MetaCompliance®
Make it personal.

The Key Steps to Effective Data Breach Management

The Key Steps to Effective Data Breach Management

Imagine the panic when a massive data breach is detected, perhaps one that has been ongoing for months.

In 2023, the American retail company Target announced that it had suffered a massive data breach that exposed the personal information of over 100 million customers.

The breach was caused by a vulnerability in the company's payment processing system. Target had been aware of the vulnerability for months, but had failed to patch it. As a result, hackers were able to gain access to Target's systems and steal the credit and debit card information of millions of customers.

The Target data breach was one of the largest data breaches in history, and it had a significant impact on the company. Target was fined $192 million by the U.S. government, and its stock price fell by more than 20%.

The breach also led to a loss of trust among consumers, and Target is still struggling to recover from the damage.

The Target data breach is a reminder of the importance of data security. Organisations need to take steps to protect their data from unauthorised access, and they need to have a plan in place to respond to data breaches if they occur.

By “walking a mile in someone else's shoes”, we can understand how each part of an organisation effectively deals with a data breach. By reflecting on how each department can help to de-escalate the chain of events that lead to a data breach, data exposure can be managed more effectively.

The Who, How, and Why of Data Breach Management

Data breaches affect everyone in an organisation. By the same token, everyone can help to prevent or minimise the impact of a data breach. Let's now look at the different responsibilities of five key areas in an organisation, and the type of responsibilities each has, in managing a data breach.

The Security Incident Team

Cyber-breach detection and prevention is the mainstay of the Security Incident Team. This team has been increasingly called upon as data breaches increase in numbers and intensity. Their role is central to the management of a data breach, and the team relies on a robust process to help them in this task.

The security team should be able to turn to an Incident Response Plan and a Disaster Recovery Plan to help them contain the breach. These plans help to inform actions once a breach occurs. Typical steps in breach containment and management include:

Confirm the breach

It may seem an obvious step, but confirm that the breach has happened, and if it impacts confidential or sensitive data. The data collected during breach analysis will be called upon if the breach is bad enough to notify a Supervisory Authority. Information that should be collected and documented includes:

- How the breach was detected
- Where it occurred
- Who is impacted (include any ecosystem vendors)
- Who reported the breach
- The date(s) any breaches occurred
- What level of risk the breach poses to the organisation/customers, etc.
- Is the breach now fully contained?

How did the breach occur?

An analysis of the breach is not only needed for compliance reasons, but it can also help mitigate future data exposure. Breach dynamics are varied. Data can be exposed by a variety of both accidental and malicious mechanisms. Identify these mechanisms: was this an accidental employee exposure, or a malicious hack? Understanding the vectors and tactics used can help alleviate the exposure and mitigate the attack.

The type of data affected

Being able to identify the risk level of data impacted is crucial both for breach notification and compliance, as well as understanding the overall impact on the business. Document the type and risk level of data breached. An organisation hould already have developed a classification system based on a standard such as ISO 27001. This standard sets out four categories of data:

1. **Confidential** (only senior management have access)
2. **Restricted** (limited employees have access)
3. **Internal** (all employees have access)
4. **Public information** (everyone has access)

Containment and recovery

Once a breach has been detected it is vital to contain the breach as fast as possible. Actions taken during the breach analysis will allow a strategy of containment to be created. Breaches that involve employees may require a review of Security Awareness Training. Breaches that involve external malicious hackers will need further exploration of systems and mitigative measures. Recovery plans must be put in place to minimise the impact of the breach.

Legal and compliance

All of the documentary evidence collated on the breach is used by the legal and compliance departments to deal with the aftermath of the breach. The legal and compliance teams will decide if the breach falls under the remit of a breach notification requirement; for example, under Section 67 of the UK's Data Protection Act of 2018 (DPA 2108), a data breach notification must be made to the ICO within 72 hours of the company becoming aware of the breach.

All of the documented evidence on the breach, the where, why, and how it is mitigated, collected by the security team, will be used in this disclosure. There may also be a requirement to disclose the breach to anyone affected. This may require a full public disclosure letter published on the company website.

Notification rules

Key to the legal handling of a data breach is making an informed decision as to if/when to notify the Supervisory Authority about the breach. Questions such as: "Is there a regulatory imperative to report the breach?" can only be done by qualified, knowledgeable staff.

