An Experian Data Breach Response Planning Guide

How to prepare your business for a consumer facing data breach response

Edition 2021

Responding with confidence in a crisis

Foreword

Preparing in advance of a data breach means you will have a plan and team of experts ready to respond with confidence.

Day-to-day life has changed beyond recognition for many of us during the COVID-19 era. We've seen businesses face a completely new set of operational challenges, from how they interact to do business, how consumers utilise their services to the way our teams come together to deliver the next generation of services. Put simply, the entire business ecosystem has needed to take an unprecedented new perspective on how they do business.

This evolution is still evolving and will do so for some time and this change has presented cyber criminals with new opportunities to target businesses and attempt to access personal information of customers and employees.

In the following guide we provide a comprehensive perspective and outline of some of the key steps businesses can take to develop a strong and effective data breach response plan before it happens. The reality is the longer it takes for a business to respond, the more challenging it can be for a business to maintain the company's reputation and protect its brand and the knock-on effect to customer loyalty.

In this new world we strongly believe if businesses can work on their response planning and understand the potential challenges they could face they will be in the position to respond more confidently and protect consumers when a data breach happens.

Sincerely,

Jim Steven
Head of Data Breach Response Services, Experian UK

Contents

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

Introduction

The purpose of this guide

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 can create a challenging environment well beyond the initial intrusion for a business.

More data is available than ever before, so while there may be fewer data breaches, the amount of data at risk from 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 2019. The vast majority of these exposed records came from three data breaches, which were a 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.[1]

With a rising threat to personally identifiable information (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. Customers concerns around their personal data and increasing expectation that businesses will safeguard the information shared is of no surprise. Customers want to be assured that if their personally identifiable information (PII) was part of a data breach that the business would respond and help and support them.

The lost business from operational downtime, customer turnover and increased acquisition costs due to damage to 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, businesses can feel the financial impact of a data breach for years to come.[2]

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.[3] The only way to respond quickly is by having a data breach notification response plan already in place, which can be quickly put into play.

How important is a response plan to consumers?

Our 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.[4]

The threat of identity theft can be extremely stressful for those individuals affected so the ability for the business to respond quickly can give customers peace of mind that the business is on top of the breach and its potential aftermath. However, in order to respond and provide this peace of mind to customers the ability reach out to them directly and inform them is crucial.

[1] RiskBased Security. 2020. Mid Year Data Breach QuickView Report
[2] IBM and Ponemon. 2020. Cost of a Data Breach Report
[3] Experian. 2019. Data Breach Consumer Survey
[4] Experian. 2019. Data Breach Consumer Survey

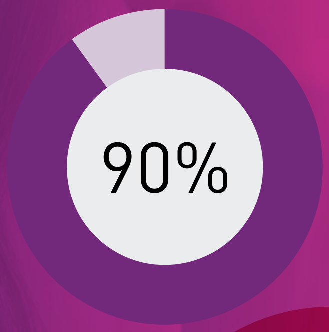
Individuals will want to know how you are going to help them protect themselves and they want to know if you will provide credit and web monitoring services. They want to be able to talk to a someone within the organisation or who can represent the organisation in answering some of their crucial questions 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 the individuals affected.

For businesses who are just starting to think about developing a data breach plan or for those looking to update current practises, this guide illustrates what a comprehensive data breach response plan should look like and how to implement one in a way that meets the potential challenges that could lie ahead.

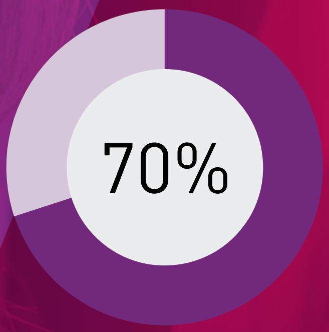
The purpose of this guide

Experian's Data Breach Response Guide is designed to support organisations prepare for a data breach response. This information will support the creation and implementation of a data breach response plan in the crucial first 24 hours after a data breach. It provides considerations when planning to notify individuals affected and addresses some of the key steps in creating, implementing and improving a response plan.

Each organisation will need to consider the type of data it processes alongside the information provided within this guide. If you already have a data breach response plan in place, this guide can help you assess how fit-for-purpose it is. If you do not have a plan, this guide can help you create one. Time is of the essence. It's also important to highlight how quickly customers expect to be contacted in the event of a breach, compared to what organisations feel is necessary. A pattern is certainly emerging once again, with customer expectation in relation to speed of notification being far greater than what businesses feel is an adequate timeframe.



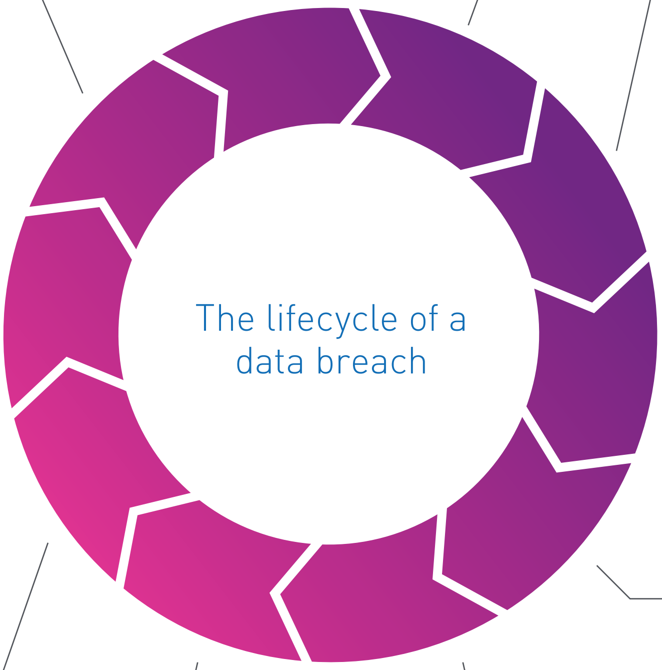
Of consumers re more forgiving of a company with a response plan in place prior to the breach



of consumers would stop using a company with a poor consumer response

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.

The lifecycle of a data breach



Resume business as usual
It is key to always remain focused on being ready for a breach.

