Experian™

Crawford®

An Experian Data Breach Response Guide

A 'Customer First' Approach For Response Effectiveness

Edition 2016

Foreword

In recent years, the data breach landscape in the UK has changed beyond all recognition. More than four in ten Britons (42%) have been affected in some way by a breach, and their levels of concern are growing.

Cybercrime has become increasingly complex and sophisticated, with unprecedented levels of personally-identifiable information being traded illegally online. More than 110 million pieces of information were traded in 2014 alone – a 300% increase since 2012. In one single day in February 2015, more personally-identifiable information was traded illegally online than in a three-month period in 2014[1]. These are worrying figures that look set to increase as the year progresses. Added to which, the UK is experiencing rapid growth in identity-related crimes, with identity fraud now accounting for 46% of all fraud attempts[2].

Alarmingly, these changes could well be just the beginning, with the issue of data breaches likely to become even more acute over the next two years. A perfect storm is brewing: tougher regulation, increasingly negative public sentiment and rising costs will leave organisations of all shapes and sizes in no doubt that being ready to respond quickly and effectively is no longer a matter of choice.

Data breaches will require not only an initial response, but also a recovery plan for both the organisation and individuals affected.

In this guide we not only analyse the need for businesses to have a data breach response plan, but also take you step-by-step through its preparation, implementation and ongoing improvement. Equipped with the information, insight and tools you need to protect your organisation from cybercrime, you can look to the future with confidence.

Sincerely,

Jim Steven

Head of Data Breach Response
Experian Consumer Services, Affinity

The cyber landscape continues to evolve as companies face up to the new reality of increasing threats and an environment of tightening data protection laws. All organisations that handle information, whether personal data for individuals or confidential data for clients, need to be aware of the risks and the security required to ensure their data is protected.

The aim for most firms is to have enough information security and protocols in place so they are not prey for hackers. But more and more, there is a realisation that to some extent, security breaches are inevitable. Having a plan to respond in the event of a breach is more than just good practice, it has become an essential requirement.

The first 48 hours following a cyber breach are critical and too many organisations still neglect their incident response planning. Cyber breaches may be the reality but becoming a headline is not. The goal must be that a breach event becomes just another alert that is dealt with efficiently and effectively.

There are very few companies that don't communicate electronically or have any kind of confidential information or aren't reliant on different software systems. As a result, the cyber threat is very real for all organisations and this guide aims to help you get to grips with the fact that there is no perfect security but you can always be prepared.

Douglas Mower

Innovation Director
Crawford & Company

1 Analysis carried every six months by an independent security consultant on behalf of Experian.

2 According to CIFAS, 2014.

3 Guidance on security management – Information Commissioner's Office (ICO).

Contents

Useful documents and templates:

