Deloitte.

**Customer Breach Support**

Data breach: A different type of crisis

**Crisis**

A time of intense difficulty or danger.

A difficult or dangerous time in which a solution is needed – and quickly. A time of great disagreement, confusion, or suffering.

An unprecedented or extraordinary event or situation that threatens an organisation and requires a strategic, adaptive and timely response.

# Introduction

## The definition of a crisis may vary depending on where you look, and much has been written on the differences between a crisis, an incident and an emergency.

We generally find that people understand a crisis to be created by an event – something happens at a point in time that we then need to react to and recover from. A natural disaster (earthquake), financial meltdown (Black Monday), technical incident (IT system failure) or a safety incident (major accident). They don't happen often, but they do happen, and the impact on individuals and businesses can be huge. Most organisations, especially mature ones, have crisis and response plans in place because they understand that high impact events, whilst rare, can be catastrophic.

In recent years, with the rise of digital crime and online activism, heightened privacy concerns, and data regulation with strict enforcement, things are now changing in the world of data. Recent data breaches and ransomware attacks show that the historic approach that has been taken to crisis planning and response is no longer effective when it comes to a data breach. A data breach can be a significant type of crisis, and has some unique complexities that raise additional challenges. All businesses need to understand why a data breach is different, and what that means for their crisis plans and response capabilities.

# What makes a data breach different?

From our experience, there are several factors to consider. Although not all of the following characteristics are unique to a data breach, it's the combination of these factors that makes a data breach different.

### It's a regulatory event

A data breach is one of the few types of crisis that may involve investigation from a regulator, with a likelihood, especially given the recent trend in enforcement, of a fine and or mandated remedial action.

### It can become very public

When your customer data is lost or stolen, and the story is leaked to the media, the impacted individuals may publicly discuss this on social media giving more fuel to the issue.

### It's personal, but on a mass scale

By its very nature, a breach of customer data is a personal event for each of the many individuals impacted. As the UK data protection regulator, ICO, noted back in 2018, "A breach can impact business transactions and your staff's ability to work, but remember the risk in a personal data breach is to the data subjects."

### It's an event that is fast-evolving and full of uncertainty

Whilst you may (eventually*) be sure that a breach has happened, confirming the full scope of the incident is not straightforward. External technical and forensic experts are often required to help organisations contain the data breach and understand just what data has been (or could have been) breached. For example, what may have looked like 90 customers on a Friday afternoon could become 900,000 by Monday morning. The facts are usually unclear in the early stages, which means that making decisions and agreeing on strategies requires very careful consideration and can be very difficult.

### Timeframes are uncompromising

Whether driven by regulatory timeframes or media and social media sentiment, businesses need to react very quickly, and in a way that shows ownership and control.

*The average time taken to identify and contain a data breach is 279 days, based on the research by IBM and Ponemon: Cost of a Data Breach Report (2019)

### It's often targeted at your company

Someone, or some group or organisation, has specifically gone after your systems and data, whether an outsider or insider, often for criminal gain. You're in the spotlight.

### You are likely to need 'surge capacity' and specialist support

From the technical and forensic experts to customer notification, support and protection, a data breach presents challenges that require unique skills and experience (given the financial, reputational and regulatory impacts). If the data breach is material your business as usual capacity probably won't be able to cope with the scale of response required, so you'll need to find a supplier who can provide a high volume of skilled resources at very short notice.

### Victim vs villain

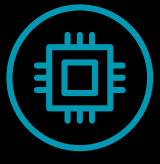
A malicious actor has broken into your system, so you feel like the victim. But your customers and the general public see things very differently. Why weren't your security systems stronger? Why did you not install the latest, publicly available patch or upgrade? To your customers, now facing the risk of financial loss or significant personal inconvenience, you are seen as the villain.

### It challenges both competence ("you lost my details") and character ("we don't trust you")

Where other crises just reveal a failure of competence or a crisis of character. Your brand will take a double hit, with a drop in brand value or share price and an increase in customer attrition.

### The legal claims will follow

With the advent of GPDR and the arrival of US-style litigation firms in Europe, not to mention recent cases such as *Justice Warby and Lloyd vs Google,* the risk of group or class actions after a breach is now material.



