Deloitte.

Responding to a data incident: a consumer duty

Mar 2024

A customer-centric response to a data breach

In today's digital age, businesses collect and store vast amounts of personal and behavioural data, which creates a lucrative industry for cybercriminals to exploit. A data breach can have severe consequences for both customers and organisations. Whether it's financial data, healthcare information, or basic personally identifiable information (PII) that an organisation holds, all of it can be sold on the dark web. Cybercriminals then make vast amounts of profit through transactions with other criminals.

The Information Commissioner's Office (ICO) defines a personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data", which would deem it a reportable incident.

40% of businesses experienced a cyber-attack in the last 12 months, with the ICO receiving over **10,000** reports of data breaches annually [1]

In our experience, regardless of whether an organisation concludes that an incident is deemed a reportable personal data breach by the ICO, they will still notify their customers and affected data subjects, notifying them of a cyber security incident.

This offers a level of transparency and demonstrates that an organisation is aware of, and on top of the situation, even if they conclude that there was no malicious activity to scrape or harvest the data for further use. A customer or data subject then has the option to take steps to protect themselves or contact the organisation for further support and assistance.

A duty of care to the customer or data subject is ever present, as it is their data that is held and at risk. Organisations must ensure they act and communicate swiftly and adequately.

A well-run, supportive and customer-centric approach can build reputational prowess, instilling confidence and maintaining consumer trust.

A poorly executed response could be detrimental to a company's reputation and future financial success. If a customer's trust is lost, due to poor communication, the customer could very well take their business to a competitor.

This insight piece focuses on the key components of a successful customer-centric response. This aspect of a data breach is often the most complex and publicly scrutinised, in addition to being the most overlooked and most impactful.

[1] Information Commissioners Office: Cyber Security Breaches Survey 2022

Preparing a response

According to a survey by Deloitte[3], **73% of consumers would lose trust in a company if their data was compromised.** It is therefore no surprise that 51% of organisations are "planning to increase security investments as a result of a breach, including incident response (IR) planning and testing..."[2].

There is a glaring opportunity for organisations to retain customer trust by implementing a response that is informative and supportive for victims, to help limit or offset potential physical, material and non-material damage.

$4.5 million the average cost of a data breach in 2023 (a **15% increase** from 2020) *[2]*

When it comes to the initial incident response, regulatory and legal impacts are vital to consider, as well as document/data reviews and intrusion forensics which help identify what has happened. However, a crucial component during and after these phases is being able to notify, support and protect affected data subjects in line with consumer rights and the ICO regulations.

To fulfil these objectives and to minimise the risks of reputational and regulatory fallout associated with a data breach, **organisations must have an effective, tried and tested response plan in place, ready to be invoked at any time.** This will include an operational readiness strategy and playbooks to manage the aftermath of an incident.

[2] IBM's Cost of a Data Breach Report 2023
[3] The Deloitte Consumer Review – Consumer data under attack: The growing threat of a cyber crime

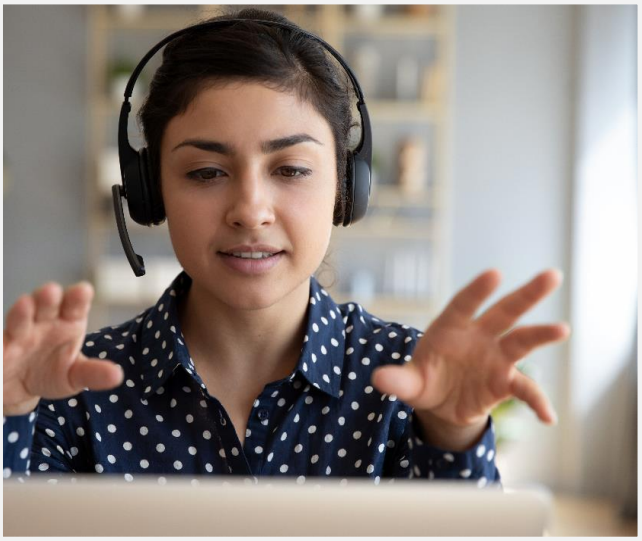
Supporting customers after an incident - the components of a response

There are **three key components** to a data incident customer-centric response. All should be carefully considered and planned for.

Notify **Support** **Protect**

1. Notify: outbound communications to affected data subjects. Organisations must communicate with affected data subjects to inform them of the breach, the type of data exposed, and the steps the organisation is taking to address the issue.

2.Communication should be clear, concise, and timely. A dedicated communication plan should be developed and implemented to ensure that customers are kept informed throughout the process. This can include email notifications, social media updates, and website alerts; there may also be multiple release phases in more than one language.



2. Support: organisations should expect an increase in inbound calls from concerned customers following a data breach. To manage this surge in activity, organisations should have a plan in place to increase call centre staffing levels and be equipped with the appropriate message and FAQs for a consistent and informative response. This will ensure that callers get the help they need and reduce wait times.

Call centre staff should be trained to handle conversations surrounding sensitive customer information and be able to provide clear instructions on how to further protect themselves and their data post incident. Telephone infrastructure must also be rapidly scalable to be able to cope with the anticipated load.

3. Protect: offering dark web and credit monitoring services to affected customers can help to mitigate the impact of a data breach. Dark web monitoring can alert customers if their information is being sold or shared on the dark web.

Credit monitoring services can alert customers to any suspicious activity on their credit report, enabling them to take action to prevent further damage. Offering these services demonstrates that the organisation is taking steps to protect its customers and will help to rebuild trust.

What should organisations be doing to mitigate a cyber security incident?

A customer-centric response to a data incident will minimise reputational damage and crucially, will provide vital support to the data subject. However, the mechanics can be very complex, and the scale particularly hard to meet, given the short, sharp requirement for effective and supportive two-way communications.

Organisations often lack the technological scale and agent resource capacity required to meet surges in contact demand.

To reduce the risks associated with a data breach, organisations must prepare in advance by investing time, allocating budget, and leveraging expertise to support affected data subjects/customers. Experts and specialist cyber risk services are often a consideration for organisations given the complexity, scale, and sensitivity of the risk of a data breach.

Three actionable pillars can build the foundations of a customer-centric response:

Prepare

Develop a readiness plan and playbook covering outbound communications, increased call centre staffing, and offering dark web and credit monitoring services.

Test

Exercise, test and maintain the readiness playbook alongside any interactions with third parties via live environment or desktop drills.

Partner

Seek a trusted, experienced, external party for impartial support around preparation and mobilisation in the event of an incident.

Deloitte.

How can Deloitte help?

Deloitte's Customer Breach Support is a cyber risk service that helps clients minimise the impact of a data breach — by putting the customers at the heart of a response and guiding them through the response period following an incident.

Our comprehensive response service includes customer breach notification plans, communications templates and scalable infrastructure. Trained resources are ready to engage, support and protect customers and thus the organisation, through a crisis.

Our Risk Advisory team will guide you through a readiness programme to put in place the plans, artefacts and documentation which is then exercised and drilled to prepare you for a data breach.

Contact Us

Hugo Morris
Partner,
Risk Advisory
+44 20 7303 5985
hmorris@deloitte.co.uk

Andy Hanlon
Associate Director,
Risk Advisory
+44 20 7303 8732
ahanlon@deloitte.co.uk