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

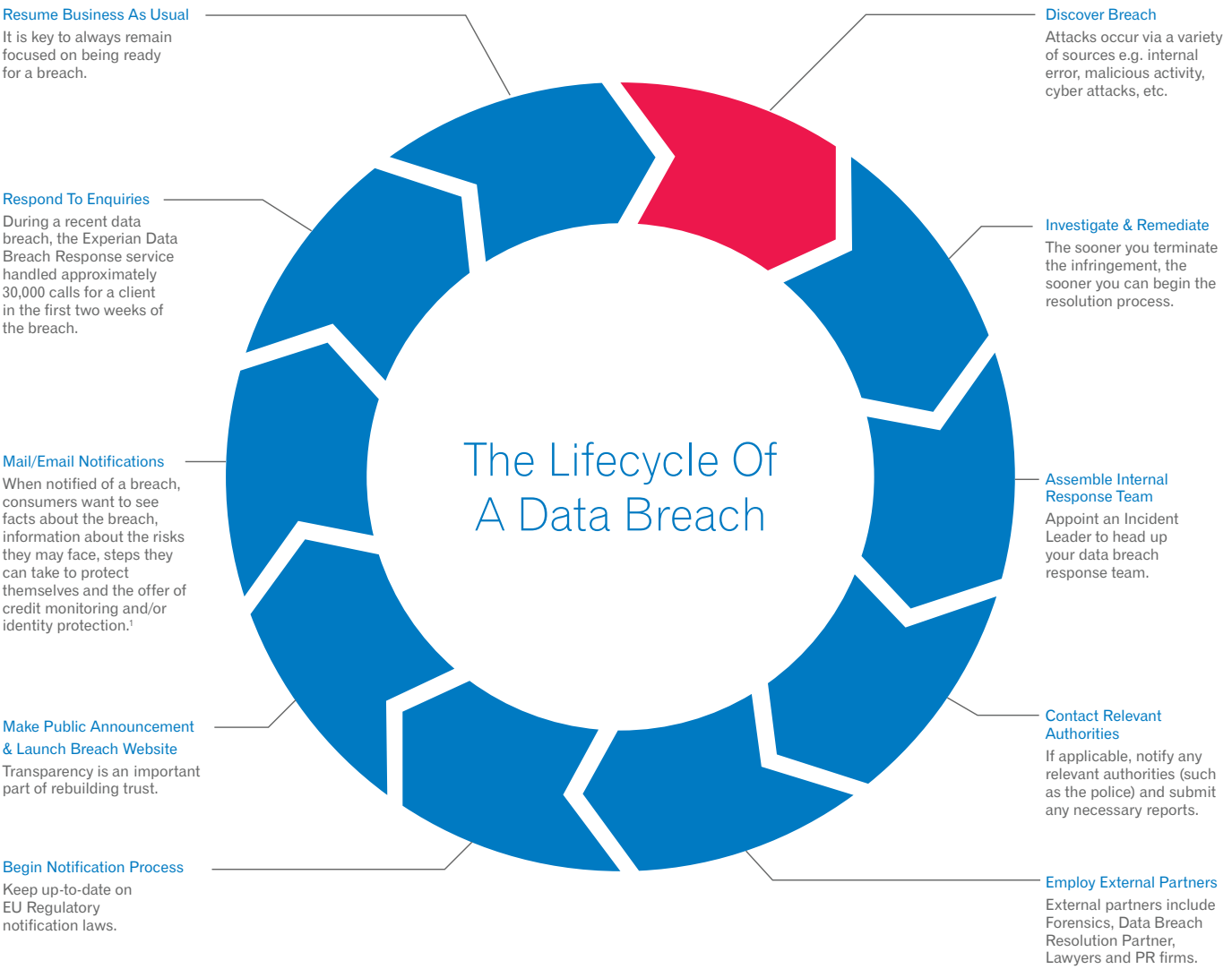
Understanding Data Breaches

The Purpose Of This Guide

Experian's Data Breach Response Guide is designed to help organisations prepare for a data breach, with information to 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 those 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. Either way, it could mean the difference between a breach that causes a brief disruption and one that causes a major incident.



1 On behalf of Experian, ComRes interviewed 400 medium and large UK businesses online between 22nd December 2014 and 3rd January 2015. All respondents were screened and had involvement or knowledge of their company's data breach policy. ComRes also interviewed 2,056 GB adults online between the 9th and 11th January 2015. Data was weighted to be representative of all GB adults aged 18+.

The Evolving Landscape

Legal Issues

The current regulatory framework in the United Kingdom does not require most businesses to provide notifications of a data breach.

Under the Privacy and Electronic Communications Regulations, providers of publicly available electronic communications services – such as internet service providers or telecommunications providers – must notify the Information Commissioner's Office (ICO) of any personal data breach. If a breach is likely to adversely affect the personal data or privacy of an individual or user, the service provider must also notify that individual or user without undue delay.

The ICO's Guidance On Data Security Breaches

The Information Commissioner's Office has issued the following guidance:

For organisations that are not providers of publicly available electronic communications services, their senior leaders must consider the risks to individuals and recommend whether they should notify those potential individuals who are at risk of being affected by a breach.

These organisations must also consider the effect of a breach on individuals – so they should assess their ability to comply with the current Data Protection Act and their ability to help individuals mitigate the effects of a breach (what they can do, for example, if individuals' passwords have been stolen). If a breach places individuals at risk of harm, organisations should be able to notify users of breaches, determine the best course of action and address their requirement to notify affected individuals.

The latest version of the proposed European General Data Protection Regulation, as drafted on 15th June 2015, will place an obligation on organisations to notify data subjects and their supervisory authority where a breach is likely to result in high risk to the rights and freedoms of individuals.

Organisations should ensure that they maintain a log of personal data breaches, including the facts surrounding the breach, its effects, and remedial action taken.

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 travel across national borders in the blink of an eye. Large data centres host data from individuals all over the world. 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 breach is currently a major compliance challenge.

Notifying individuals and providing some form of identity protection across multiple countries and jurisdictions is increasingly complicated. The situation is further compounded by the fact that 83% of UK consumers think companies should be subject to increased data breach regulation. So tougher regulation – whether driven by the EU or the UK – seems inevitable. And compulsory notification would have the added effect of raising public awareness of breaches.

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 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 company's systems. As a result, it is always good practice to establish procedures for safeguarding consumer data, including limiting access to that data to only those employees who genuinely need it to perform their jobs effectively.

Look to C-level executives to make data breach preparedness a continuing priority for the entire company.

The Data Breach Response Plan

Why Create A Response Plan?

A data breach can take a heavy toll on any company, whatever its size. Having a data breach response plan in place can help you act quickly when required, which in turn can help you prevent further data loss, avoid significant fines, and prevent costly customer backlash.

