+44 345 094 0945
www.waterstons.com
Article

Get Breach Ready - Minimise the impact of a successful cyber attack

Breadcrumb

1. Home /
2. Print /
3. Pdf /
4. Node /
5. Entity Print

Insight navigation

- Latest insights
- Latest news
- Articles
- Case studies

Download PDF

Apr 2024

Get Breach Ready - Minimise the impact of a successful cyber attack

The main topic of conversation around cybersecurity often focuses on preventing data breaches, but what we forget is the processes needed to minimise their impact. Even with staff training and patching, organisations will often overlook the mitigation of data breaches should they occur, and this is a common GDPR shortfall.

Categories Cyber Resilience

Apr 2024

Simon Holroyd

Senior Information Security Consultant

Email

simon.holroyd@waterstons.com

However, organisations that are ahead of the game will have already transitioned their legacy data with robust cyber security, in addition to the reorganisation of their folder structures.

To get your organisation ahead of the game and breach ready, let us guide you through implementing some effective strategies so you can be sure your data is secure.

Managing breach risks

Risk is generally defined as a combination of the likelihood that something unwanted will happen multiplied by the impact it would have and there are many methods to reducing cybersecurity risks, including:

1. Establish a cyber vision
2. Build the human firewall
3. Build your cyber resilience
4. Plan to respond and recover
5. Establish strong partnerships

However, for whatever reason, somewhat less effort goes into reducing the impact of a breach. That doesn't mean organisations aren't putting in place good practice such as network segregation and immutable backups but, with its GDPR-driven emphasis on storage limitation, it is the data protection community which is pushing hardest on getting rid of old data and in turn helping organisations reduce their exposure in the event of a successful breach.

Declutter your data

There are lots of good reasons for deleting old data, such as:

- Reducing storage costs
- Reducing Scope 2 and Scope 3 emissions
- Making it easier to find the information you need

But the GDPR-compliance assessments we've carried out across a range of organisations show deleting data to be the main area where many of us are falling short.

The reason given most for holding onto data indefinitely is 'just in case it's needed' but in practice legacy data is rarely needed and, without a well thought-through information management strategy, it is often too hard for future colleagues to find anyway.

The organisations we are helping get to grips with this are putting old data in cold storage, wrapped in governance and beyond the reach of hackers. They are implementing the folder structures they wish they had always had, and they are putting in place processes which will lock-in the hard-won gains they are making. Most importantly though, they are minimising the impact of a successful breach.

Here are our five tips for deleting data to minimise the impact of a successful data breach:

1. **Implement regular data audits**
2. **Adopt data retention policies**
3. **Have secure deletion processes**
4. **Encrypt sensitive data**
5. **Have clear document deletion procedures.**

Even if you are in the beginning stages of improve your cyber security or want to make sure your organisation keeps on top of it, consider this your go to guide.

For more information on how we can help you get breach body ready this summer,head to our page or get in touch at cyber@waterstons.com.