

A helpful guide for businesses: Data Breach Response Readiness

A guide to preparing your customer first data breach response plan

Edition 2019



Foreword

Getting prepared in advance of a data breach is now an essential component of managing business risk.

With awareness of data breaches at an all-time high board members and senior leaders are increasingly involved in their organisations data breach readiness planning. Additionally many organisations are now investing time to establish employee privacy and cyber security programmes to raise awareness of the threats and manage increasing risk.

Whilst there is greater awareness and an increasing sense of urgency to prepare for a data breach by organisations, many are still not confident of their ability to secure data and manage the aftermath of a data breach. Those organisations with a response plan in place need to review their plans to ensure they are up to date and indeed ensure they are in a position to successfully respond to individuals affected and governing regulatory bodies.

Experian's Data Breach Response guide provides organisations with a step-by-step review of the key areas for consideration, providing useful insight and tools needed to prepare your organisation. Throughout this guide we also focus on how putting the individuals affected at the 'heart of the response' can support your recovery and manage reputational damage.

We hope you find this guide helpful and this supports your organisation to look to the future with increased confidence to respond, reassure and recover should a data breach incident occur.

Sincerely,

Jim Steven

Head of Data Breach Response
Experian Consumer Services



Contents

Introduction	2
The lifecycle of a data breach	3
Legal considerations	4
The data breach response plan	7
Creating your plan	9
Prepare	10
Key influencers	13
Purchase cyber insurance and regularly evaluate coverage	14
Selecting legal partners	15
Incorporating PR and communications	15
Practising your plan	17
Responding to a data breach	21
Protecting your brand reputation through effective communications	25
Putting customers at the heart of your response	26
Useful aids and auditing your plan	27
How prepared are you? – Check list	28
The first 24 hours - Check list	29
An Example Data Breach Response Team Contact List	30

Introduction

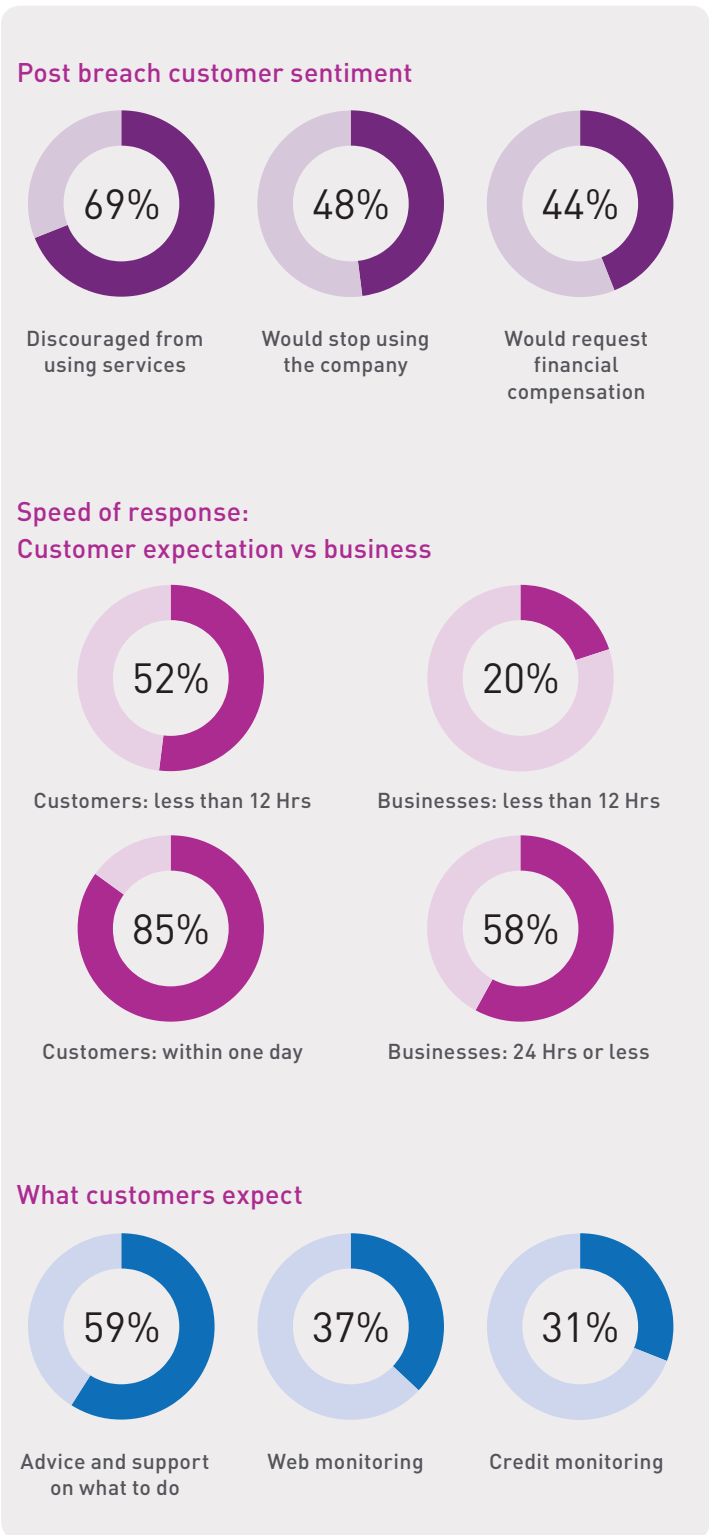
The purpose of this guide

Experian's Data Breach Response Guide is designed to support organisations prepare for a data breach. 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.