With increased public awareness of data breaches, the likely heightened effect on an organisation's reputation and its customer loyalty – as well as the multiplying effect of 'adverse advocacy' – adds a new dimension to the financial impact of a data breach. The outcome is 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 data breach response activities.

Incident Preparedness

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 company's various departments, fulfilling two primary functions:

1. Develop the data breach response plan and prepare the entire organisation for the appropriate steps to take during a data breach.
2. If a breach occurs, implement the response plan, engage the appropriate resources and track the efforts.

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 the Information Commissioner's Office), 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 resolution partner. Many data breach resolution 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.

Prepare

Creating Your Plan

A comprehensive data breach response plan includes a variety of specific elements and covers a wide range of disciplines. Even so, a well-constructed data breach response plan – no matter how comprehensive and detailed – is only as good as the team that is responsible for putting it into action.

Assemble Your Response 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 roles:

Incident Leader

The Incident Leader will help you to understand your legal obligations along with 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.

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.

Information Technology & Security

Your IT and security teams are likely to lead the way in putting preventative measures in place, but not necessarily in investigating it. You should have someone from IT and/or security on your response team to:

- Train personnel in data breach response, including securing the premises, safely taking infected machines offline and preserving evidence.
- Work with a forensics agency to identify the compromised data and delete hacker tools without compromising evidence and progress.

Legal & Privacy

Rely on internal and/or external legal, privacy and compliance experts to shape your data breach response plan and help minimise the risk of litigation and fines. Your legal representatives will need to:

- Determine whether to notify affected individuals, the media, lawyers, regulatory bodies and other relevant third parties.
- Establish relationships with any necessary external legal representatives before a breach occurs.
- Continually review and stay up to date with the latest regulatory updates.

Outline a structure of internal reporting to ensure executives and everyone on the response team is up to date and on track during a 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. The decision to do so should be based largely on the seventh data protection principles in the Data Protection Act, which requires businesses to take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Where the breach is of sufficient concern, organisations may wish to notify:

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

Public Relations

Depending on the size of the data breach and your industry, you may need to report the breach to the media and/or notify affected individuals. Your representative from your PR or communications department will need to:

- Identify the best notification and crisis management tactics before a breach ever occurs.
- Handle any information pertaining to a data breach and manage both internal and external enquiries.
- Track and analyse media coverage quickly, responding to any negative press during and after a breach.

Customer Care & Human Resources

Data breaches may affect both your customers and your employees, therefore you should appoint representatives from both customer service and HR to your response team to provide the necessary support. Your internal representatives should:

- Create simulation training for your customer service representatives that demonstrates how their roles would change during a data breach.
- Outline a plan for setting up a data breach hotline for customers and/or employees if a breach occurs. Determine in advance if you will use internal or external resources.

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

Data Breach Resolution Partner

Contract with a data breach resolution 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 notifications, including drafting, printing, mailing letters and address verification.
- Offering proven identity protection, web monitoring and secure call centre services for all affected individuals.

Practise and test your preparedness plan, and perform regular reviews to ensure you have everything covered.

Conduct Preparedness Training

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

Each member of the team has a responsibility to apply prevention and preparedness 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 training/re-training at least once a year.

Make sure everyone on your data breach response team understands their specific responsibilities – both in preparing for, and responding to a breach.

Implement

Responding To 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 agencies and legal professionals.

Of those organisations affected by a data breach in the last two years, 91% now have their board of directors, chairman and CEO informed and involved in the plans to respond to a possible future breach.[1]

Keep Your Response Efforts On Track

Resolving a data breach requires a coordinated effort between your response team members, executives, external resources, lawyers, forensic agencies and data breach resolution partner. Staying organised – including documenting every step and decision – should be a top priority. Act quickly to minimise the damage, but do not lose sight of your priorities or the needs of the individuals affected.

Never send sensitive information – such as National Insurance numbers – to partners supporting the breach response unless absolutely necessary.

The First 24 Hours

As soon as you discover a data breach, respond quickly but do not panic. Immediately contact your legal representatives for guidance on initiating these 10 critical steps:

- **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).
- **Alert and activate everyone on the response team** – including external resources – to begin executing your preparedness plan.
- **Secure the premises** around the area where the data breach occurred to help preserve evidence.
- **Stop additional data loss.** Take affected machines offline but do not turn them off or start probing into the computer until your forensics team arrives.
- **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.
- **Interview those involved** in discovering the breach and anyone else who may know about it. Document your investigation.
- **Review procedures regarding disseminating information** about the breach for everyone involved at this early stage.
- **Assess priorities and risks** based on what you know about the breach.
- **Bring in your forensics team** to begin an in-depth investigation.
- **Consult your legal representatives and senior management** to clarify if any regulatory agencies should be notified and, if so, notify them.