Respond to enquiries
Ensure you have resources to answer enquires through a call centre is essential as people may want to call or email in to discuss any concerns.

Letter notifications
When notified of a breach, consumers want to see facts about the breach, information about the risks they may face, steps they can take to protect themselves and the offer of credit monitoring and/or identity protection.

Make public announcement & launch breach website
Transparency is an important part of rebuilding trust.

Begin notification communications to individuals affected
Keep up-to-date on EU Regulatory notification laws.

Discover breach
Attacks occur via a variety of sources e.g. internal error, malicious activity, cyber attacks, etc.

Investigate & remediate
The sooner you terminate the infringement, the sooner you can begin the resolution process.

Assemble internal response team
Appoint an Incident Leader to head up your data breach response team.

Contact relevant authorities
If applicable, notify any relevant authorities (such as the Police) and submit any necessary reports.

Employ external partners
External partners include Forensics, Data Breach Response Partner, Lawyers and PR experts.

An 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%.[5]

The Identity Theft Resource Centre 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.[6]

Data breaches can also be particularly expensive in financial services. 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.[7]

[5] VMWare Carbon Black. 2020. Modern Bank Heists 3.0
[6] Identity Theft Resource Center. 2020. 2019 End of Year Data Breach Report
[7] IBM and Ponemon. 2020. Cost of a Data Breach Report

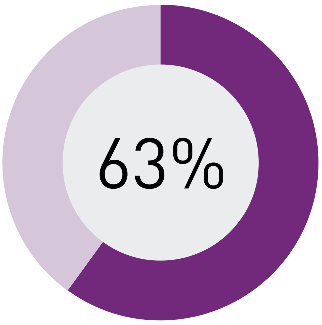
Small and Medium-Sized Businesses

The threat of data breaches impacts every business, large and small. In the aftermath of a data breach, companies may deal with financial loss, potential hefty fines, a reputational hit and potential loss of customers. A data breach can be as devastating to large enterprises as it is for smaller companies.

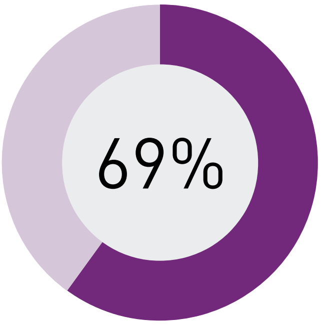
While the average cost of a data breach has fallen for the smallest companies (down to $2.35 million for companies with fewer than 500 employees), data breaches continue to have disproportionately higher relative to the number of employees when compared to large firms. Medium-sized organisations saw an increase in average data breach costs compared to previous year.[8]

In recent years, data breaches have also become more prevalent for SMBs, and cyber-attacks 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).[9]

Some SMBs may falsely believe they won't be targets if they do not 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.[10]



of SMBs reported experiencing a data breach in the past 12 months



of SMBs say they agree that cyberattacks are becoming more targeted

[8] IBM and Ponemon. 2020. Cost of a Data Breach Report
[9] Keeper Security and Ponemon. 2019. Global State of Cybersecurity in Small and Medium-Sized Businesses
[10] Microsoft. 2020. Digital Defense Report

Ecommerce

More and more organisations are going online in an effort to engage and expand into the connected online world. With this comes the challenge of managing the valuable real estate and brand, which is open more frequently to potential hacks. The need for a secure online website interfaces has become an absolute necessity. With focus on point of sale where customer's personal information is of particular interest to criminals. This means organisations are putting more focus on continually improving servers, software and card payment platforms as hackers look for new ways to access personal information, which can then be sold on.