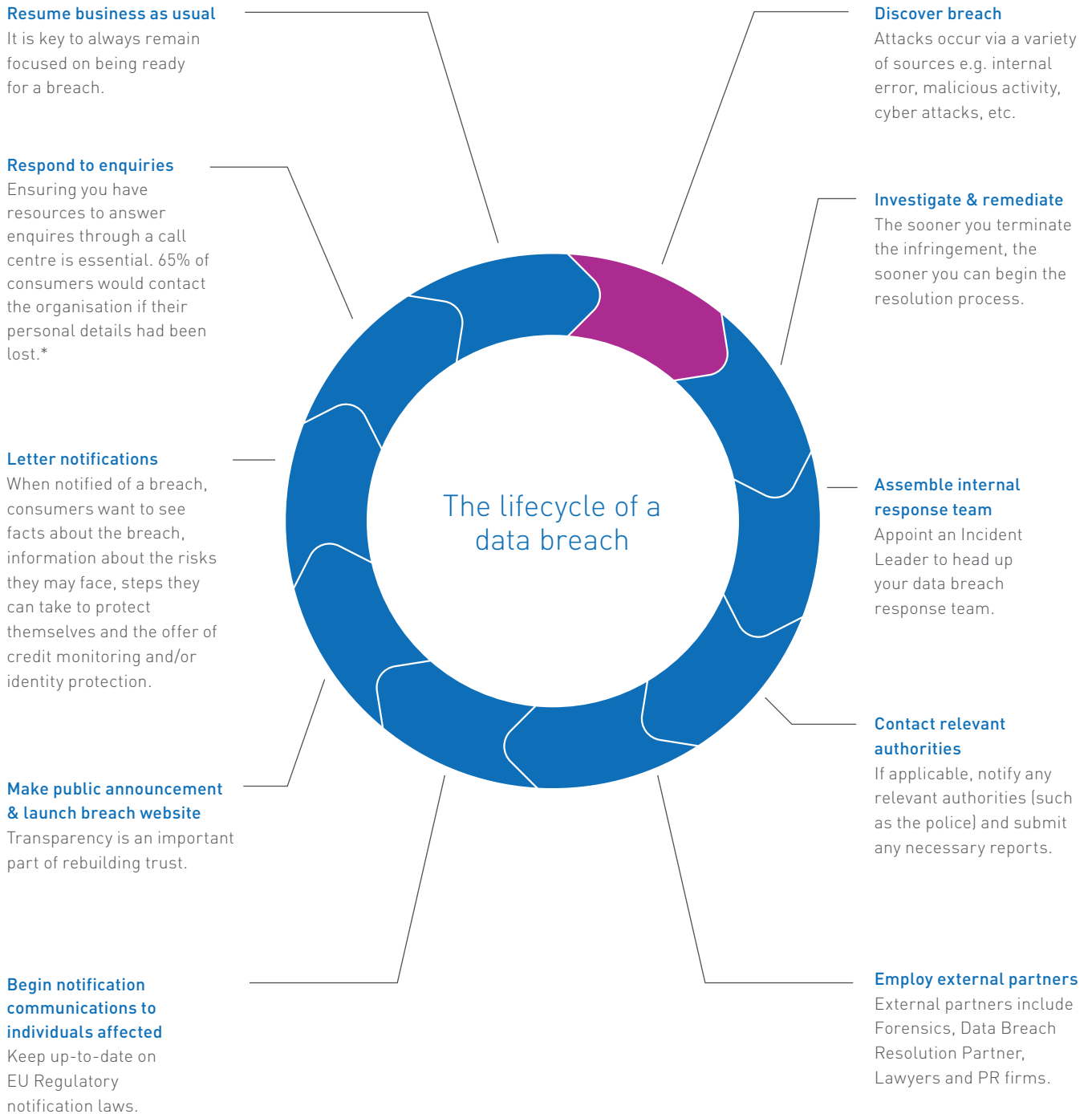
Time is of the essence

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.



* Experian commissioned ComRes to conduct an online survey of IT business decision-makers at small, medium, large businesses in GB and 2,001 British adults in January 2017. Experian Data Breach Response: readiness vs reality whitepaper.

The lifecycle of a data breach



* Experian commissioned ComRes to conduct an online survey of IT business decision-makers at small, medium, large businesses in GB and 2,001 british adults in January 2017. Experian Data Breach Reponse: readiness vs reality whitepaper.

Legal considerations

The Information Commissioners Office (ICO) guidance on data security breaches

Organisations now need to comply with the requirements of The General Data Protection Regulation (“GDPR”) which imposes an obligation on organisations, in certain circumstances, to notify the ICO in the event of a personal data breach. The section below sets out further information that the ICO has issued relating to this new obligation. This information is based on information provided by the ICO at the time of printing this guide. To find the latest updates on legislation visit www.ico.org.uk.

What is a personal data breach?

The term “personal data breach” is defined in GDPR and means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. As such, a personal data breach includes much more than just losing personal data and includes a wide range of issues affecting personal data.

In what instances may I need to notify the relevant supervisory authority?

Organisations will be required to notify the relevant supervisory authority of a personal data breach unless it is unlikely to result in a risk to the rights and freedoms of individuals. The repercussions of a data breach can result in significant detrimental impact on individuals – for example, discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Every personal data breach is different and therefore will need to be assessed on a case by case basis in order to decide whether or not the obligation to notify the regulator, applies. Having said that, in some circumstances it might be obvious when the obligation arises eg. the ICO informs that this might be the case where the loss of customer details exposes the customer to the risk of identity theft.

When do individuals have to be notified?

Where a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, organisations will also be required to notify those individuals affected.

What information must a breach notification contain?

Article 33(3) of GDPR sets out what information the notification to the regulator must include (as a minimum):

The nature of the personal data breach including, where possible:

- (a) the categories and approximate number of individuals concerned; and
- (b) the categories and approximate number of personal data records concerned;

The name and contact details of the data protection officer (if your organisation has one) or other contact point where more information can be obtained;

A description of the likely consequences of the personal data breach; and

A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, where appropriate, measures to mitigate its possible adverse effects.

How do I notify a breach?