This decision may require the breach to be made public: this has obvious long-lasting reputation effects and will likely involve the Marketing Department to minimise brand impact. Here are a few examples of public breach notices:

- Equifax
- CapitalOne
- Twitter
- People's Energy

The breach notification rules vary across different regulations. For example, according to the EU's General Data Protection Regulation (GDPR), breach notification must be done within 72 hours of identifying a breach has occurred. However, under the Privacy and Electronic Communications Regulations (PECR, regulation that is applied to internet and telecommunication service providers) a personal data breach must be reported to the ICO no later than 24 hours after detection.

The staff

By making staff part of the breach management process, they become a frontline resource in the fight against cyber attacks. Staff and their security behaviors cover a wide spectrum of potential vulnerabilities from accidental data exposure to phishing, and collusion with external hackers.

Around 23% of data breaches can be traced back simply to errors. This is up from 17% in 2020.

Source: Report by IBM and Ponemon Institute.

For example, employees sharing passwords, or reusing passwords across multiple applications is poor security practice. Phishing is still the cybercriminals' weapon of choice; phishers love to mimic brands like Microsoft to trick users into handing over corporate credentials. Security Awareness Training teaches employees about the many positive ways they can help to maintain a good company security posture.

In terms of breach management, staff awareness must extend to an understanding of their responsibilities within various regulations, such as ensuring that customer data is respected and used within the confines of legislation such as DPA 2018 and GDPR. By understanding where a breach could occur, along with responsibilities under various relevant regulations, an organisation can co-opt staff into the breach management process.

It is important, however, to train staff to the relevant level. Some staff, such as technical employees, may need specialist security training and/or go through certification.

New hires must be onboarded to an organisation's Security Awareness Training programs from day one. Regular reviews of Security Awareness Training of staff in areas such as:

- Phishing
- Security hygiene
- Awareness of data security responsibility

Security Awareness Training should be incorporated into the organisation's security policy as part of a data breach management process.

Third party vendors

Vendor ecosystems can be complex and can involve fourth and fifth-parties According to a report by Cybersecurity Ventures, 45% of security breaches in 2023 will be caused by supply chain attacks. This is up from 40% in 2020.

Vendor risk management is part of the effective management of a data breach. Vendor-related data breaches are a two-way consideration. As well as performing a vulnerability analysis of the vendor links to mitigate cyber attacks when a breach occurs, the vendor ecosystem must be analysed to see if the breach impacts the vendor.

A UK Gov report, "Cyber Security Breaches Survey 2023 by the UK Government", found that: 81% of businesses believe that cyber security is a high priority for their directors or senior managers.

As a result of the high-profile of data breaches, more boards now include security domain experts. When a data breach occurs, an educated board can support the rest of the organisation in handling the breach, ensuring that regulatory requirements are met, and ensuring that a budget is available to manage the breach and mitigate against further attacks.

Using frameworks to manage data breaches

Security frameworks are an invaluable tool, offering guidance on data breach management and creating a robust security posture. Two important frameworks that help in delivering exceptional security and managing data breaches are:

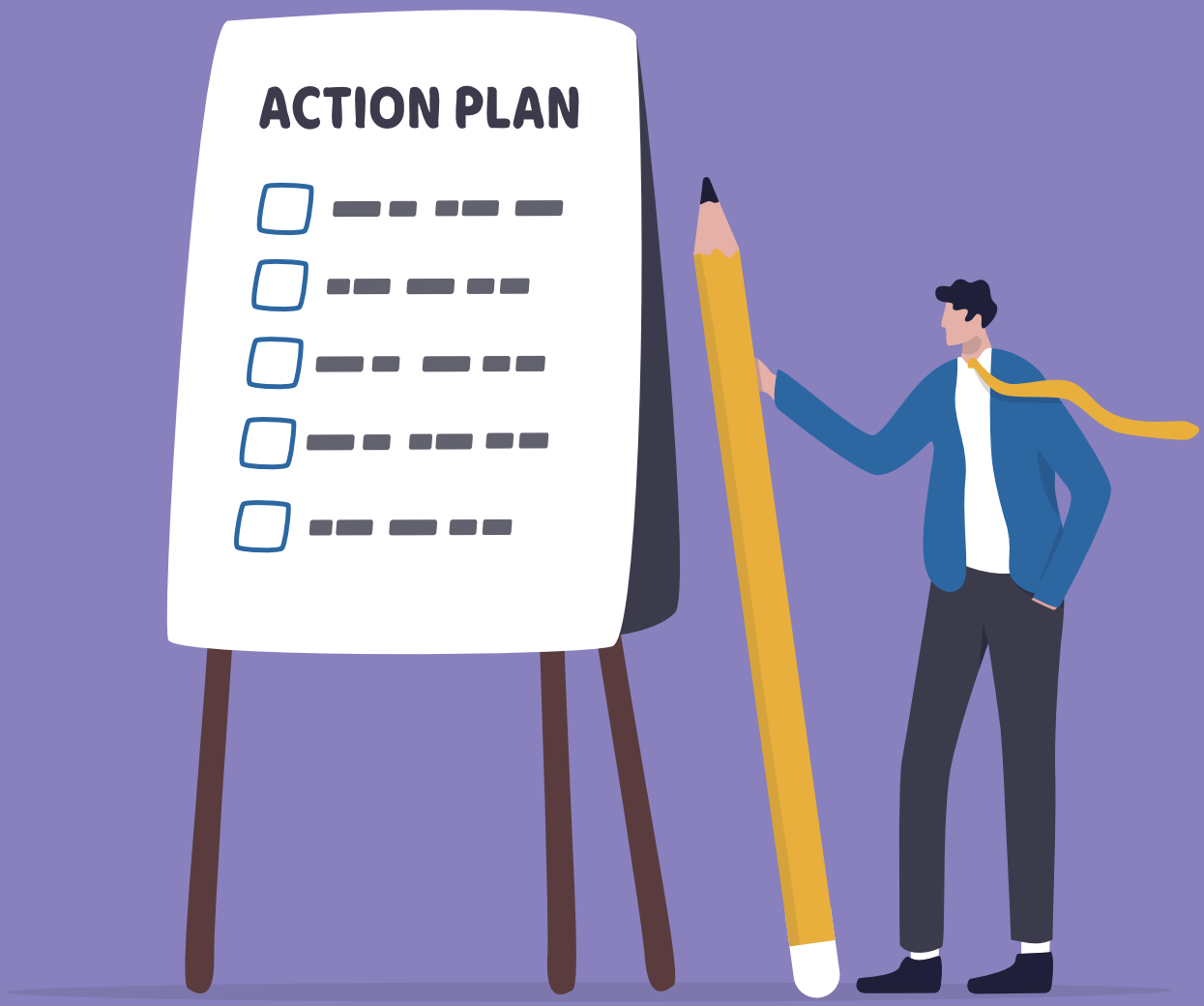
ISO 27001

ISO 27001 is an international standard that offers specifications on building an information security management system (ISMS). ISO 27001 is a certification-based standard that is recognised across the world. Any organisation holding ISO 27001 certification demonstrates they take information security seriously. The standard is based on people, process, and technology.

Cyber Essentials

UK security framework Cyber Essentials includes assessment of several security measures used by an organisation, including supply chain security, patch management, and access control. This standard comes with two certification levels, the lower of the two being self-assessed.

Do Employees Know What to do When There is a Breach?



Putting breach management measures in place is a whole business task. One of the key parts of delivering effective data breach management is in the way that you train your staff. Relevance is key in ensuring that incident management works for your organisation. Every organisation must develop its own relevant and unique approach to reporting and managing a security breach.

Drilling down to optimise awareness begins at the people and process level. Every aspect, from the smallest detail to the big picture, must be thorough enough to ensure that your Incident Response Policy is robust and understandable by all staff. This must include:

Communications — From the telephone numbers used, to the email address, or any other system used to report a breach

Roles and responsibilities — Highlighting the relevant incident managers and their responsibilities

Actions — Who does what, when they do it, and how they carry out their role in helping to manage a data breach

Remediation — How to fix the breach and lessons learned, including any update to Security Awareness Training

In larger multinational companies these lines of communication need to consider the entire organisation, bringing the company departments and offices together.

Everyone needs to buy into this plan, from employees to managers to board members.

Reduce the Risk of a Data Breach ⇦

In need of a complete solution for Security Awareness Training and compliance?

To hear how MetaCompliance can help mitigate the risk of cyber threats and develop cyber resilient staff, get in touch.

info@metacompliance.com
www.metacompliance.com

MetaCompliance®
Make it personal.