Cybercriminals

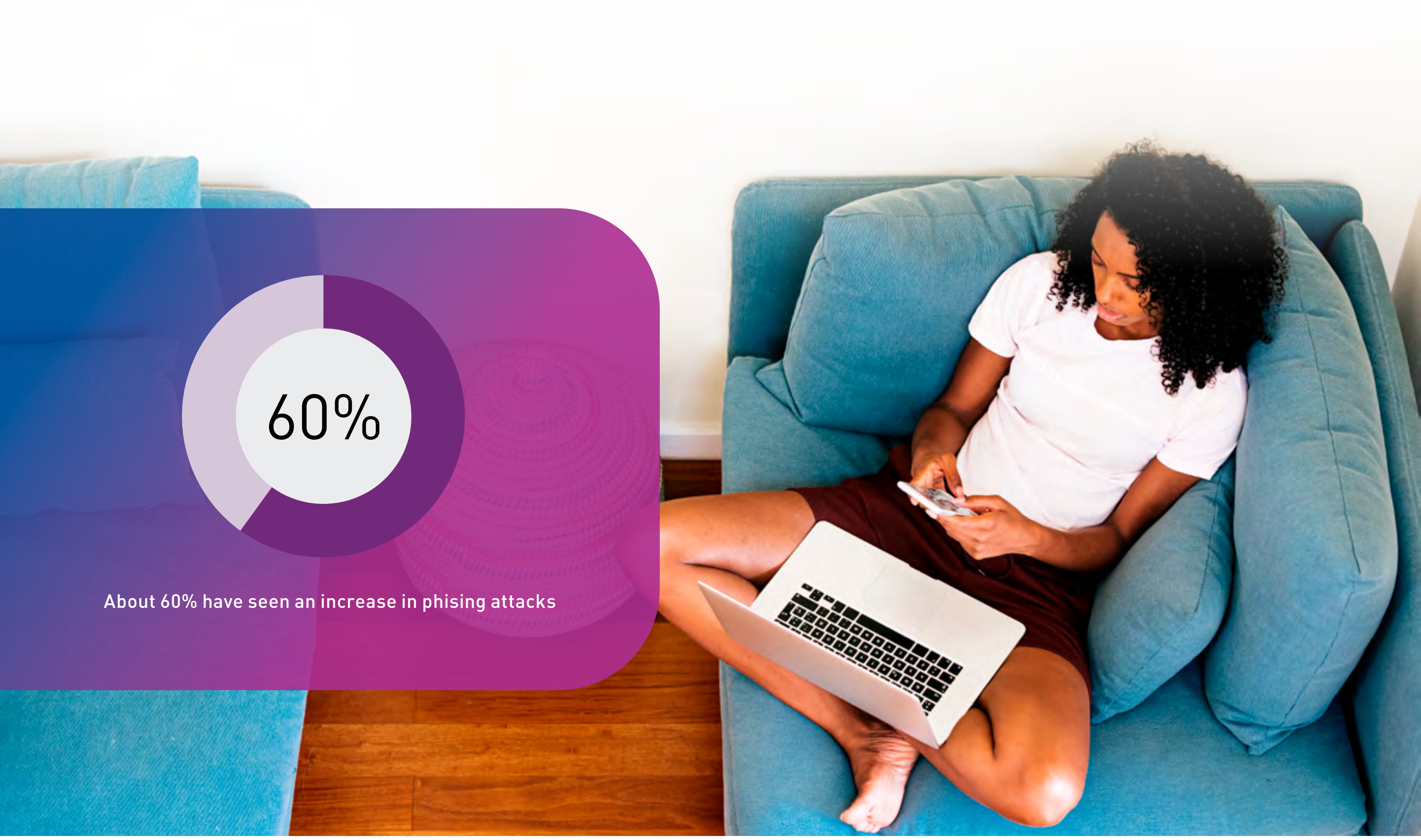
The world of cybersecurity is evolving

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).[11] However, criminals and state actors are also finding new ways to infiltrate corporate networks.

Taking advantage of evolving business operational practises

Cyberattacks are moving away from some of the old familiar methods to modern approaches. Or better put, cybercriminals go to where the action is. For example, the rapid shift to remote working has opened companies up to new vulnerabilities. Chief information security officers (CISOs) were asked about the incidence of attacks related to COVID-19. Over half said they've seen and expected an increase in risk from the use of non-enterprise devices or software due to remote working. About 60% have also seen and expected an increase in phishing attacks.[12]

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 organisations, doctors or scientists and use fear or false hope as a hook. Securing devices may also be more difficult for companies.



About 60% have seen an increase in phising attacks

[11] Verizon. 2020. Data Breach Investigations Report
[12] PwC. 2020. Digital Trust Insights Pulse Survey

Criminal tactics and techniques

AI, cloud and new era technology and cyber attacks

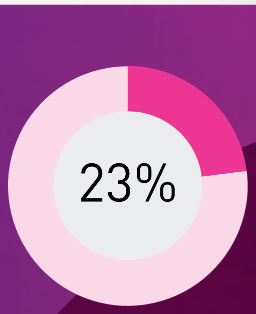
While developments in artificial intelligence (AI) and machine learning (ML) enable cybersecurity professionals to predict and identify potential threats, these technologies present a double-edged sword as more and more hackers leverage them to create more sophisticated attacks.

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.

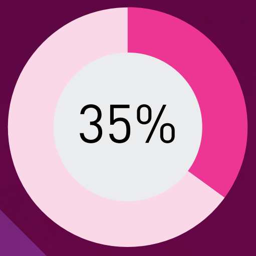
There's also been a trend in cybercriminals using popular cloud, email delivery and file-sharing services in addition to compromised web hosting infrastructures to launch phishing campaigns. The campaigns are frequently changed in an attempt to avoid detection, and a variety of phishing delivery methods 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. 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 organisations 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.[13] This may be a particularly important area of focus in the future. In the first half of 2020, there was an approximated 35% increase in attack volume on IoT devices.[14]



of organisations said they were highly or fully prepared (7+ out of 10) to deal with an IoT-based attack



increase in attack volume on IoT devices

While anticipating the next approach cybercriminals will make is nearly impossible to predict. Taking a look at previous and current trends help to identify potential threats 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.

[13] Experian and Ponemon. 2020. Seventh Annual Study: Is Your Company Ready for a Big Data Breach?
[14] Microsoft. 2020. Digital Defense Report

Engaging C-suite in the plan to protect and prepare the business

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

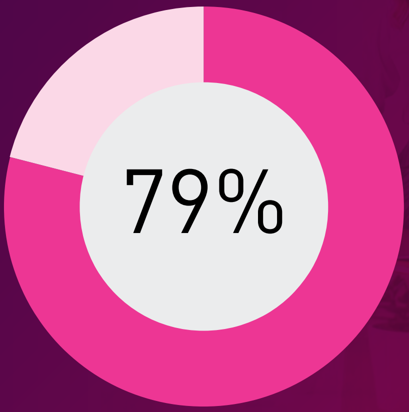
Lack of leadership engagement in the creation and implementation of a response plan can cause organisations significant challenges in creating a culture of cybersecurity.

Despite the importance of their involvement, many Boards of Directors, Chairperson and CEOs are not actively engaged in the responsibility of data breach preparedness.

A little more than half of surveyed organisations (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.

Organisations 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, reputational standing and customer loyalty.

How engaged is the organisation?



of organisations believe increased participation and oversight from senior executives could make their data breach response plan more effective.

Planning to put your business in a stronger position

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

Like most global companies, you may have invested in IT security to ensure a data breach does not occur – firewalls, IDS, tokenisation, MFA, security services, vulnerability assessments, penetration testing, etc. But we all know that even the most prepared/most secure companies could get hacked. Given the reality in IT, can you determine:

- How much has my company budgeted or invested in guaranteed customer response resources?
- Have we invested in a comprehensive readiness program to ensure a successful response at speed, quality and scale to consumers?

Are we proactively prepared to deliver on our customer data breach response requirements of – Customer notification, call centre and response support (agents) and web or credit monitoring services?

It is challenging to estimate the number of inbound customer calls, emails, or messages expected

A data breach can create a 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 incoming phone calls. When people believe their identity information has been compromised, they may prefer to speak to an expert who can help them understand (1) what has happened and (2) what is being done to mitigate their risk. So, it's important to consider how many calls, emails and/or messages could occur in the worst-case scenario and whether there are enough resources to meet the demand whilst continuing business as usual.

The notification plan has never been tested by a live drill

You have 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 commentary in the notification letters and tested the secure transfer of files to a mail house) with a live drill talking with a live call centre agent. Crucially testing out each element of the process and resources to completion to understand resource and capability.