1 Experian Data Breach Readiness Whitepaper 2.0 2015.

Legal Notice: Always check with your legal representatives in order to identify the notification requirements for your specific incident.

Any data breach could lead to legal action. Work closely with your legal and compliance experts to analyse risks and ways to mitigate them.

Next Steps

Once you have completed the 10 initial steps, take time to review your progress to ensure your preparedness plan is on track. Then, continue with these next steps:

Fix The Issue That Caused The Breach

- Rely on your forensics team to delete hacker tools.
- Determine if you have other security gaps or risks and address them.
- Put clean machines online in place of affected ones.
- Ensure the same type of breach cannot happen again.
- Document when and how the breach was contained.

Continue Working With Forensics

- Determine if any countermeasures – such as encryption – were enabled when the compromise occurred.
- Analyse back-up, preserved or reconstructed data sources.
- Ascertain the number of people who might be affected and the type of information that was compromised.
- Begin to align compromised data with customer names and addresses for notification.

Identify Legal Obligations

- Determine all the different groups who need to be notified, including: customers, employees, the media and regulatory bodies.
- Ensure all notifications occur within any mandated timeframes.

Report To Senior Management

- Compile daily breach reports for senior management.
- The first report should include all the facts about the 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.

Identify Conflicting Initiatives

- Make your response team and executives aware of any upcoming business initiatives that may interfere or clash with response efforts.
- Decide whether to postpone these efforts and for how long, enabling you to focus your efforts on the breach.

Alert Your Data Breach Resolution Partner

- Contact your pre-selected partner so that you can determine the relevant business services needed for your company, and the protection products needed for individuals affected in the breach.
- Determine how many activation codes you will need for identity and web monitoring products, based on the number of affected individuals.
- If you do not have a pre-breach agreement in place, draft and sign a data breach resolution agreement.
- Engage your partner to handle notifications (learn more in the next section: Notifying Affected Individuals) and set up a call centre so affected individuals have access to customer service representatives trained on the breach.
- Work closely with your partner's account manager to review incident reporting and metrics.

Legal Notice: The information you obtan herein is not, nor is it 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 professionals.

Notifying Affected Individuals

Under the proposed European General Data Protection Regulation, as drafted on 15th June 2015, data controllers will be required to notify any affected data subjects without undue delay of any data breach which results in a high risk for the rights and freedoms of individuals, such as:

- discrimination;
- identity theft or fraud;
- financial loss;
- damage to reputation;
- unauthorised reversal of the anonymisation of data; or
- loss of confidentiality of data protected by professional secrecy.

This notification is not required where:

- appropriate technological and organisational measures were applied to the data which is the subject of the breach, particularly those which render such data unintelligible;
- the controller has taken subsequent measures to mitigate the risks of the breach;
- disproportionate effort would be involved; or
- a substantial public interest would be adversely affected.

Mishandling notifications can lead to severe consequences, including fines and other budgeted expenses. It can also impact an organisation's reputation and customer loyalty, leading to potential revenue loss.

The likelihood of improving the outcome in the event of a data breach is significantly higher if you have already organised the external resources you are likely to need. Having these resources in place in advance means that you can work quickly and efficiently with your forensics team, legal representatives and data breach resolution partner to meet your obligations and minimise the impact of the breach.

Legal Notice: Always check with your legal representatives in order to identify the notification requirements for your specific incident.

What you say, how you say it and when you say it are all important elements of data breach notification.

It is the organisation's responsibility to determine the deadlines for notification, in line with the latest EU Data Protection Regulations. Pre-determining your data breach strategy and how you will handle the notifications before a breach occurs enables you to take action quickly without delay or stress. In many cases, you can save money by signing a pre-breach contract with a data breach resolution partner.

What Your Data Breach Resolution Partner Should Do

Above all, your data breach resolution partner should make security a top priority throughout the notification process. Unlike standard direct mail production, data breach notification requires critical service and quality assurance elements to ensure compliance. Look for a single partner who can seamlessly handle notifications from beginning to end, making a positive impact on your brand.

Account Management

Your partner should assign an experienced account manager to your breach to help streamline and simplify the notification process. They should know the details of your breach, your priorities and your deadlines.

Notification letters may contain sensitive data and require secure handling through every stage of drafting, printing and mailing.

