response activity promptly, including conversation notes and emails with law enforcement.



Review: Go over notification protocols that touch on communication information about the breach for everyone involved in this early stage.



Assess and prioritize: Based on what you know about the breach, rank your risks and priorities and work with your forensics firm to begin an in-depth investigation.

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 DATA BREACH LIFECYCLE

- Data incident is discovered
- External legal counsel is engaged
- Forensics determines "who" and "what"
- "Go/No Go" for consumer response
- Public Relations drafts 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)

⁷¹ Verizon 2021 Data Breach Investigations Report



On day two, compare your progress against your plan, then:

1 IDENTIFY THE CAUSE

- ☐ Have your forensics team remove hacker tools and address any other security gaps.
- ☐ Document when and how you contained the breach.



2 ALERT EXTERNAL PARTNERS

- ☐ Notify your partners and include them in the incident response moving forward.
- ☐ Engage your data breach resolution vendor to handle notifications and set up a call center.



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 UPDATE THE C-SUITE

- ☐ Generate reports that include all breach details and 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 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 re-train employees in their specific response roles and their security and privacy practices.



Managing Communications and Protecting Your Reputation

Along with the direct financial impact of a security incident, companies also have to consider the potential damage to their reputation and relationships with their consumers. Understanding best practices before an incident happens and preparing proper crisis communications strategies and messaging is critical.

While early planning is a core component of successful security incident management, organizations must always expect the unexpected. Data breaches often cause a windfall of misinformation and confusion, and 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 follow:



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 send 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 a breach also increases the possibility that your company will face some form of litigation. Because the litigation risk is exceptionally high, you should take steps to protect the legal privilege of the response process.

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



Mark all written materials “privileged and confidential” and add a legal department team member to your distribution list.



External counsel should handle all external partner contracts, so their work is part of the course of providing legal counsel to your organization.



Be thoughtful about what information you document and put in writing versus what you should discuss in-person or on a phone 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, 87% of consumers are willing to walk away and take their business elsewhere if or when a data breach occurs, and 32% say they will leave a business because of a data breach whether or not their information was stolen. Additionally, over half (55%) of consumers believe that companies aren't doing enough to protect their data⁷².

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.



⁷² Experian and Ponemon. 2022. Ninth Annual Study: Is Your Company Ready for a Big Data Breach?



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*

*The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company under group or blanket policy(ies). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions. Review the Summary of Benefits.



WHY ARE CREDIT SOLUTIONS A PART OF IDENTITY THEFT PROTECTION PROVIDED TO BREACH VICTIMS?

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.

⁷³ Experian and Ponemon. 2022. Ninth Annual Study: Is Your Company Ready for a Big Data Breach?



Managing Your Crisis Response



A Crisis Response Management plan allows you to communicate with your consumers when you need it most.

When an incident occurs, our team of experts taps into the power of Experian's notification system, multilingual call centers, and crisis specialists to build a custom and effective notification plan that will notify your consumers about relevant incident details and potential threats.

Crisis Response Management is a non-breach system that can fill in the existing infrastructure gaps, making executing both U.S. and international communication possible across digital and print channels.

"The pandemic has shown organizations that staying ready for a data breach is non-negotiable. Having a strong plan to keep your customers informed is also an important preparedness step."

- Kyle Walker
Account Manager



Crisis Management Scenarios



Scenario 1:

You are a healthcare provider, and your technology outage results in consumers losing online account access.



Scenario 2:

You are a small business, and your digital store goes down weeks before a major holiday.



Scenario 3:

You are a financial institution that needs to update your consumers, but you don't have the notification or call center infrastructure to support the response.



Experian Reserved Response™

Experian® Reserved Response™ is the first and only industry data breach program that guarantees the workforce, infrastructure, and response readiness your company needs with service level agreements (SLAs) with built-in penalties if our response fails. But don't worry, we have you covered. Our experienced and dedicated team has handled thousands of high-profile breaches in nearly every industry, all without missing a single SLA.

Our Take Charge Technique

Our partnership success relies on Experian's proactive and proprietary Response Ready™ process, which 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
- Collaborating with your internal and external incident response teams to build a customer-facing breach response plan that delivers notification, support, identity protection services, and more.
- Detailed response drills designed to trial run your plan and identity and address gaps.
- Yearly planning evaluation to ensure your plan and team are up to date.

A tested plan can save your organization time and money when a data breach happens. With thorough and repetitive training, your staff will be ready, although you may require additional resources to deal with the inevitable spike in communication needed to respond.

\$2.46MM

is the average organizations can save by having an established incident response team with an extensively tested response plan⁷⁴.

Guaranteed and Scalable

Experian® Reserved Response™ delivers the guaranteed breach response, workforce, and infrastructure you need to execute a customer-facing response for a breach of any size. With Experian, you can be ready to execute in as little as three days with guaranteed SLAs, unlike our competitors, who can take up to five days.

Experian's service also includes:

- Preconfigured annual templates and workflows
- Dedicated account manager to supervise your rapid response
- 24-hour compliance review and turn-around to ensure you won't miss notification requirements
- Penalties if we miss an SLA
- Full-service notification services, including template letters, custom messaging, address verification, printing, and mailing
- Dedicated 24/7 toll-free number call center with US-based agents
- Multiple levels of data breach protection available for your customers and employees
- Ongoing reporting of call centers, notification, enrollment, identity theft, and fraud resolution metrics to share with key stakeholders and regulators

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.

⁷⁴ IBM and Ponemon. 2021. 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. 2021. Data Security Incident Response Report
<https://www.bakerlaw.com/>
- Experian and Ponemon. 2022. Ninth Annual Study: Is Your Company Ready for a Big Data Breach?
www.experian.com/NinthAnnualStudy
- Forbes. 2020, March 21. FBI Coronavirus Warning: 'Significant Spike' In COVID-19 Scams Targeting These Three States
[www.forbes.com/FBI Coronavirus Warning](https://www.forbes.com/FBI-Coronavirus-Warning)
- IBM and Ponemon. 2021. Cost of a Data Breach Report
www.ibm.com
- Identity Theft Resource Center. 2021 Annual Data Breach Report
www.idtheftcenter.org
- Identity Theft Resource Center. 2021. 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. 2021. Digital Defense Report
www.microsoft.com
- PwC. 2022. Digital Trust Insights Pulse Survey
www.pwc.com
- RiskBased Security. 2020. 2020 Mid Year Data Breach QuickView Report
pages.riskbasedsecurity.com
- Verizon. 2021. Data Breach Investigations Report
enterprise.verizon.com
- VMware Carbon Black. 2021. Modern Bank Heist 4.0
www.carbonblack.com



About Experian® Data Breach Resolution

When every minute counts, count on Experian Crisis Solutions, a leader in helping businesses plan for and mitigate consumer risk after a data breach.

Powered by the nation's largest credit reporting agency, Experian Crisis Solutions creates better outcomes and unmatched value by delivering expertise, ease, and guaranteed speed when our partners need it the most. With over 15 years of experience, Experian Crisis Solutions has successfully serviced some of the largest and highest-profile breaches in history.

Our turnkey solutions include data breach resolution, Experian Reserved Response™, crisis response management, and proven credit and identity protection products. Our swift and effective incident management, notification, call-center support, and reporting services support millions of affected consumers.

Experian is ready to help you plan for and respond to a data breach.

**Contact us now at 1.866.751.1323 or
databreachinfo@experian.com**