The maximum number of customers that could be breached is unknown

Given data archive plans, multiple data centres, cloud service providers and other business realities many companies proclaim, "We have data everywhere!" How accurate is your current data "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 call centre experts to service incoming calls to the business

Many companies have internal call centre resources or utilise outside call centre help should an event occur. However, it is important to understand 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

Importantly you may need to notify a number of regulators and bodies of a data breach including, The Information Commissioners Office (ICO) and The Police. Understanding who within your jurisdictional environment to notify is a key preparation step to take in this initial process.

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

Creating your plan

Build a strong team of response experts

Regardless of the size of your organisation, 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 operational business and reputation.

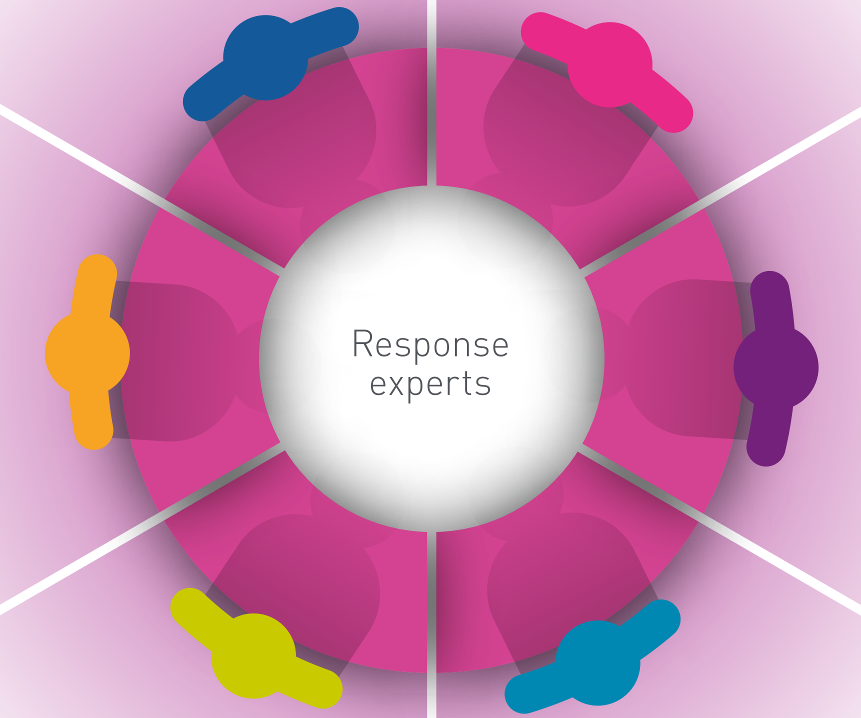
If you are waiting until the discovery of a breach to decide who will be responsible for leading and managing the incident, you could severely hamper your ability to respond quickly and effectively. A response team should be assembled well in advance and involve the coordination of multiple departments.

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 the appropriate documentation of incident response processes and procedures.
- Coordinates with legal to understand regulatory notice requirements.
- Determines how to notify affected individuals, the media, regulators, government agencies and other third parties.
- Establishes relationships with any necessary external legal counsel before a breach occurs.
- Signs off on all written communications and materials related to the incident.

Customer Care

- Assists in or crafts phone scripts.
- Logs call volume and top questions and concerns.
- Crafts and fulfils notifications.
- Provides a dedicated call centre and email response capacity



HR

- Develop internal communications to inform current and former employees
- Organise internal meetings or webcasts for employees to ask questions

C-Suite

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

PR/Corporate Communications

- Determines the best notification and crisis management tactics before a breach ever occurs.
- Tracks and analyses media coverage and quickly responds to any negative press during a breach.
- Crafts consumer-facing communications related to an incident (website copy, media statements, etc.)
- Creates 'Frequently Asked Questions' document and responses for incoming queries.

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 jeopardising evidence and progress.
- Considers what regulatory and support bodies, such as The Information Commissioners Office requirements will be.

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.

Engage external partners:

Crisis communications partner

Communications partners should have experience helping companies manage highly publicised 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 partners

- Forensics partners have the skills to translate technical investigations of a data breach into enterprise risk implications for decision-makers within the organisation.
- Advises your organisation on how to stop data loss, secure evidence and prevent further harm.
- Preserves evidence and manages the chain of custody, minimising the chance of altering, destroying or rendering evidence inadmissible in court.

Customer first data breach response partner

- A data breach response 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 credit and web (identity) monitoring service.
- Offers an enhanced call centre 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 that are included within the scope of work.

Legal counsel

- Legal partners will have established relationships with local regulatory entities, such as The Information Commissioner's Office to help bridge the gap during post-breach communication.
- They will indicate what to disclose to avoid creating unneeded litigation risks based on the latest developments in case law.
- Ensures anything recorded or documented by your organisation balances the need for transparency and detail without creating unnecessary legal risk.

Key influencers and regulators

It is important to establish relationships early with appropriate regulatory bodies, including Information Commissioners Office and Police Cyber Crime Unit to streamline the process and timeline in the event of a data breach.

- Create a list of key contacts aligned to the appropriate regulatory notification requirements. Regularly review regulatory requirements to keep up to date on evolving requirements.
- Some breaches may require involvement from the Police. Meeting with your local Cyber Crime Unit ahead of an incident to establish relationships and best practise will support your efforts in the event of live data breach scenario. In the event of a data breach they can help to:
- Look for evidence that a crime has been committed.
- Sometimes be the one to inform the organisation they have had a data breach which has not be identified by the company.

What to look for in a breach response partner

While the right external partners may vary depending on your organisation, we've identified five important considerations when considering 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 who can handle the "What If" Scenarios? Partners should provide compelling insights, counsel and relevant tools before, during and after an incident to help your organisation better navigate the response and prevent future incidents.

3. Relationship with regulators (if possible), data breach partners and legal firms – should have established relationships with government stakeholders and regulators. Organisations with a collaborative relationship with attorneys in general are more likely to have their support.

4. Ability to scale select partners who can scale to your organisation's size and potential needs 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 who has a global knowledge base and service capabilities, including awareness of breach laws in different countries or the ability to implement multi-lingual call centres.