Critical Notification Services

A full-service data breach resolution partner should offer a range of options – as well as strict security standards – to match your organisation's needs and the scope of your breach. These include the following:

Comprehensive Letter Management

- Templates you can customise to your organisation and breach scenario
- Management of multiple letter versions for different groups of affected individuals e.g. customers and/or employees
- Four-colour or black-and-white letter options
- Professional printing with your company logo and electronic signature

Address Validation & Delivery

- Return mail management to securely handle and discard any returned notification letters
- Certified address cleansing to ensure address details are up to date and correct
- Coding accuracy support system – address standardisation
- Delivery point validation – validate address exists
- Traceable postage for future reporting

Quality Assurance For Printing & Fulfilment

- Dedicated quality assurance personnel
- Robust integration controls to ensure 100% produced and mailed
- Tier-1 data security protocols along with a secure/restricted access production area
- Ongoing training and certification of personnel

Reporting For Compliance

- Daily inventory reporting
- Initial mailings
- Address changes
- Undeliverable and returned letters
- Electronic letter copies for proof of notification
- Traceable postal delivery services reporting

Where an organisation decides to notify individuals of a data breach, the ICO recommends that:

- those affected are notified in the most appropriate way, bearing in mind the security of the medium and the urgency of the situation;
- the notification includes, at least, a description of how and when the breach occurred, what data was involved, the risks posed, and what the organisation has done so far in response;
- clear and specific advice is provided to data subjects; and
- further contact details are provided to ensure individuals have a point of reference to call with concerns.

Not all breaches require a notification. If your data was encrypted or an unauthorised employee accidentally accessed but did not misuse the data, you may not need to notify. Be sure to seek and follow legal advice before deciding to forego notification.

10 Steps: Working With A Data Breach Resolution Partner

1. Partner assigns a dedicated account manager and conducts initial meeting.
2. Client selects products and services and signs a data breach resolution agreement.
3. Partner provides samples of notification letters and options for identity and web monitoring products.
4. Client provides final data files and letter materials using secure data transfer capabilities.
5. Partner aligns affected individuals with addresses and generates applicable product activation codes.
6. Partner prepares call centre using incident-specific FAQs.
7. Client and partner jointly approve final letter.
8. Partner oversees mailing, delivery and re-mailing from secure fulfilment centre.
9. Partner provides regular reporting and metrics to client to track engagement.
10. Client identifies affected individuals, determines notification requirements and contacts partner.

An Example Notification Letter

Each notification should be tailored to the breach and aligned to the company's data breach response plan.

Company contact details

Company Address

Company Telephone

Greeting/salutation

Dear or Hello Mr/Mrs/Ms/Miss/Dr/Professor/Sir/Madam/first name

Introductory paragraph

We want to let you know about a security incident that we have had recently. On **<date>**, we found that **<what happened>**. **<length of time activity took place over>**. **<level of breach severity/information compromised>**.

Initial action we've taken

<explanation of what has been done immediately>

Specifics of breach

<what data was compromised and action that customer can initially take>

Apology and steps taken to remedy situation

We are really sorry that this has happened and want to do everything we can to fix the problem and prevent this from happening in the future. We take the security of your data very seriously and will be taking action to improve our systems and procedures. To start with, we want to offer you a **<length of subscription to Experian product>**.

About the product

<DataPatrol>

DataPatrol is an early warning service that will alert you if your information is found online or in the public domain so you can protect yourself from the risk of online crime. It monitors the web, social networks and public databases on your behalf 24/7, looking for your details to immediately detect any theft, loss or disclosure of your vital personal and financial information. If your information is found, you'll be instantly alerted by email or text message and given help and advice on what to do next to protect yourself from fraud

You can also control how much information DataPatrol monitors, adding basic details or registering more such as your passport number, driving licence and other important data. The more information you add, the better protected you are.

OR

<PMID>

ProtectMyID offers an end to end solution to help with the impact of data loss, including online credit identity fraud monitoring, alerting and assistance for victims of fraud. Once your membership is activated, your data and information will be protected with the following features:

- Unlimited access to your Experian Credit Report.
- Alerts to certain changes on your Experian Credit Report, such as the addition of a new account or credit search.
- Identity Theft Resolution service if you do become a victim of fraud through a dedicated case-worker who will walk you through the process of fraud resolution from start to finish.

- If you are at a higher risk of fraud, Experian can add protective Cifas registration to your credit report to help prevent credit being taken in your name.

Product 2 – PMID and web monitoring

This service helps detect possible misuse of your personal information and provides you with support focused on the immediate identification and resolution of identity theft.

Once your ProtectMyID membership is activated, your data and information will be protected with the following features:

- 24/7 monitoring of your data – monitors the web, social network and public databases.
- Unlimited access to your Experian credit report.
- Alerts of key changes and suspicious activity found on your Experian Credit Report.
- Identity Theft Resolution service if you do become a victim of fraud through a dedicated case worker who will walk you through the process of fraud resolution from start to finish.
- If you are at a higher risk of fraud, Experian can add protective CIFAS registration to your credit report to help prevent credit being taken in your name.

