Data Breach Response Steps

Why Fast Response Matters

Feeling overwhelmed by a data breach can happen to anyone at any time but especially at a small/medium sized business may not have sufficient IT or legal resources on hand to deal with it. Ensuring that you act fast and in a methodical manner will greatly help limit the damage; demonstrate to others that this was taken seriously and assist in fulfilling your obligations under the UK's GDPR and Data Protection Act 2018.

Responding quickly and calmly will help lessen the effects on your customers, employees and your reputation. Additionally, this will help you determine if you should notify the ICO within the required 72 hours; which is a critical requirement if certain conditions are met with respect to the breach. Taking too much time or panicking can serve to only exacerbate your position.

This report provides a clear, concise framework based on guidelines from the ICO to provide you with the tools needed when responding to a data breach; including definition of breaches; steps to follow when responding to a breach; documentation and report writing methods; etc… Once you have completed review of this document, you will know more about the next steps you will need to take in order to respond appropriately.

What Counts as a Data Breach Under UK Law?

Breach of Personal Data

"A breach occurs when there is a failure of security and results in the unplanned or unauthorised destruction, loss, alteration, unauthorised access or disclosure to personal data."

What constitutes Personal Data?

Personal Data is made up of the following:

- Names
- Email Address
- Payroll Information
- Customer Records
- HR Files
- Data that can identify a specific living person.

There are different types of breaches that can happen, including accidental and cyberattacks.

Accidental breaches:

- Mis-Mailing of Email
- Lost Device

Cyberattacks:

- Hacked Accounts
- Ransomware.

It is also worth noting that not all types of breaches related to personal data are a result of cyberattacks.

Common Breach Types in UK SMEs

- Emails Sent To The Wrong Address
- Phishing Attempts And Account Compromise
- Laptops Lost Or Stolen
- USB Drives Not Encrypted
- Ransomware Attacks
- Cloud Folder Sharing Too Much
- No Removal Of Ex-Employee Access
- Brief Descriptions Of Each Type Of Breach.

Step-by-Step Breach Response Framework

1. Contain the Breach (Immediate Actions)

- How can you stop any further exposure?
- Disable any compromised accounts.
- Revoke user access from any affected accounts.
- Disconnect any infected devices.
- Retrieve any emails or files that were sent in error, if possible.

2. Assessing Risk to Individuals

- Was any of the data involved sensitive?
- Could any of the data involved cause harm to anyone?
- Was the data encrypted?
- Is it likely to be misused?
- Clearly and calmly explain the “risk to individuals” test.

3. Document Everything

- Date and time the breach was discovered.
- Describe the circumstances of the incident.
- What type of data was involved?
- Who was affected?
- What actions did you take?

4. Determine if Notification of the ICO is Required

- Determine if the 72-hour rule applies (from when you became aware of the breach).
- Provide a high-level explanation of the breach.
- Is there an impact on an individual's rights and freedoms?
- When do you need to notify the ICO?
- When do you not need to notify the ICO?

5. Notify Victims (If Required)

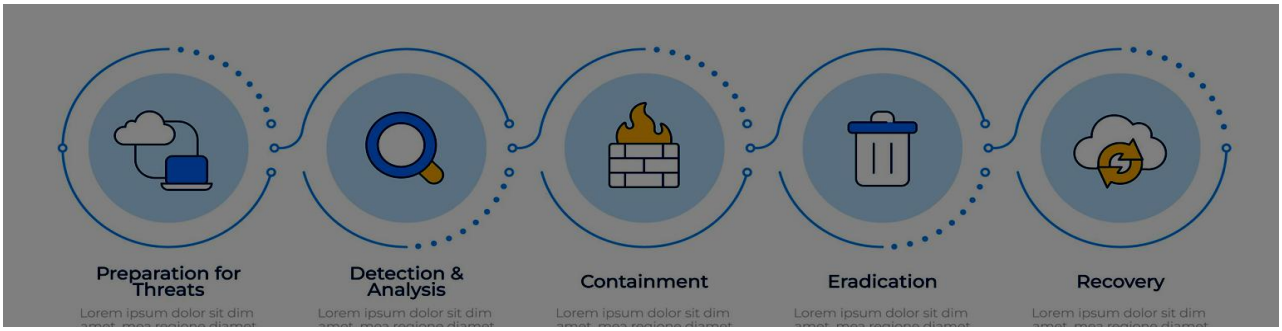
- If a high risk exists notify individuals.
- Clearly communicate with all affected individuals.
- What to include in your message.
- Avoid placing blame on anyone.