A personal data breach which invokes the obligation to notify the regulator must be notified to the regulator without undue delay and, where feasible, within 72 hours of the organisation becoming aware of it. If the organisation does not notify the regulator within this timescale, it will be required to explain the reasons for the delay. The GDPR recognises that, in some circumstances, it will not be possible to investigate a data breach fully and notify all relevant information to the regulator within that time-period. In those circumstances, organisations may provide information in phases but without further undue delay.

If the breach is sufficiently serious to warrant notification to affected individuals, the organisation responsible must do so without undue delay.



Failing to notify a breach in accordance with the requirement of EU GDPR could result in a fine (the greater of) 4 per cent of your organisation's global annual turnover or 20 million Euros.

What should I do to prepare for breach reporting?

You should make sure that your employees understand what might constitute a personal data breach and, in particular, that this is more than loss of personal data. You should ensure that there is an internal breach reporting procedure in place to help ensure that breaches are detected, managed and escalated in a timely manner. This will help ensure that the breach is contained and investigated in a timely manner. It will also help those responsible for determining whether or not the personal data breach should be notified to the regulator or affected individuals, to make an informed decision as to whether or not notification is required and if so, to whom.

Having robust breach detection, investigation and internal reporting procedures in place is particularly important in light of the tight timescales and prescriptive information requirements set out in GDPR.

Technology considerations

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


The global cloud

The data breaches of tomorrow are likely to be global in nature, adding significant complexity to the data breach response process. With the rise of cloud computing, massive quantities of sensitive data now travels across

national borders in the blink of an eye. Yet, while these data flows are global, the data breach laws and cultural norms for responding to an incident are local. Clearly, responding responsibly, effectively and legally to a large data breach is currently a major compliance challenge. Notifying individuals and providing some form of identity protection across multiple countries and jurisdictions is increasingly complicated.

Encryption is critical

While encrypting internal and travelling data may be expensive and time-consuming, it is clearly a worthwhile undertaking for organisations – especially in light of increasing data breaches and potential regulatory scrutiny. Organisations should also keep up with IT security and install the latest software to protect their systems. But technology alone is not the answer. Numerous data breaches are actually caused by insiders. In these cases, an employee purposely steals sensitive consumer data or carelessly opens a link and infects his or her organisation's systems. As a result, it is always good practice to establish procedures for safeguarding customer and employee data, including limiting access to data to only those employees who genuinely need it to perform their jobs effectively.



C-level executives need to be driving force behind data breach readiness and make it a continuing priority and focus for the entire organisation.

The data breach response plan



Why create a response plan?

A data breach can take a heavy toll on any organisation, whatever its size. Having a plan in place can help you act quickly when required, which in turn can help you prevent further data loss, ensuring you can respond, reassure and recover in the event of a data breach.

With increased public awareness of data breaches, the likely heightened effect on an organisation's reputation and customer loyalty is a real consideration. In reality organisations who suffer an incident are presented with a halo effect of financial and reputational implications. Organisations that have not adequately prepared and are subject to a data breach will increasingly suffer costs associated with lost business, as well as the direct cost of fines and an impact on brand reputation.

Incident readiness

It is important to develop your response plan and build your response team well before you need them. Your team will play an important role in coordinating efforts between your organisations various departments, fulfilling two primary functions:

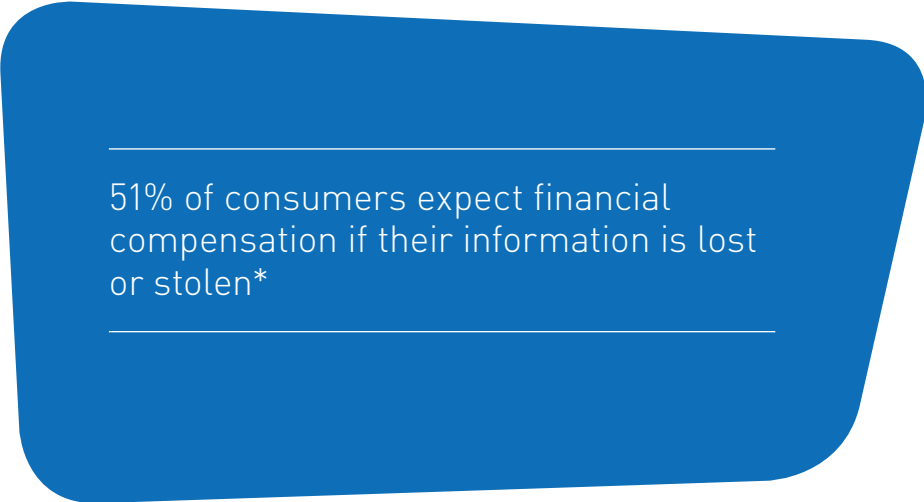
1. Development of a data breach response plan and prepare the entire organisation for the appropriate steps to take during a data breach.
2. Implement the response plan, engage the appropriate resources and track the efforts. Having the right information will ensure you can provide essential information about the data breach to relevant regulatory bodies, such as Information Commissioners Office (ICO).

A comprehensive approach

Because a typical data breach involves several actions, many of which need to be dealt with simultaneously, it is best to establish a response plan that takes into account every scenario and responsibility that could come into play. This includes assembling a strong internal response team, interfacing with relevant regulatory bodies (including ICO), and notifying affected individuals, communicating with the media and responding to enquiries.

Secure a proven breach response partner

The quickest – and often most effective – way to develop a data breach response plan is to retain the services of a data breach response partner. Many data breach response providers specialise in a specific aspect of resolving a data breach, but only a few offer the breadth of services and proven expertise needed to address every point along the resolution lifecycle.



51% of consumers expect financial compensation if their information is lost or stolen*

*Experian commissioned ComRes to survey 2001 british adults aged 18+ online November 2017. Data Breach: Supply Chain Risk whitepaper.