How to activate your subscription

Activating your ProtectMyID membership is simple and only takes a few minutes:

1. Visit the ProtectMyID Web Site to sign-up: http://partner.protectmyid.co.uk/protection/
2. Click on the red button Join ProtectMyID (on the top right hand side)
3. Enter your details and use the following activation code: **XXXXXXXX**
4. Ensure that you sign up by: **XX Month 201X** (Your code is valid until this date)

Acknowledgement and restatement of commitment

We will be constantly monitoring this situation, keeping you up to date with any developments and letting you know about all of the steps and measures that we are taking to fix it.

What to do if the customer has questions

We are always here to help, if you still have unanswered questions regarding the incident, or have difficulties signing-up online, please call Experian on **T XXXX XXX XXXX** - this is free from all landlines. If you are calling from a mobile or from overseas, the number is **T XXXX XXX XXXX**. Calls to this number from a landline or mobile will be charged at your standard call rate.

Sign off

Please do take advantage of this cover with Experian.
<further details on how the cover is being administered/paid for>.

Once again, we are really sorry that this has happened and we will continue to monitor the help we are providing to ensure that you are properly supported.

Yours sincerely,

<full name>

<position/title and company>

Managing Communications

Successfully Managing The Communications Impact Of A Data Breach

With data breaches frequently being given prominence in the news, executive boards are increasingly recognising this as a serious risk to their business. The threat of cybercrime also shows no sign of abating despite the heightened attention of policymakers and regulators.

Some valuable learnings have emerged about how best to respond to the onslaught of media and customer attention that an organisation faces during a major incident.

It is essential that your company's communications department is involved in all aspects of data breach planning to ensure proper alignment of this key function. Often companies will have a technical incident response team and plan, but it is not as closely integrated with the communications function within the organisation as it should be.

Data breach response teams should take the following steps to effectively integrate communications:

1. Develop a communications incident response process and plan that clearly outlines who will be responsible for developing and approving the key messages that will be communicated to media, as well as to internal audiences.
2. Ensure that the communications plan includes drafts of key media materials that will be useful during an incident. Documents you need to draft could include:
    - Holding statements for media for a variety of breach scenarios
    - Q&As covering likely questions from media, financial stakeholders and customers
    - Letter from senior management to be shared with customers
    - Key messages document
    - Customer web portal to post information when available
3. Conduct a data breach crisis communications simulation to test how effectively your breach is likely to be managed.
4. Provide media training for key spokespeople on how they are likely to respond to questions from the media related to a data breach.
5. Identify and vet an outside public relations firm with specific expertise in data breaches to be your partner during an incident.

Lesson No. 1: Be Lean Yet Integrated

Determine who is on the team – and who the team leader is with the authority to make decisions about press statements and media strategy – and keep it as small as possible. In most cases, the essential individuals are represented by the heads of IT, security, legal, marketing, PR, communications, the business lead and, perhaps, the CEO.

Lesson No. 2: Be Prepared For A Fluid Situation

In major breaches, it can take a month or two of round-the-clock work to answer: How did the attackers get in and when? What did they view? What did they steal? Are they still in there? If you must communicate something, say what you know, acknowledge what you do not know and continue to keep people updated.

To do this, companies must be diligent in resisting communicating numbers early in an investigation, while also being careful about claiming too soon that the issue has been fully resolved. A company is likely to receive scrutiny in the media for taking its time to provide more details, however this is easier to manage than communicating misinformation.

Lesson No. 3: Manage The Message

Communicating the right messages at the right time in the lifecycle of a breach will have a significant impact on how it is reported. While developing messages should not be one-size-fits-all, the following are key principles that could be followed:

1. Focus initial messages on the steps being taken to investigate the issue and frame it as a criminal issue.
2. Think through what you publicly communicate and the appropriate channels. Social media can quickly get out of control and open up the floor for public debate in front of followers.
3. Set up the appropriate media/social monitoring and listening posts to see how the breach is being covered.
4. Customers must be your priority, so make sure that you communicate with them clearly and effectively through traditional and digital channels.
5. Do not, however, neglect the wide variety of stakeholders interested in breaches – including policymakers, regulators and industry stakeholders such as payment brands.

While taking these steps will not fix all of the problems, it will significantly lessen the pain once the issue surfaces while allowing you to focus on the problem at hand.

Managing Global Breaches

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

For today's global organisations, preparing for an international incident – which can be far more complex than a local breach – is essential. A global breach can involve multiple languages, varying notification laws and, most importantly, a variety of diverse cultures and differing views of privacy, as evidenced by the European Union pushing for stricter standards.