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.

Additional considerations

Selecting Insurers and insurance policies

Modern cyber insurance policies offer several other valuable resources to companies, including access to leading partners, forensic investigators, data breach resolution providers and communications firms to help navigate complex incidents. 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 needs.
- **Understand your security posture:** Being able to demonstrate a strong security program and types of security incidents most likely to impact your organisation 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 questions:** It's important for you and your broker to ask the right questions when selecting a provider. Make sure you understand the potential exemptions in policies, as well as their history of paying out claims for incidents.

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.

Selecting PR and Crisis Comms partners

- 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 organisation 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 your process: Create a detailed process for developing and approving internal and external communications, including a well-defined approval hierarchy.
- Consider your audience: Confirm your plan accounts for communicating with your employees, customers, regulators and business partners.
    - **Prepare templated communications:** Prepare draft materials with content placeholders including: Holding statements for a variety of incident types.
    - Public Frequently Asked Questions (FAQs) document to address customers, investors and media.
    - Letter to customers from company leadership.
    - **Internal employee communications:** Who would you engage and how to ensure they can support in a live scenario. What would you want them / not want them to do.
    - **Test your communication process:** Create a tabletop drill for executives to gauge the team's ability to manage communications challenges such as media leaks, customer complaints, questions from employees and enquiries from legal, regulators and authorities.

Managing International data 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.[17] This is not 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 organisation 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/ Data Protection Act 2018, 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.

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

- **Create 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 organisations 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.
- **Organise consumer notification and support:** One of the biggest challenges companies face when responding to an international data breach is activating multi-lingual consumer notifications and call centres. This multi-faceted approach includes ensuring impacted parties receive notifications in the correct language as well as access to a secure, multi-lingual call centre for their questions and can they handle the number of inbound email questions. Another consideration is whether your company will offer identity protection services to affected consumers. While not mandated, these services can help dispel the fears of those impacted by the breach and ultimately help improve a company's reputation post-breach.

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

Practising your Response Plan

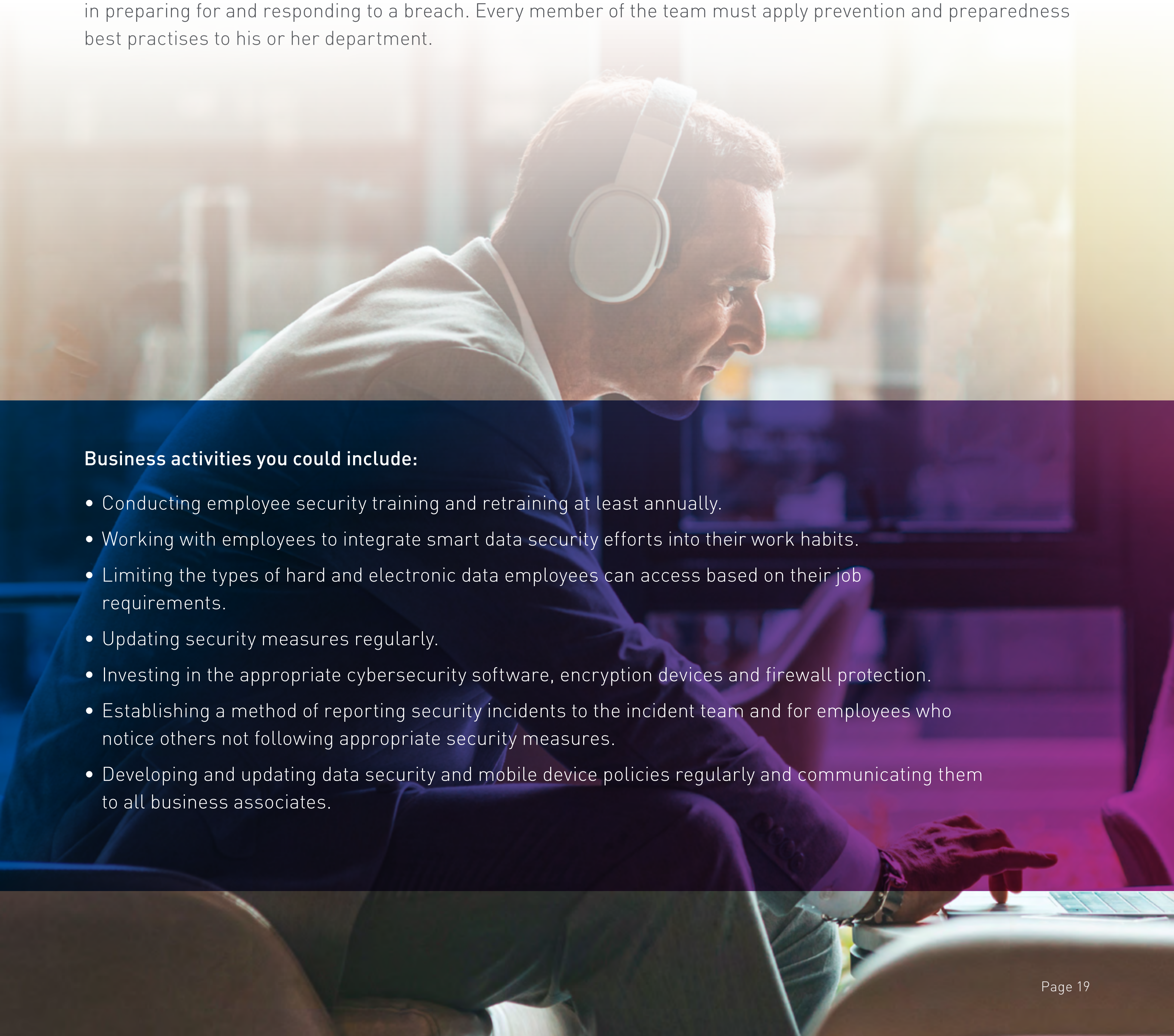
Of the 75% of organisations that practise their response plans, less than half (45%) practise them at least twice a year.[18]

Once you've established your breach response team and finalised 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 practising its elements.

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

Responsibilities of your team

Make sure everyone within 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 practises to his or her department.



Business activities you could 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 appropriate security measures.
- Developing and updating data security and mobile device policies regularly and communicating them to all business associates.