Creating your plan



Ready your team

Your internal data breach response team

Assembling your internal team

Assembling a complete team comprising of strong, capable representatives, will go a long way towards ensuring an efficiently executed response. Your data breach response team should include the following key roles:

Incident leader

Typically a Chief Privacy Officer or Legal Partner will be designated your Incident Leader driving forward the following considerations:

- Manage and co-ordinate your company's overall response efforts and team.
- Act as an intermediary between C-level executives and other team members to report progress and problems.
- Identify key tasks, manage timelines, and document every response effort from start to finish.
- Outline the budget and resources needed to respond to a breach.
- Ensure contact lists remain updated and team members are ready to respond.
- Analyse response efforts post-breach to better prepare for any future incidents.

Your Incident Leader, as well as every response team member, needs a back-up and should be reviewed regularly.

Executive leaders

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

This will help to:

- Ensure decisions are made by the team and have the support of executive management.
- Have a line of escalation and platform to update and communicate to senior board members and other key stakeholders, such as investors.

Information technology and security

IT and Security teams will play a crucial role in putting preventative measures in place, as well as:

- Identify the top security risks to the organisation that should be incorporated into written incident response plans.
- Train personnel in data breach response, including securing the premises, safely taking infected machines off-line, whilst preserving evidence.
- Work with IT forensics experts to identify the comprised data and delete hacker tools without compromising evidence and progress.

Legal & privacy

Engage with internal and/or external legal, privacy and compliance experts to help shape your data breach response plan and minimise the risk of litigation, fines, enforcement action and/or adverse media attention. Your legal representatives will (amongst other things) need to:

- Determine whether to notify affected individuals, the media, lawyers, regulatory bodies and other relevant third parties.
- Consider whether to establish relationships with any necessary external legal representatives before a breach occurs.
- Continually review and stay up to date with the latest regulatory updates on this subject.
- Outline a structure of internal reporting to ensure executives and everyone on the response team is up to date and on track during a personal data breach.

The Police & Regulatory Bodies

Depending on the severity of the breach and its potential consequences, organisations may decide to involve the police or other regulatory bodies.

Where the breach is of sufficient concern, organisations may also wish to notify (amongst others):

- the Financial Conduct Authority, if relevant; or
- the Cybercrime Unit of the Police.

Public relations

If you need to report the data breach to the media and/or notify affected individuals, your PR expert will play a key role to:

- Identify the best notification and crisis management tactics before a breach ever occurs.
- Craft consumer-facing materials related to an incident (website copy, media statements, etc).
- Track and analyse media coverage quickly, responding to any negative press during and after a personal data breach.

Customer Services

In the event of a personal data breach customer care leaders will play a key role in preparing front-line experts to answer enquiries directly from affected or concerned customers/employees. They will be responsible for:

- Developing and assisting in the development of Frequently Asked Questions.
- Holding simulation training for front-line experts answering calls.
- Preparing the dedicated data breach hot-line for affected individuals, as well as logging call volumes and frequently occurring questions and concerns from callers.

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

Assemble your external response team

Identifying key partners and securing pre breach readiness contracts beforehand is crucial. This will serve to secure credible experts and resources, but also help reduce the time to respond and better manage cost negotiations at this crucial time.

Waiting to identify key partners until an issue arises may result in compromising standards. Additionally this may hamper the ability to deliver each element of the plan and may result in increasing risks and costs.

Below are key partners you should consider:

Data breach response partner

Contract with a data breach response partner in advance of a breach to benefit from their strategic expertise and assist with:

- Assigning you a dedicated account manager to handle escalations, tracking and reporting.
- Handling all aspects of individual notifications, including drafting, printing, mailing letters and address verification.
- Offering proven identity protection, web monitoring and secure call centre services for all affected individuals.

IT forensics

Forensics partners play a key role in investigating, translating and articulating the technical findings and risk implications. They can provide reports to key decision makers, including:

- Advise the organisation on the potential or live data loss scenario and provide evidence and a plan to stop further data loss.
- Experts to preserve key evidence and manage the chain of custody, minimizing the change that evidence will be altered, destroyed, or rendered inadmissible in court.

Crisis management/communications

Specialist crisis management/communication experts should have experience of helping organisations manage highly publicised security issues and demonstrate the ability to understand the technical and legal nuances of managing a data breach.

They will:

- Help develop all public facing materials needed during an incident.
- Provide counsel on how to best position the incident to key audiences and help manage and mediate questions related to the incident.
- Onboarding this partner in advance of an incident will allow you to identify risks and weaknesses within the existing team and present an opportunity to pro-actively participate in test 'war room' scenarios in advance of a data breach.

Legal counsel

Legal partners should preferably have strong experience in data and privacy legislation and have strong links with local regulatory authorities. They should also have the expertise to be able to provide guidance on (amongst other things):

- What information (if any) should be disclosed to relevant parties in order to effectively manage any associated risks.



Key influencers

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 time line in the event of a data breach.

- Have a list of key contacts aligned to the appropriate regulatory notification requirements.
- Regularly review regulatory requirements to keep up to date on evolving requirements.

The Police

Some breaches will require involvement from the Police. Meeting with your local Cyber Crime Unit ahead of an incident to establish relationships and best practice 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 is a pre-breach readiness agreement?

A contract with a partner that is executed before a data breach occurs. This clearly establishes the relationship and allows key components of planning to be pre-determined and put in place in readiness for a data breach. This can include preparation in relation to notification letters, call centre support, data cleansing, web and credit monitoring and frequently asked questions.

What to look for in a partner

Organisations will have a clear set of unique parameters they have identified when selecting the right partners. Below are five key important traits for your consideration:

1. Understanding of security and privacy

Partners should have a background supporting different types of data breaches, along with a well-rounded knowledge and expertise of the entire data breach life cycle.

2. Strategic insights

Partners should be able to provide compelling insights, counsel, and relevant resources and tools before and during an incident to help the organisation better prepare. Test whether they can respond to the 'what if' scenarios.