6. Remediate and Strengthen Controls

- Reset all user passwords.
- Implement multi-factor authentication.
- Encrypt data.
- Make sure you have the latest patches installed.
- Conduct backups and verify they are working properly.
- Provide additional training for staff.

7. Learn from Incident & Update Policies & Procedures

- Review your processes to determine changes required.
- Provide staff refresher training on policy/procedure changes.
- Make necessary technical improvements.
- Ensure compliance with Cyber Essentials.



When to Inform Affected Individuals

The following are examples of potential victimised persons who would be at some risk for identity theft, fraud, etc.:

- Payroll data breach
- Identity information exposed
- Financial information comprised
- How To Calmy Communicate For Containment Purposes

Technical Containment Steps

- Lock Account
- Apply MFA
- Reset Passwords
- Check Email Rules
- Scan For Malware
- Check Backup Integrity
- Preserve Logs

Communication Strategy (Internal & External)

Internal Communications

- Notify Directors
- Notify Human Resources (if employee data involved)
- Provide Clear Messaging To Employees

External Communications

- Notify Customers
- Notify Suppliers
- Notify I.C.O.
- Notify Charity.
- In the event of a crime: Police law enforcement.

Downloadable-Style Breach Response Checklist Template

Incident Log Template

- Date found
- Discovered by

- What happened?
- What systems impacted?
- What Personal Data impacted?
- Containment action taken
- Risk assessment summary
- ICO notification decision
- Individuals updated?
- Future actions following agreement with ICO

ICO Decision Chart

- Is personal data involved?
- Is individual at risk?
- Is there likely to be Harm?
- Data encryption?
- Is misuse likely?
- 72 hours from discovery?

Internal Reporting Process

- Staff report
- Manager reports upward
- IT investigates issue
- Director notified
- DPO, if applicable, is consulted

Post-Breach Review Checklist

- MFA reviewed
- Password Policy reviewed
- Access check completed
- Backups tested
- Employee Training refreshed
- Policy updated

FAQs

- **What happens if we don't submit our report within 72 hours?**

Submit immediately with explanation for delay. The ICO will take into account whether there was timely reporting, as well as general handling of the incident.

- **Is it mandatory to report breaches?**

No, only report when there is a potential high-risk type of breach impacting a person's rights/freedoms. If low risk/very little or no risk, you should have it noted inside the organisation only.

- **What do I do if I am unsure whether to report?**

Write down how you came to this conclusion. You may want to contact your DPO, an advisor, or the ICO helpline for assistance. The ICO prefers you to over-document than under.

- **Who from the business is responsible for this?**

A senior person will be responsible (director/owner), but management should appoint a person to be the lead on incidents.

- **Will cyber insurance pay for this?**

Most have covered notification, forensics and PR in their policies. Check yours. Quick action can help your claim.

About This Guide

Computer Support Centre (CSC), an IT & Cybersecurity consultancy based in the United Kingdom, has developed this guide to assist small to medium-sized entities (SMEs) implement practical data protection, incident response, and compliance frameworks. The content of this guide is drawn from Computer Support Centre's experience working with organisations to respond to accidental sales/disclosures; phishing; ransomware; and loss of devices in a consistent, proportionate manner. The objective of this guide is to provide directors and managers with simple, non-technical guidance that they will be able to use right away and without unnecessary legal complexity. This guide is supplied for education-related purposes only; no legal opinion is intended or created. For more information regarding how Computer Support Centre can assist with your Cyber Security needs please visit https://computersupportcentre.com.

Conclusion

Data breaches do not always equate to a failing business or a reason to panic or think of it as a regulatory disaster. Most data breaches experienced by small companies in the UK come from unintentional human error, such as failure to properly implement access controls, losing devices, phishing scams, etc., rather than from an organised hack. The critical consideration is how quickly and effectively the business can react to a breach. To be considered appropriate and responsible, businesses must have, at a minimum, a structured approach to responding to a data breach that includes containment of the breach, evaluating risk to data subjects, documenting their actions, and notifying relevant parties (if required) under the UK GDPR. Preparation is what will help you! Having a well-thought-out response plan prior to an incident can help reduce lots of confusion and stress and provide a more seamless transition for all concerned after a breach occurs. If businesses have established and implemented the required processes and minimal safeguards necessary to enable them to manage a data breach professionally and transparently, they can do so.