Implementing a crisis simulation drill

Data breach response plans must repeatedly be practised to not only be effective, but to give your organisation the chance to identify any 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 practised adequately.

Making sure your organisation is ready to carry out the response plan:

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

Enlist an outside facilitator: Have someone outside the organisation act as a moderator and facilitate 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.

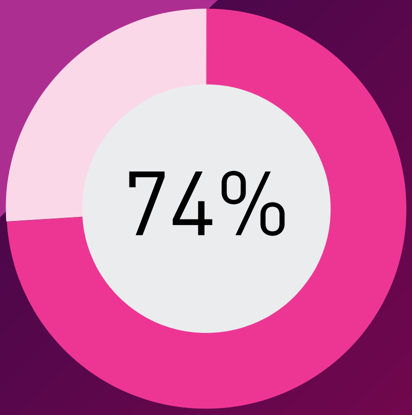
Debrief after the exercise: The team should review and discuss the lessons learned from the session and look at areas to improve to update the response plan.

Conducting drills every 6 months:

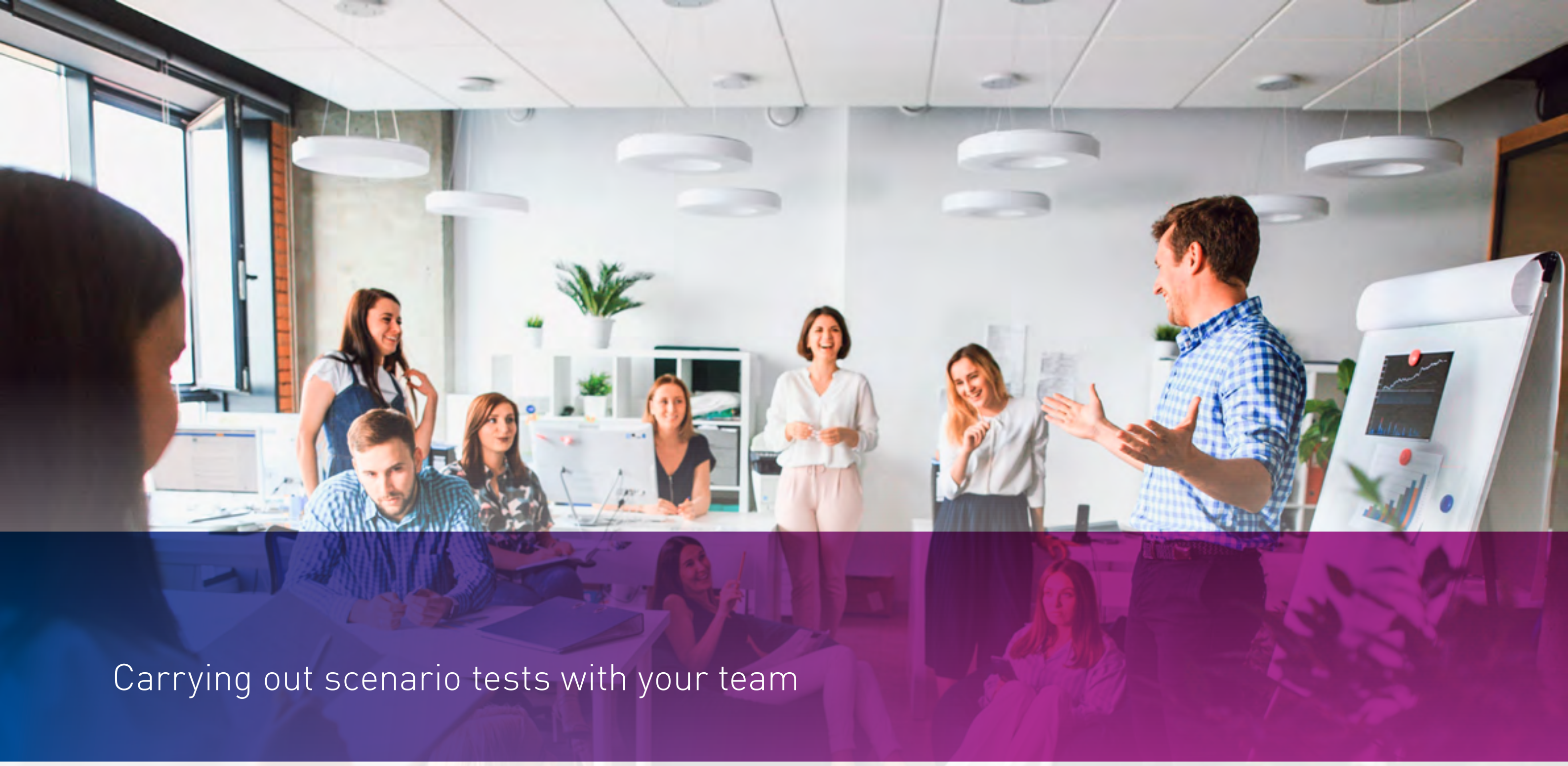
Make sure to stay ahead of the latest changes internally and externally with regular simulation exercises.

Who do you involve in the drill exercise?

- 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)



of organisations believe their data breach response plan could be more effective if they incorporated what they learned from previous breaches.[19]



Carrying out scenario tests with your team

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

Crisis scenario drills (examples)

1. The Police contact your organisation. They suspect that a user of the dark web is in possession of usernames and passwords of your customers and are selling them to the highest bidder. They recommend investigating the matter and suggest it is only a matter of time before the press find the posts.
2. A hackivist organisation send your company a note claiming to be in possession of PII (names, addresses, DOB, and National Insurance Numbers) of your customers. They threaten to release the data unless the company meets their specific demands.
3. A company vendor that handles customer data notifies you that they suspect a data breach may have compromised your data. They are not sharing any information, citing a forensics investigation, and advise that their legal counsel will be in touch.
4. Your organisation is targeted with ransomware that takes critical business systems offline. Make it real by injecting 'changes to the scenario' part way through the simulation training. As your response team respond to the simulation scenario start to inject more information about the incident so that they are forced to respond and act based upon new developments.