Engaging Resources Abroad

When working overseas, it is crucial for companies to secure lawyers who are familiar with existing local data breach notification laws. An organisation will benefit from expert legal advice not only on the political climate surrounding privacy issues, but also on any current and proposed legislation in the affected region. Some countries have specific laws, while others provide only suggested guidelines related to breaches. Similarly, a company may also need to engage a local public relations consultant and nearby call centres who are familiar with local sentiment regarding privacy issues.

A local public relations or crisis management partner can properly advise an organisation on how much information to release and when to release it to the public. Local call centres can hire people who speak the native language and can relate better to residents. Securing these resources ahead of time enables companies to avoid the pressure of finding them when a crisis hits.

Engage with the right resources ahead of time, both locally and abroad.

Always seek advice from legal and compliance when drawing up partner contracts, especially ones involving data management or transfer.

Expect The Unexpected

Preparing for an international breach is challenging. Organisations should assess the risk and focus on protecting their most valuable assets – their customers and employees.

Legal partners play a crucial role throughout any data breach response, especially when dealing across borders.

It is therefore important to secure the right resources ahead of time, which can help you navigate the complexities of a far-reaching breach.

Continuous Improvement

Auditing Your Plan

Once you have created your data breach response plan, you will have helped your organisation to effectively respond should a data breach occur. But your plan can only help you succeed if it is comprehensive and current. Each quarter, make it a priority to update, audit and test your plan. Consider the different scenarios that could occur and whether your plan would help address each one – including an internal or external breach, accidental data sharing and loss or theft of a physical device.

Most Overlooked Details

Here is a quick overview of a few commonly-overlooked details that should be on your radar during a data breach response plan audit.

Call Centre

Getting your call centre up to speed on a data breach, or bringing external resources on board to help handle the high volume of calls, is an important part of your preparedness. The period immediately following a data breach is the time to be supporting affected individuals. You need to be readily available to answer their questions in order to reinforce the value of your brand and your commitment to their continued security.

Whether you plan to use internal or external resources, be sure you:

- Are prepared to swiftly pull together training materials, such as incident FAQs. Highly knowledgeable and empathetic call centre representatives can make a positive impact on your brand during a crisis.
- Are able to scale the call centre element of your data breach response plan to fit any incident. In addition to identifying the required call centre resources in advance of a breach, create a call centre script template specifically geared towards crisis management.
- Conduct ongoing crisis training for your regular call centre – whether it is internal or external – ensuring representatives are trained in handling sensitive information as well as emotional callers.
- Oversee several test calls to confirm the call centre is ready to handle incident-related calls.

Audit your data breach response plan immediately after a data breach so you can clearly remember what went wrong and what went right.

Supplier Negotiations

Many companies can overlook their suppliers when reviewing their security measures, but this can be a very costly mistake.

It makes sense for organisations to put plans and contractual obligations in place. Here are some of the areas for consideration:

- Maintain a written security programme that covers the company's data.
- Only use the company's customer data for the sole purpose of providing the contracted services.
- Promptly notify the company of any potential security incidents involving company data and co-operate with the company in addressing the incident.
- Comply with all applicable data security laws.
- Return or appropriately destroy company data at the end of the contract.

Operational Challenges

Even when you have determined all the steps and precautions you need to take if a data breach occurs, it is important to realise that responding to one can require significant company resources. Does your data breach response plan address the operational challenges of managing a breach in conjunction with managing day-to-day business?

For example, if your head of security and/or IT is tied up with breach response, who oversees the department in the meantime? Answering questions like these highlights that data security, data breach preparedness and data breach response require company-wide awareness and involvement.

Auditing Your Plan

Update Data Breach Response Team Contact List — Quarterly

- Check that contact information for internal and external members of your data breach response team are current.
- Remove anyone who is no longer with your company or an external partner, and add any new department heads.
- Re-distribute the updated list to the appropriate parties.

Verify That Your Data Breach Response Plan Is Comprehensive — Quarterly

- Update your plan as needed, to take into account any major organisational changes, such as recently established lines of business, departments or data management policies.
- Verify that each response team member and department understands their role during a data breach. Create example scenarios for your response team and departments to address.

Double Check Your Supplier Contracts — Quarterly

- Ensure you have valid contracts on file with your forensics team, data breach resolution partner and other relevant suppliers.
- Verify your suppliers and contracts still match the scope of your organisation.

Review Notification Guidelines — Quarterly

- Ensure the notification element of your response plan takes into account the latest regulatory guidance.
- Update your notification letter templates, as needed, to reflect any new laws.
- Verify your contacts are up to date for the lawyers, government agencies or media you will need to notify following a breach.

Check Up On Third Parties That Have Access To Your Data — Quarterly

- Review how third parties are managing your data and if they are meeting your data protection standards.
- Ensure they are up to date on any new legislation that may affect you during a data breach.
- Verify they understand the importance of notifying you immediately about a breach, and working with you to resolve it.

