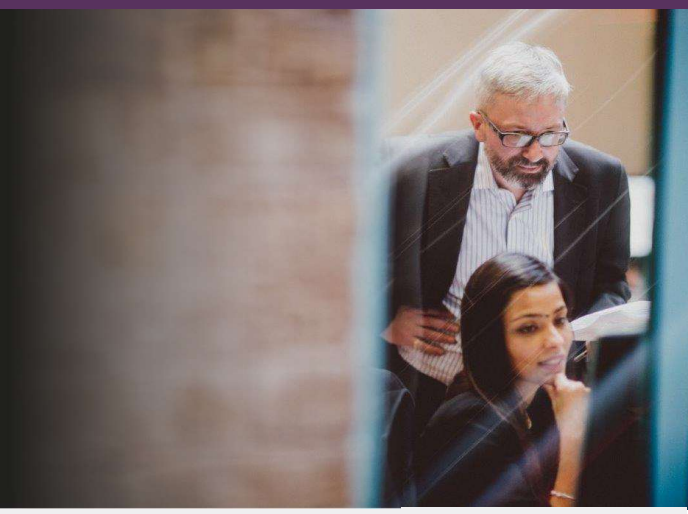
RIAA Barker Gillette

Always Available

Cybercrime: Managing the legal issues for victims



February 2018

Government statistics show that nearly seven out of 10 larger firms in the UK have been hit by a cyber-attack or a breach in the last year.

But it is not just the big names with an online presence being targeted. Increasingly smaller companies are finding themselves in the firing line, with nearly half of all UK businesses reporting at least one attack or breach.

Over 4 million individuals have also found themselves the victim of cybercrime, with 66% of cases resulting in a loss of money or goods.

The legal position

Cyber-attacks can cause havoc to a business. As well as raising questions about the security of IT systems, it also brings up many legal implications too. Just as it is a relatively new and constantly developing problem, it is also a relatively new and very complex field that requires expert legal knowledge.

If your business has been the victim of a cyber-attack, you could face a number of repercussions that can affect your profits:

- claims from customers who have suffered a financial loss as a result of the attack;
- loss of client data;
- disruptions of sales/staff work time; and
- damaged reputation.

Business owners can also face claims from customers for breach of data protection. If your contracts with clients state your responsibility for data protection, you could have to deal with being held in breach of contract.

What responsibilities do businesses have regarding customer data?

Currently, under the 1998 Data Protection Act (the DPA), organisations must take "*appropriate technical and organisational measures*" to protect personal data from unauthorised access or disclosure. However, as legal firms have found out over the last few years, the DPA has some serious holes in it that are being exploited, leaving businesses reeling not just from the attack itself, but the subsequent fallout.

To shore up those holes, in May 2018 the EU's General Data Protection Regulation will come into force. This will require all organisations to undertake data protection impact assessments for the riskiest uses of personal data.

It means that companies will need to 'continuously' identify risks that could put personal data at risk. Fines for any breach are expected to be significantly higher to a maximum of €20million or 4% of annual global turnover, whichever is higher. There will also be new legal obligations to report serious data security breaches and clearer guidelines on what data is regarded as 'vulnerable'.

The government has already stated that this regulation will continue to be enforced after Brexit.

Legal solutions if your business is a victim of a cyber attack

In the short-term:

- **Investigation**: be prepared for an in-depth investigation into any cyber breach, so make sure you have a solid plan of action to cope. Our lawyers can help you to decide if the incident needs to be reported to the Information Commissioners Office (the ICO).

Ensuring that breaches are reported sooner rather than later, and with full disclosure and details of preventative action initiated as a result can mean the difference between a 'lessons learned' scenario or regulatory enforcement.

- **Dealing with claims**: seek legal advice around any liability claims arising from the cyber breach. This could include investigation into the contractual position with any outsourced IT or virus protection providers to see if any losses can be recovered.

Longer-term:

- **Risk assessment**: cyber security risks should be assessed and a cyber security plan needs to be put in place. Because the threats to businesses are constantly changing, this needs to be regularly reviewed to ensure you are complying with legal obligations, giving customers and clients that all-important peace of mind that their data is safe.

  For more information visit the GDPR and employment and regulatory law pages of our website.

- **Review and training**: your legal team can advise on any review of systems to protect your business from future attacks and training required to help staff respond effectively.

Prevention

Our lawyers can review your situation before you fall foul of an attack. They can check your business complies with legal requirements and has the correct contracts, policies and procedures in place to effectively protect it.

Speak to data protection specialist, Veronica, today.

Veronica Hartley
020 7299 6922
veronica.hartley@riaabg.com
www.riaabarkergillette.com