By including these 'injects' participants will be forced to make decisions, involve different functions and potentially take different actions as a result. When designing an effective response drill, it is essential that there are injects designed to engage all parts of the response team.

Possible 'inject' examples could include: A media enquiry from a reporter claiming to have information about the incident with tight deadlines where the company has to respond.

- A letter from the regulator threatening an investigation into the incident if they do not receive a detailed account.
- Forensics update where the IT teams get additional details of what systems and data has been compromised.
- Mocked up displeased email from customers or employees about the incident.

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

Checklist

How prepared and resourced is your team?

Here are some questions to help you evaluate your level of preparedness. If you answer **NO** to more than one or two, you and your team should look to address these as quickly as possible

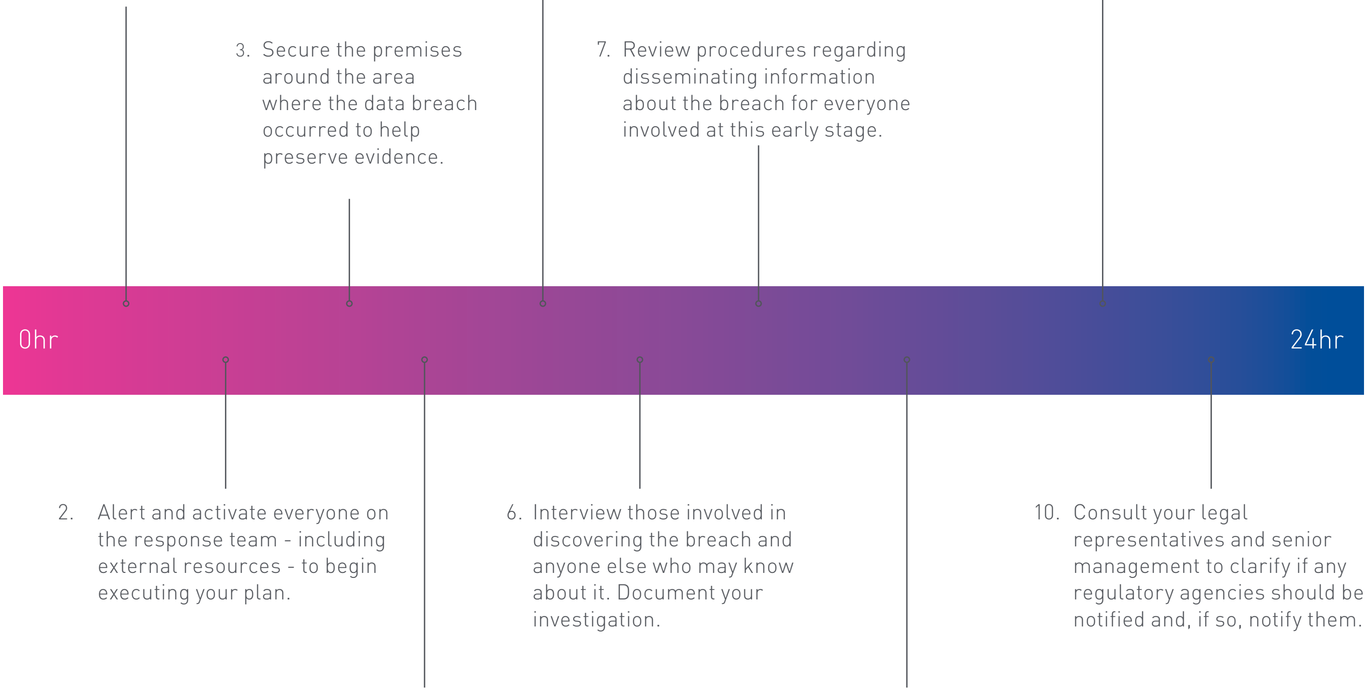
	Do you have an internal response team assembled?
	If you have a preparedness plan in place, have you updated, audited, and tested your plan in the last 12 months?
	Have you identified third-party vendors and signed contracts to engage in the case of a breach?
	Do you have a relationship with relevant legal experts in case of a breach?
	Have you identified what your breach notification process would look like and do you have up-to-date and accurate contact lists for employees, customers, etc. in place to activate quickly?
	Have you researched credit and web monitoring services that you could offer to help those affected?
	Have you taken inventory of the types of information you store that could be exposed during a data breach?
	Do you have the technology and processes in place to conduct a thorough forensic investigation into a cyber security incident?
	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's covering likely questions, letter from company leadership?)
	Have you media trained your spokespeople and executives specifically on security matters?
	Have you conducted a data breach crisis tabletop exercise or simulation to test how effectively your company would manage a major incident in the last 12 months?
	Have you conducted employee training to apply security best practises in the last 12 months?

Notes:

The first 24 hours

Acting quickly and strategically following a data breach can help you regain your security, preserve evidence and protect your brand. Always collect and keep a record of as much information as possible about the data breach and your response efforts, including all conversations with regulatory bodies and legal professionals.

As soon as you discover a data breach you will need to quickly respond by initiating your team and immediately contacting your legal counsel and senior stakeholders. Consider the following critical steps



1. Record the date and time the breach was discovered, as well as the current date and time when response efforts begin (i.e. when someone on the response team is alerted to the breach).
2. Alert and activate everyone on the response team - including external resources - to begin executing your plan.
3. Secure the premises around the area where the data breach occurred 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 IT forensics team arrives.
5. Document everything known thus far about the breach, including who discovered it, who reported it, to whom was it reported, who else knows about it, what type of breach occurred, what was stolen, how was it stolen, what systems are affected and what devices are missing.
6. Interview those involved in discovering the breach and anyone else who may know about it. Document your investigation.
7. Review procedures regarding disseminating information about the breach for everyone involved at this early stage.
8. Assess priorities and risks based on what you know about the breach.
9. Bring in your IT Forensics team to begin an in-depth investigation.
10. Consult your legal representatives and senior management to clarify if any regulatory agencies should be notified and, if so, notify them.

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.

Putting customers at the heart of your response

When communicating a complex or difficult message on mass across a diverse group of demographics and/or across multiple geographies there is potentially more to think about than one might first think.

Below are some of the key questions you could consider when starting to review how you will respond?