3. Ability to scale

Select partners that can scale to the organisation size and potential needs during an incident. Whilst a data breach may initially seem small, relating to the amount of data and/or individuals affected, it can subsequently be discovered to be much larger or more complex. Organisations that are formed of multiple sub brands will need to further consider the complexities in relation to this.

4. Relationship with governing bodies

Where possible, it is important for partners, particularly legal firms to have established relationships with government stakeholders and key governing bodies. Organisations who have established collaborative relationships with relevant parties are more likely to have their support.

5. Global considerations

If your company has an international footprint, it is important to identify what knowledge base and service capabilities the partner has globally. This can include awareness of the breach laws in different countries or the ability to implement multilingual call centres.

Purchase cyber insurance and regularly evaluate coverage

With the average cost of a data breach continuing to rise it is vital organisations consider purchasing cyber security insurance to help manage this risk. Along with providing financial protection after an incident, modern cyber insurance policies offer several other valuable resources to companies. These resources include access to leading lawyers, IT forensics investigators, data breach response partners and crisis management and communication experts. Additionally many offer other valuable services ahead of an incident such as access to risk management tools and pre-breach consultation with response experts.

Selecting a policy

There are a several key considerations to keep in mind when selecting your policy.

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 partners to assist with the buying process. Working with an insurance broker who has specific expertise in cyber insurance will help your company select the right policy and insurer to meet your specific needs.

Understand your security posture

Being able to demonstrate a strong security program and the types of security incidents that are most likely to impact the organisations can help ensure you obtain the right level of coverage. Working with your insurance broker to demonstrate a strong security posture to insurers can also prove useful when negotiating the terms and cost of a policy.

Ask the right questions

Given cyber insurance is still relatively new, it is important that you and your broker ask the right questions when selecting a provider. In particular, ensuring you understand the potential exemptions in policies, as well as their history of paying out claims for incidents.

Organisations will benefit greatly from cyber insurance if they are informed about their security risks, educated on the variety of policies, and aware of the coverage they need.

Selecting legal partners

From a legal partner perspective, when considering who to work with in order to support you in managing the risks associated with personal data breaches, there are several nuances that can be taken into account, which might have an impact on who you choose.

Below are a few considerations that organisations may wish to take into account:

- Previous experience managing data breach litigation and have established relationships with local regulators.
- Ability to provide insights about the latest developments in case law.
- Experience that goes beyond simply helping with formal legal notification and ability to serve as an overall breach coach with a strong understanding of what is needed ranging from technical investigations, as well as the potential implications of legal decisions.
- Ability to connect you with other external experts ahead of (or during) any incident to assist in relation to other major areas of a data breach response (including forensic investigators and PR consultants, for example).

Incorporating PR and communications

It is also important to ensure that communications is incorporated into the broader incident response process and there is a clearly documented plan for how your organisation will make key communication decisions, the channels you will use to get out the message and what to say.

Here are examples of key considerations:

Enlist an expert

Ensure a communications representative is part of your core incident response team and is included in legal and IT forensics discussions.

Map out your process

Document a detailed process for developing and improving internal and external communications that includes a well-defined approval hierarchy.

Cover all audiences

Ensure your plan accounts for communicating to your employees, customers, regulators, and business partners.

Prepare templated materials

Prepare draft communication materials with content placeholders including holding statement from a variety of incident types; a public Q&A document to address questions from customers, investors, and media; a letter to customers from company leaderships; and an internal memo to employees.

Test your communication process

Create a table top simulation for the key executives to gauge your ability to manage communication challenges such as media leaks, customer complaints, questions from employees and enquiries from regulators.

Conduct preparedness training

In addition to a company-wide focus on data security and breach readiness, department-specific training should also take place.

Global data breaches

A global data breach presents a different set of challenges for organisations; it can involve many languages, notification laws, most importantly, a variety of diverse cultures and differing views of privacy.

As the economy becomes more globalised, the odds of experiencing an international data breach are now higher than ever before.

The following are ways to prepare if your organisation has an international footprint:

- Develop a roster of legal counsel in your respective countries who are familiar with existing local breach notification laws.
- Consider the need to engage a local PR expert should a breach occur.
- Assess if you need local call centre expertise that is familiar with local sentiment regarding privacy issues.
- Ensure you notification partner can handle multi-language notification letter production.

Practising your plan



Conduct readiness training with your teams regularly

Establishing your data breach response team is a key step in the right direction in effectively responding to a data breach, but many organisations still need to bridge the gap by practising the key components of the plan itself.

Each team lead has a responsibility to apply prevention and readiness best practices to his/her own department.

- Work with employees to integrate smart data security efforts into their daily work habits.
- Develop data security and mobile device policies, updating them regularly and communicating them to all organisation associates.
- Invest in the appropriate cyber security software, encryption devices and firewall protection. Update these security measures regularly.
- Limit the type of both hard and electronic data everyone can access, based on their job requirements.
- Establish a method of reporting for employees who notice that others are not following the appropriate security measures.
- Conduct employee security awareness/re-training regularly.