Evaluate IT Security — Quarterly

- Ensure proper data access controls are in place.
- Verify that company-wide automation of operating system and software updates are installing properly.
- Ensure automated monitoring and reporting on systems for security gaps are all up to date.
- Verify that back-up tapes are stored securely.

Review Staff Security Awareness — Yearly

- Ensure all your employees are up to date on appropriate data protection procedures, including what data, documents and emails to keep, and what to securely discard.
- Review how to spot and report the signs of a data breach from within everyday working environments.
- Verify employees are actively keeping mobile devices and laptops secure – onsite and offsite – and changing their passwords regularly.

Selecting The Right Resolution Partner

Looking for a resolution partner who provides a turnkey approach that includes incident management, data breach notification and reporting, as well as identity protection and call centre support for your customers will be a key consideration.

With a comprehensive data breach response plan, organisations can protect their business interests and the personal identities of affected individuals at the same time. This would address both your need for quick data breach resolution and your customers' demand for extended data breach protection to help you maintain your brand integrity and customer loyalty.

The Right Resources

Choose a partner who has the right resources and experience to keep your data breach response plan on track. Outlined here are some of the key resources your partner should provide:

- **A Dedicated Account Manager**

  You need an assigned, experienced account manager both to help guide you through every aspect of your data breach resolution, and to provide you with an implementation checklist so that you know what to expect during each phase of the resolution process.

- **Incident Response Education**

  The way you communicate internally and externally about a data breach can impact your brand integrity and resolution efforts. Your partner should train your key staff members on addressing the breach and preparing for situations that may arise.

Data Breach Notification

Your partner should help you act quickly to notify affected individuals within the outlined regulatory guidance in line with your unique incident.

- **Effective Notification Letters**

  Request a data breach notification letter template for you to customise and use. This can be a four-colour letter or black-and-white.

- **Address Verification**

  Obtain current and appended addresses, as well as research addresses for incomplete records. This is an important step to help ensure you reach the right individuals in a timely manner.

Identity Protection Products

A data breach puts your customers at higher risk of identity theft. By offering them a product which can help monitor their personal/financial information online can provide not only peace of mind, but also an early warning if their data is being misused.

When selecting the right product to offer those affected by the data breach, your partner should be able to advise on a number of features and their capabilities. These should include (but are not limited to):

- Consumer Credit Report
- Credit Monitoring
- Fraud Resolution Services
- Web Monitoring

Without the benefit of a credit and/or identity monitoring product, those affected are likely to only realise their identity has been stolen when they have already become a victim of fraud and learn that a new credit service or account has been opened in their name.

Secure a data breach resolution partner who employs a truly comprehensive approach.

Call Centre Support

Call centre services should serve the individuals affected by a data breach with the following:

- **Easy Enrolment**

  A partner can assign a unique, freephone number that your customers can use to enrol in their protection product. They can also develop a script related to your specific incident to remind your customers and employees that you are providing this protection product as a special precaution for them.

- **Daily Customer Service**

  Customer service should be available seven days a week to ensure your customers and employees have the identity protection support they need. This also helps to escalate a case to a fraud resolution specialist when necessary.

- **Customised FAQs**

  A partner should provide its call centre with a list of FAQs regarding to the data breach, so their team can answer questions your customers or employees might have regarding the incident. This eliminates the need for you to use internal resources for communicating with individuals affected by the breach.

Incident Reporting

Make sure your partner can provide the tracking and reporting you need to monitor your data breach resolution, report back to your key stakeholders and comply with appropriate regulatory governance.

- **Escalation Reporting**

  You will need timely updates on the status of any escalated concerns that your organisation submits.

- **Notification Metrics**

  Stay informed about the results of your data breach notification process, including the number of notices sent, received and returned.

- **Enrolment Metrics**

  Request reports on enrolment numbers as individuals sign up for the identity protection and web monitoring product you have provided. Be sure the partner can track both online and offline enrolments.

- **Call Centre Metrics**

  You should track daily call volumes, type of calls, speed of answer, and other metrics so you can monitor the efficiency of the call centre and your customers' and employees' use of the protection product.

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

Helpful Resources

Helpful Links

International Association of Privacy Professionals
www.iapp.org/about

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

Experian Links

Read our whitepaper on data breach response:

www.experian.co.uk/databreach.html

www.experian.co.uk/consumer-services/databreach.html

Crawford Links

Read our whitepaper on data breach response:

http://www.crawfordgts.com/services/cyber-risk.aspx

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

0844 4810 062
BreachResponse@experian.com
experian.co.uk/databreach

Trinity Court
42 Trinity Square
London
EC3N 4TH
United Kingdom

020 7265 4000
information@crawco.co.uk
crawfordgts.com/services/cyber-risk.aspx

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

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

© Experian 2016.

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 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.