

HOW TO RESPOND TO A DATA BREACH

No organisation is immune to cyber threats. Breaches can happen in any sector and to any size of business. A clear plan helps you act fast, reduce harm, and stay compliant

WHAT IS A DATA BREACH?

A data breach happens when sensitive information is accessed, lost, disclosed, or changed without permission. It can result from criminal activity such as ransomware, or simple mistakes like sending personal data to the wrong person. The data involved might include names, addresses, National Insurance numbers, or medical records.

WHAT TO DO FIRST

When a breach is suspected, move quickly. Alert your IT and cyber security teams, contain the incident, and preserve evidence. Record what you know, including when the issue was discovered, which systems are affected, and what type and amount of data may be involved. Carry out a risk assessment to understand possible harm to individuals and to spot any control weaknesses.

REGULATORY DUTIES

If the breach poses a high risk to people's rights and freedoms, you should notify the Information Commissioner's Office within seventy two hours of becoming aware of it. You must also inform affected individuals without undue delay. Even when notification is not required, keep an internal record of every breach. A consistent reporting process supports accountability and ongoing compliance.

HOW TO PREVENT FUTURE INCIDENTS

Use every breach as a prompt to strengthen defences. Review risks regularly, enforce strong access controls, and encrypt sensitive data. Maintain and test an incident response plan, and bring in certified cyber security professionals where needed. These steps help reduce legal, financial, and reputational exposure.

Protect your business today. Book a cyber risk review with our team:

01730 265500 | hello@robison.co.uk