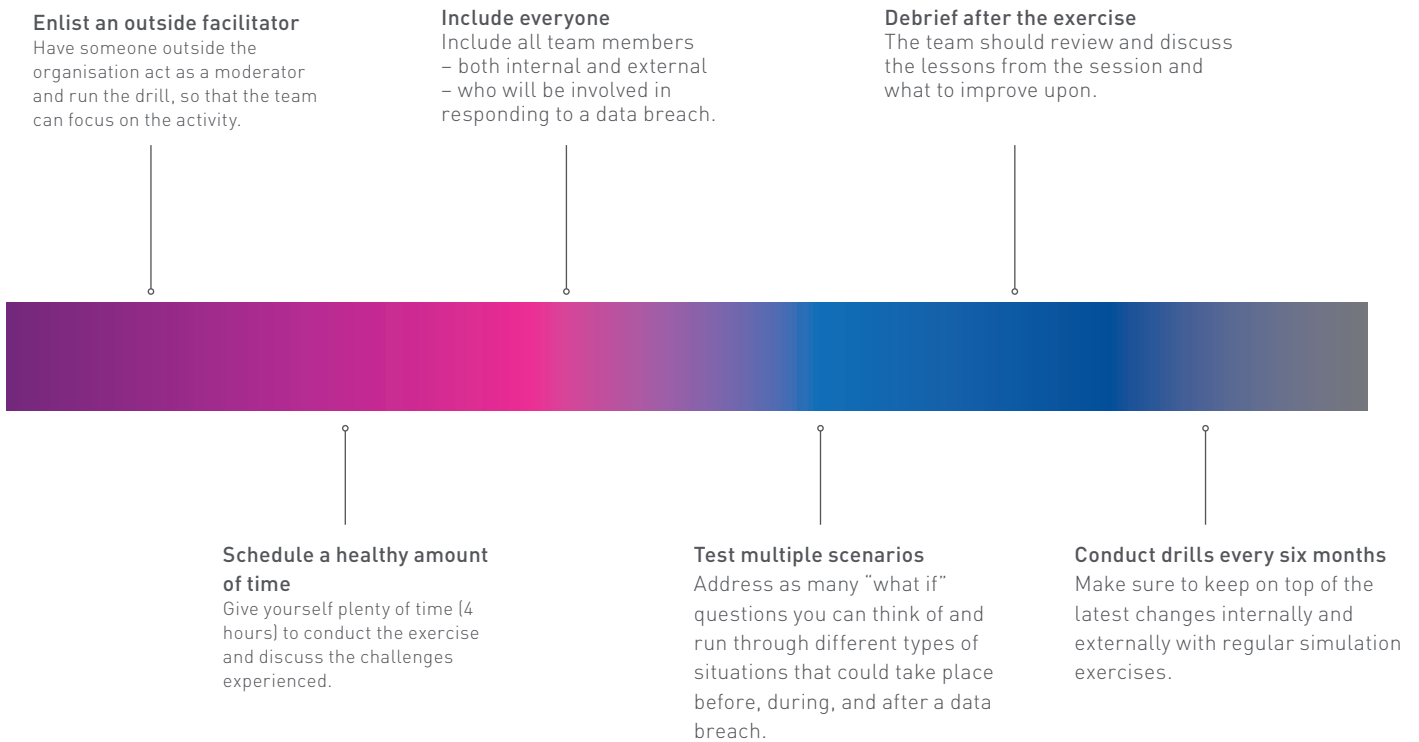
Carry out simulation training to test the plan and experts

A key way to review and test your plan and identify key strengths and weaknesses is to carry out simulation training. By bringing all of your data breach response team members together you can effectively replicate the challenges that you could face in the event of a data breach. This will help to expose gaps in your plan or skills that need to be addressed.

Make sure everyone on your data breach response team understands their specific responsibilities – both in preparing for, and responding to a data breach and this becomes a key component of your organisations daily culture.

57% of British Adults can name a business that's been affected by a data breach and 95% of consumers say they would take action if their personal data was lost or stolen*

*Experian commissioned ComRes, a member of the British Polling Council. Research of 302 IT business decision-makers within small, medium-small and medium-large enterprises in January 2016. Experian Whitepaper SMEs under threat.



Who should you involve in your simulation training to make it effective?

- CIO, CISO or other board members
- IT
- Legal
- Public Relations
- Human Resources
- Risk and Compliance
- Customer Services
- Outside partners: Legal counsel, public relations and crisis management, data breach response partner, cyber insurers.

A sample simulation training day

Addressing a few different scenarios that your organisation can relate to will help you to get the very most from your experience. Create an environment and simulation brief which is relevant to your industry, the type of data you collect and hold and is true to the way in which you are structured. Scenarios may not be truly realistic and will have to allow for the fact in the real data breach environment it may take several weeks, not hours to determine the true picture.

Sample simulation scenario 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 ransom ware 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.