- How many people's personally identifiable information has been compromised?
- What type of data has been stolen? Is it personally identifiable information?
- Do you have up to date email addresses, telephone numbers and address information of your customers?
- Would you know how to craft a notification letter and what to include within your communications?
- Do you have a facility to be able to translate the notification communications in multiple languages if it were across country borders?
- Do you have the ability to upscale resources/expertise to be able to communicate a clear and concise message on scale and quickly?
- Do you have call centre telephone support, offering multilingual capability and can you upscale this facility so those who are affected can call in and talk to an expert and be reassured?

Not all data breaches require notification

If your data was encrypted or an unauthorised employee accidently accessed, but did not misuse the data, you may not need to notify individuals.

Protecting affected individuals

Increasingly consumers are looking to organisations to provide a remedy in the event of a data breach. Providing credit or web monitoring services will serve to support the individual and offers the potential to decrease the chances of becoming a victim of fraud.

Whilst no product will detect every possible instance of fraudulent activity, the more types of information (eg. name, date of birth, national insurance, credit card details, etc) and places of misuse monitored (eg. Dark web, public records, etc) by the service can greatly increase the level of protection provided to those individuals impacted.

After the first 24 hours

at a glance check list

1	**Responding to a Data Breach**	• Identify the cause report to senior management • Alert your external partner • Continue work with forensics • Identify legal obligations • Ensure your forensics team removes hacker tools and address any other security gaps.
2	**Document when and how you contained the breach**	• Generate reports including all the facts about the breach, as well as the actions and resources needed to manage it. • Create a high-level overview of priorities and progress, as well as problems and risks. • 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 centre. • Determine if any countermeasures, such as encryption, were enabled during the breach. • Analyse all data sources to ascertain the compromised information. • Revisit local laws that apply and then determine which entities to notify. • Ensure all notifications occur within any mandated timeframes.
3	**Identify conflicting priorities**	• Determine if any upcoming business initiatives • may interfere or clash with response efforts. • Decide whether to postpone these efforts and for how long.
4	**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 practises.

As you progress through the process it will be important to review and assess your progress against your plan to ensure you have effectively implemented the initial steps.

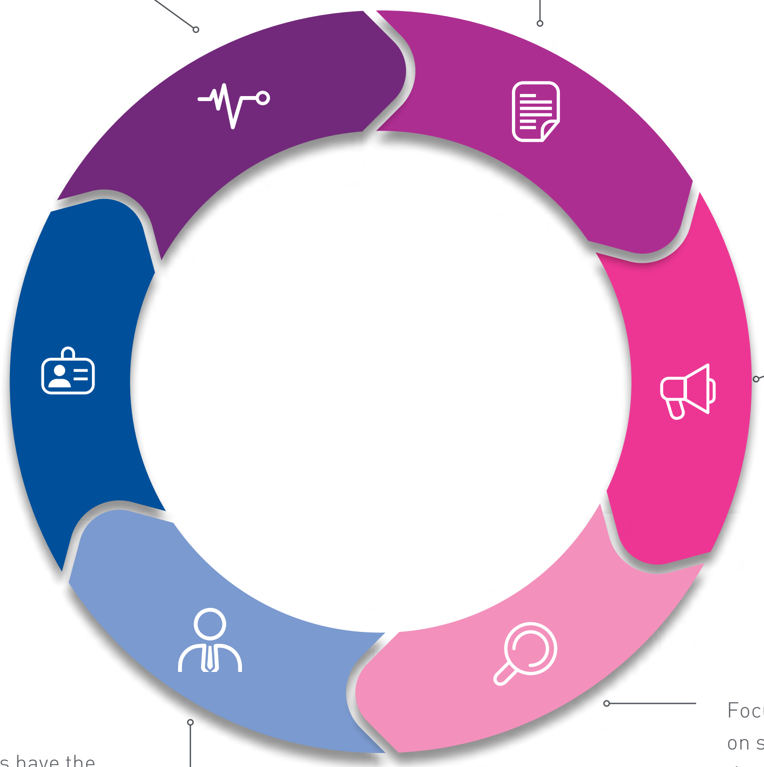
Legal Notice The information you obtain herein is not, nor intended to be, legal advice. We try to provide quality information but make no claims, promises or guarantees about the accuracy, completeness or adequacy of the information contained. As legal advice must be tailored to the specific circumstances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

Managing and protecting the company's reputation

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

While early planning is essential to manage a security incident successfully, organisations must always expect the unexpected. Data breaches can often cause an increase in 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 consider:



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

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

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

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.

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

Protecting legal privilege

The increasing likelihood of reach 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 with 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 organisation.
- 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.

Helpful links and resources

Information Commissioner's Office **www.ico.org.uk**

International Association of Privacy Professionals **https://iapp.org/about**

Experian **www.experian.co.uk/databreach**

Experian works with organisations every day to put pre and post breach response plans in place to respond, reassure and recover in the event of data breach.

Find out more details about how we can support you. Download our latest thought leadership materials here: **www.experian.co.uk/databreach**

Experian's Breach Response Team

Jim Steven
Head of Data Breach Response
Experian Consumer Services
M: (+44) 07972 298698
jim.steven@experian.com

Ryan Bradshaw
Senior Breach Response Manager
Experian Consumer Services
M: (+44) 07866 126733
ryan.bradshaw@experian.com

Sarah Williams
Senior Breach Response Manager
Experian Consumer Services
M: (+44) 07967 567014
sarah.williams@experian.com

Cardinal Place
6th Floor
80 Victoria Street
London
SW1E 5JL
United Kingdom

E breachresponse@experian.com
W www.experian.co.uk/databreach

About Experian Data Breach Services, UK

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 global experience, Experian has successfully serviced some of the largest and highest-profile breaches in history. The team offers swift and effective incident management, consumer notification, call-centre support, and reporting services while serving millions of affected consumers with proven credit and web (identity) services.

Registered office address:
The Sir John Peace Building, Experian Way,
NG2 Business Park, Nottingham, NG80 1ZZ

T: +44 7972 298698
E: BreachResponse@experian.com
www.experian.co.uk/databreach

Legal Notice: The information obtained 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.