SBS Cyber Security

sbscybersecurity.co.uk

186 Cheetham Hill Road,
Manchester,
M8 8LW

M: 0161 827 1600

How to create and implement a data breach incident response plan for your business

Fail to prepare, prepare to fail goes the saying. For any size business, this old adage has a particular resonance when it comes to information security. If your business suffers an information (data) security breach – a hacker breaks into your computer system and steals customer details for example, or perhaps a member of staff leaves a laptop on a train or loses a file (hard copy or digital) of information – it could already be too late to minimise the possible financial and reputational damage if you don't have a robust data breach incident response plan in place, tested, and ready to be implemented.

Surprisingly, according to figures from Experian, a third of UK businesses don't have a data breach response plan in place. But in our experience this is actually much higher. Given the media firestorm that's been raging around household brand names such as TalkTalk, Carphone Warehouse, Morrison's and M&S following data breaches, it's worrying that so many businesses are not prepared for the (almost) inevitable cyber attack.

Create your plan

Every business, even the smallest businesses, should make sure that they have done everything possible to prepare for a data breach. Here are some tips to getting your own incident response plan in place:

Information assets: know what data you have

What information is critical to your business? What databases do you have? Where do you store information? Many problems arise because businesses aren't always clear about what information they have and where it is stored.

- List all your information assets such as email, customer databases, Microsoft Office documents – Word, Excel – and understand what risks they could be vulnerable to (eg) hacking, theft, employee misuse.
- What IT services do you rely on e.g. the ability to take payments via your website for example? If these are down, you will need a back-up to trade while the hack is being investigated.

sbscybersecurity.co.uk
186 Cheetham Hill Road,
Manchester,
M8 8LW
M: 0161 827 1600

Technical: dealing with the actual data breach
Speed is of the essence after a data breach: it's key that any breach is closed off as quickly as possible to prevent any further loss of data as well as understanding what data has been lost.

Then there's the business imperative of getting systems up and running to resume 'business as usual'. Your incident response plan should have clear procedures in place as soon as a breach has been discovered.

- Make sure you have access to the necessary technical IT and computer skills. You might have these within your business or, more likely, it will be a reliance on your external IT expert to help. Check with them that they are comfortable when it comes to dealing with a data breach or hack and that they available 24/7 365 days a year if there's a problem. If not, find a supplier who is.
- Your systems must adequately record the movement of data so you can be in a position to quickly investigate what information may have gone missing/been compromised. For example, make sure your system records when customer databases are accessed and by whom.

Legal: identify your legal support
A hacker calls you to say they've hacked into your system and is going to release all your customers' details onto a file sharing site? Who are you going to call?

- Get access to the right legal support. They should be available at any time of day or night.

Communication: keeping in touch with your customers, suppliers, regulators
Good communication following a data breach can be the difference between keeping your business afloat and going under. After all, reputation is everything.

- Consider and list who you would need to notify in the event of an attack; customers, suppliers, and other third parties such as regulators.
- How would you notify them? You'll need to use multiple communications channels; possibly by phone, email and social media.
- What will you tell them? As a small business it's likely that you'll need to personalise communications as much as possible. Bigger clients for example would appreciate a phone call rather than just an email. Clients will be looking for reassurance that the situation is under control.

Test and test again
Finally, any plan is only any good if you know how to implement it and whether it remains up to date. Regular testing is important through the running of possible data breach scenarios. You can do it as a desk-based exercise to help each employee understand their role after a possible breach.