Responding to a data breach

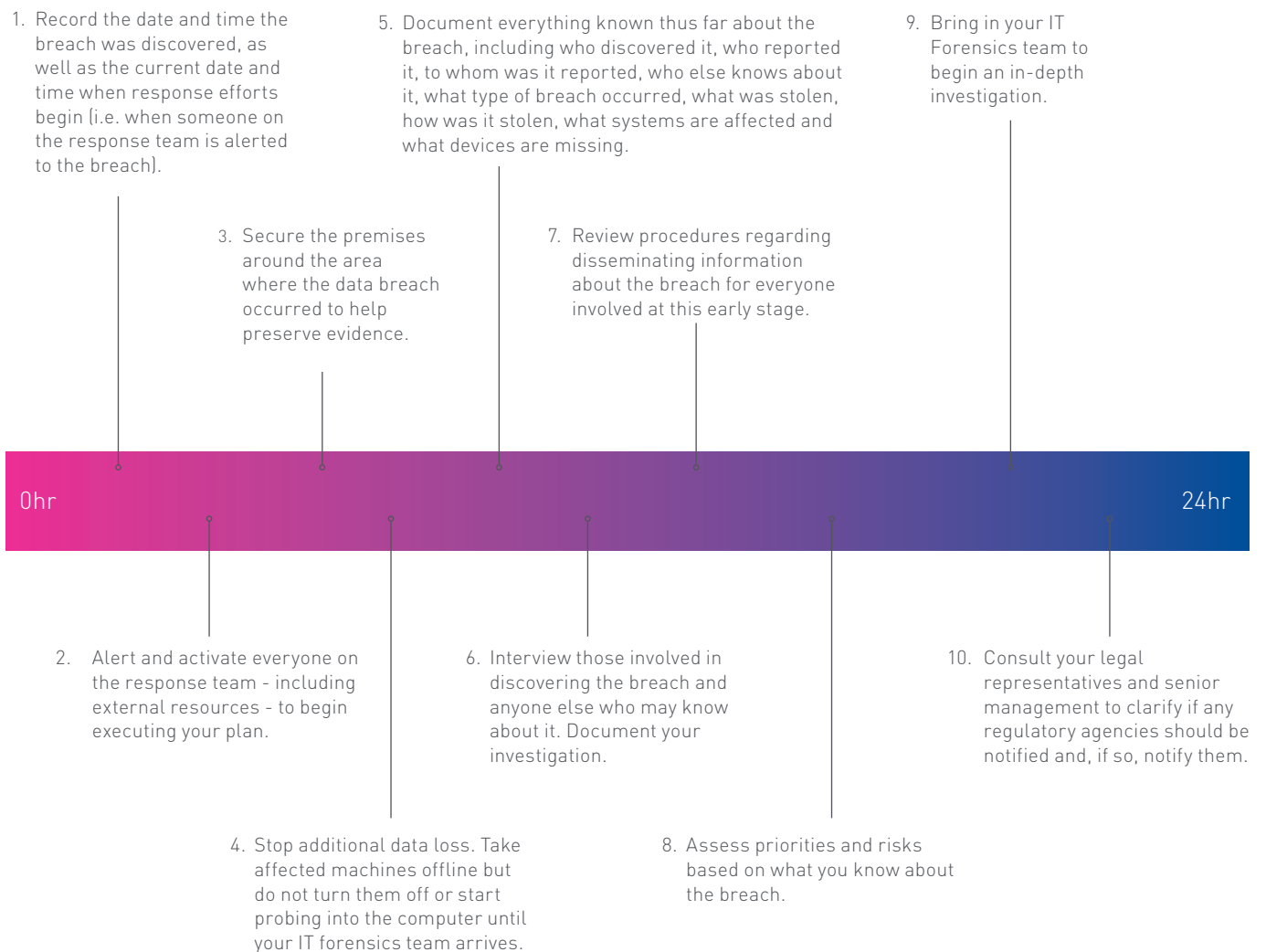


The first 24 hours after a data breach

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.

The first 24 hours of a data breach are crucial and can help you regain security, preserve evidence and crucially protect your brand reputation.

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:



Assess your progress and next steps to keep on track

After you have completed the first initial steps and identified that an incident has occurred you will need to continually review your progress and carry out key steps, including:

Step 1 – Identify the root cause

- Ensure IT forensics team removes hacker tools and address any other security gaps.
- Document when and how the breach occurred.

Step 2 – Alert your external partners

- Notify your partners and include them in the incident response moving forward.
- Engage your data breach response partner to handle notification, credit and web monitoring, call centre support, and data cleansing requirements.

Step 3 – Continue to work with IT Forensics

- Determine if any countermeasures, such as encryption, were enabled during the data breach.
- Analyse all data sources to ascertain what information was compromised.

Step 4 – Clearly assess your legal obligations

- Revisit regulatory requirements that apply and then determine all entities that need to be notified.
- Ensure all notifications occur within any mandated timeframes.

Step 5 – Report to your senior executive team

- Generate reports that include all facts about the data breach, as well as the steps and resources needed to resolve it.
- Create a high-level overview of priorities and progress as well as problems and risks.

Step 6 – Identify conflicting initiatives

- Determine if any up and coming business initiatives may interfere or clash with response efforts.
- Decide whether to postpone key activities and for how long.

Step 7 – Evaluate

Once an incident is resolved, evaluate how your organisation managed the response in order to make the necessary improvements to your readiness plans. Take time to reflect and make these adjustments to ensure that you capture key weaknesses and strengths. Use the incident as an opportunity to retrain employees not only in their specific response role when a breach occurs, but also in their own security and privacy practises. Organisations who suffer a data breach will undoubtedly put the education of employees at the forefront of their minds and start to create a culture that proactively safeguards against such an event.

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.