### Data Subject Access Requests (DSARs)

One of the many consequences of a breach, that many businesses often overlook, is that once your customers are concerned about the security of the data that you hold about them, many of those same customers will want to know just what data you do actually hold. DSARs are likely to follow (by letter, email, web form or call). You have 30 days to respond to each one, and they are often part of the "long tail" of a data breach. This heightened scrutiny from customers is likely to create more work for businesses.

# What does this mean for your crisis plans and your response capabilities? And what are the implications for your business?

In short: Generic crisis plans are insufficient when dealing with a data breach. Importantly, and as a direct result of gaps in your planning approach, your response to a data breach is likely to be slow and less effective. This could mean that the operational, financial, regulatory and reputational impacts to your business will be more significant.

From our experience of supporting businesses when planning and responding to data breaches, we see two key areas in preparing effectively for this exceptional type of crisis:

- Create specific data breach plans, and test them regularly. Where data breach plans do exist we often find that organisations test them on a sporadic basis, often only once every one or two years. With the rising frequency of cyber-attacks and the continual evolution of hacking strategies, mature organisations should ensure that their data breach plans and response strategies stay up to date and are tested regularly. Make sure you also think about your end-to-end supply chain when testing your plans, and include your key stakeholders when you test the full range of scenarios that could arise.

- Understand the capabilities and capacities that you currently have in place for breach response and those you will need to deploy to respond effectively to a breach (see Data Breach Readiness Review on the next page). Next, identify where gaps exist and take a risk-based approach to prioritisation and remediation where required. You will need to consider what expertise you may need, and at what scale to respond rapidly and effectively. Think carefully about what could be delivered in-house and where it would be more effective to utilise specialist third parties. Where third party help is needed, identify the right partners and build the necessary relationships. Given the fast-moving nature of a data breach, and how quickly you need to respond, a data breach is one crisis where you need to make your friends before you need them. And ensure you involve those 'friends' in your data breach response tests.

# Preparation and readiness

Conducting a Data Breach Readiness Review (DBRR) provides a comprehensive, cross-functional review across all key aspects of a data breach response, providing full visibility of gaps and vulnerabilities and thereby highlighting areas for training and remediation.

To manage a response successfully you need to have a fully aligned plan ready and tested. Our review checks every component to provide insight into your current level of preparedness.

The DBRR covers all of the following elements:

- Technical and cyber response plans and playbooks
- Forensic investigation strategies and resources
- Customer notification, support strategies and implementation plans
- Customer engagement capacity and infrastructure
- Stakeholder management plans, resources and templates
- Insurance awareness, strategy and reality
- Legal support and access to privacy expertise
- Regulatory strategy and response
- Incident response capabilities
- Cyber crisis strategies
- Executive awareness
- Third party support strategies
- Training, awareness and exercising
- Media monitoring, management and social media response
- Assurance and governance.

Use the Data Breach Readiness Review to measure your capabilities. As noted above, the review provides your organisation with full visibility of any gaps and vulnerabilities. A risk-based view is then taken to allow you to prioritise any training and remediation activities, helping you feel prepared should a breach occur.


## Conclusion

A data breach starts as a technical incident but can quickly grow into a brand-damaging crisis. They are full of complex information, uncertainty and critical timelines. As such they are fully deserving of a robust playbook that brings together the various teams involved, clarifies responsibilities, identifies desired strategies and tests them regularly.

When we are called in to support businesses we often see a lack of sufficient understanding at senior levels of the complexities of the solutions required. Training is key to build up the awareness of these issues and the possible solutions. Regular scenario-based discussions and exercises allow clarity to develop and confidence to build.

As the great adage goes, if you fail to plan you are planning to fail, although for a data breach it may be better written as "if you fail to plan and practice, you are planning to fail to perform."

# Get in touch


**Mark Whitehead**

**Director**

+44 20 7303 0698

marwhitehead@deloitte.co.uk



**Hugo Morris**

**Partner**

+44 20 7303 5985

hmorris@deloitte.co.uk


Deloitte.




Designed and produced by Deloitte Creative CoRe RITM0455499