Protecting your brand reputation through effective communications

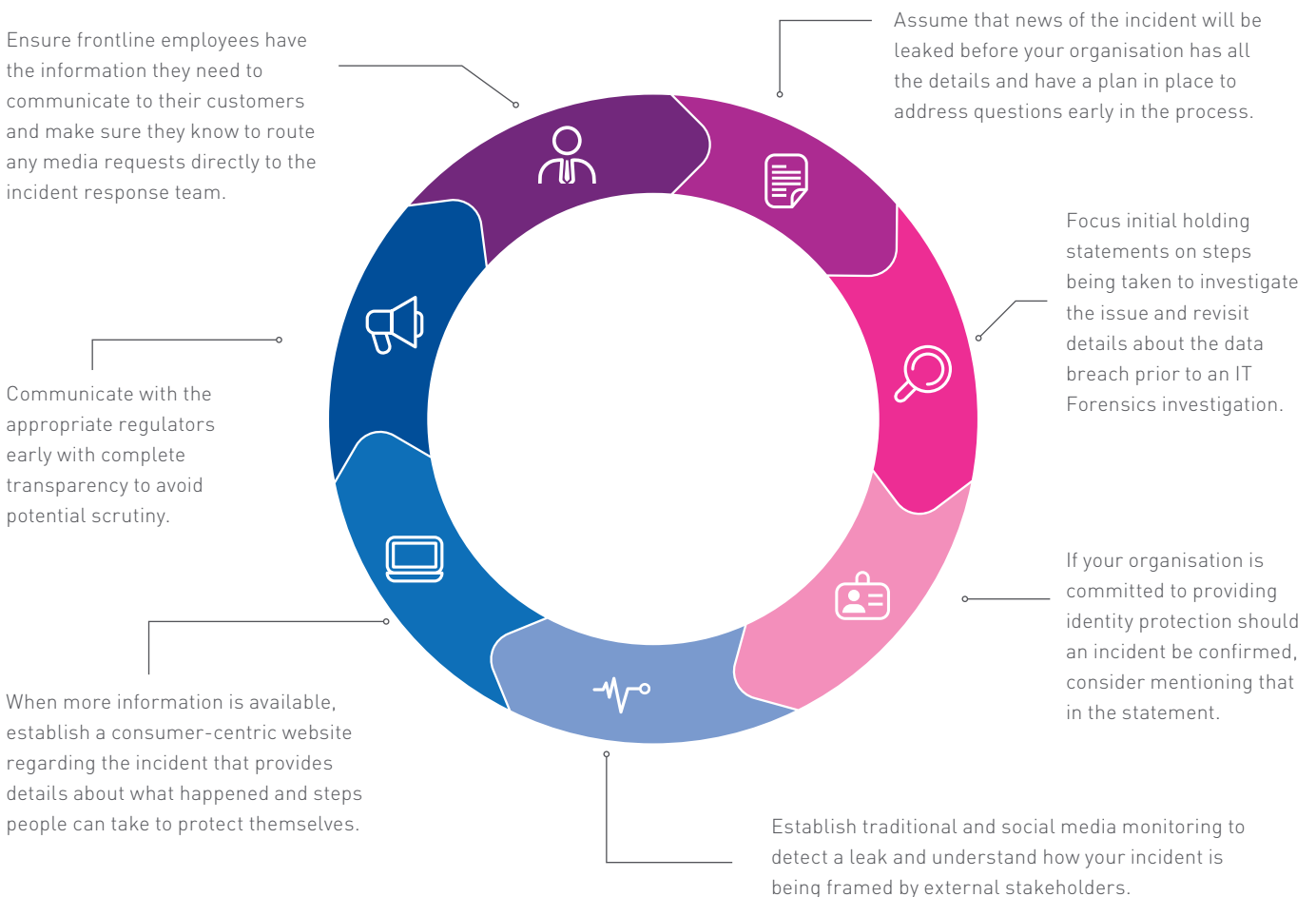
In the event of a data breach incident there will be two key priorities

1. Managing reputational damage and erosion of customer loyalty and
2. Reduce financial impact.

As outlined previously there are key practical steps that organisations can take in the event of a data breach. One of the more challenging areas to manage is the effective communication of the incident, which looks to proactively stop misinformation and rumours from occurring.

Not forgetting that every incident presents a different set of scenarios and challenges. Outlined below are six key principals that will help to support your communication planning:

Seven key principals for effective communication



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 accidentally 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.



Every organisation has an opportunity to put the 'what if' into play and test scenarios. Just imagine how positive it would feel to be able to confidently manage and provide reassurance to your employees and customers affected.

Useful aids and auditing your plan



On the following pages we have prepared a number of supporting auditing tools for your reference:

How prepared are you? – Check list

Here are some key questions to help you evaluate your level of preparedness. If you answer NO more than once or twice, you and your team should immediately address the gaps to get fully prepared.



Response Planning

- Do you have an internal response team assembled?
- If you have a preparedness plan in place, have you updated, audited, and tested your plan in the last 12 months?



Key Partners

- Have you identified third-party vendors and signed contracts to engage in the case of a breach?
- Do you have a relationship with relevant state attorneys general to contact in the case of a breach and ensure you are following state guidelines?



Notification and Protection

- Have you identified what your breach notification process would look like and have the up-to-date contact lists for employees, customers, etc. in place to activate quickly?
- Have you evaluated identity theft protection services to offer to affected parties if you experience a data breach?



Security Planning

- Have you taken inventory of the types of information you store that could be exposed during a data breach?
- Do you have the technology and processes in place to conduct a thorough forensic investigation into a cyber security incident?



Communications

- Have you developed a communications incident response plan including drafts of key media materials that will be useful during an incident (e.g. holding statements, Q&A covering likely questions, letter from company leadership)?
- Have you media trained your spokespeople and executives specifically on security matters?



Training and Awareness

- Have you conducted a data breach crisis table top exercise or simulation to test how effectively your company would manage a major incident in the last 12 months?
- Have you conducted employee training to apply security best practices in the last 12 months?

The first 24 hours - Check list

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 readiness 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.

An Example Data Breach Response Team Contact List

Position	Company	Name	Contact Number	Email	Internal/ External
Incident Lead					
• Incident Lead Primary/Secondary					
C-Level Executives					
• Chief Executive Officer					
• Chief Financial Officer					
• Chief Information Security Officer					
• Chief Privacy Officer					
• Chief Compliance Officer					
Response Team Members					
• IT Primary/Secondary					
• Security Primary/Secondary					
• Privacy Primary/Secondary					
• Legal Primary/Secondary					
• PR Primary/Secondary					
• Customer Care Primary/Secondary					
• HR Primary/Secondary					
Resolution Partners					
• External Legal Counsel					E
• Public Relations/Crisis Management Firm					E
• Forensics Firm					E
• Notification Vendor					E
• Contact Centre Support					E
Third Parties					
• Business Partners					E
• Vendors					E
• Regulators					E
• Media					E



Contact us: breachreponse@experian.com www.experian.co.uk/databreach

Helpful links and resources

Information Commissioner's Office

www.ico.org.uk

International Association of Privacy Professionals

<https://iapp.org/about>

Experian links:

Experian works with organisations every day to put pre and post breach 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**

For further information please contact:

Jim Steven

Head of Data Breach Response
Experian Consumer Services

+44 7972 298698

BreachResponse@experian.com

www.experian.co.uk/databreach



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

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



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

© Experian 2019.

Experian Ltd is authorised and regulated by the Financial Conduct Authority. Experian Ltd is registered in England and Wales under company registration number 653331.

The word "EXPERIAN" and the graphical device are trade marks of Experian and/or its associated companies and may be registered in the EU, USA and other countries. The graphical device is a registered Community design in the EU. All rights reserved.

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.