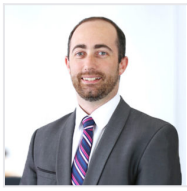
Legal Considerations Relating to Cyber Security and Cyber Insurance

AUTHOR / KEY CONTACT



Edward Adamson
Partner

edward.adamson@LA-law.com
01202 786115

The National Cyber Security Alliance reports that one in five small businesses will experience a data breach, with over half of those affected having to close their doors because they cannot recover from the financial consequences.

Even a relatively minor cyber security breach can cost a business dearly, including investigative and legal fees, loss of business, loss of data, downtime, inaccessibility to data, restoration of systems, and time and money spent on damage limitation. Sensitive data may be exposed, stolen, or held to ransom, and the business could be held liable under data protection laws if it is found to be in breach of the relevant laws and that breach caused a data breach. Therefore, the costs of a cyber security breach are too significant not to be taken seriously. In this article, we consider cyber insurance as a way to get some protection from a cyber attack, together with other points to consider.

Have you got protection?

Business owners could be left footing the bill for damages from a cyber breach without appropriate cyber insurance. Cyber insurance policies can be customised to an organisation's specific needs, but reviewing policies carefully and periodically is crucial. Cyber insurance can be very bespoke. It should not be just assumed that it will cover everything.

Cyber attacks are evolving continuously and a business could easily fall victim to a new type of threat that may not have existed at the time the policy was taken out. You should check with your broker whether you will be covered in that situation.

Most cyber insurance policies are re-assessed every 12 months. The onus is on you to ensure that your organisation's cyber security details are accurate and current with your insurer. If you claim security measures are in place when they're not, the insurer may not be obliged to pay any claims. It is, therefore, important to communicate well with your IT team, whether internal or external, to ensure that the technical measures are appropriate and notified to the insurer as required under the policy.

Some insurers will supply services that are invaluable when a cyber incident strikes. These can include IT forensic services, legal assistance and public relations support.

Your insurer may put you in touch with a Cyber Incident Response organisation or their own in-house cyber incident response team. If you find that option under your policy is too expensive, then you might find the NCSC's Incident Management guidance helpful in thinking about how to plan, build, develop and maintain an effective cyber incident response capability.

As well as cyber insurance and an incident response plan, you should have a disaster recovery plan and a business continuity plan in place so they can be enacted should the worst happen.

Consider also whether you provide sufficient training to staff for cyber security and data protection, as a large percentage of data breaches are caused by human error. Taking technical, physical, and organisational security measures should also assist a business in avoiding a cyber attack and complying with its legal obligations under UK legislation, including data security and data protection.

For further information on legal issues relating to cyber security, please do not hesitate to contact our Corporate & Commercial team by emailing online.enquiries@la-law.com or calling 01202 786188.

Tel: 0344 967 0793 | Email: info@LA-Law.com | www.lesteraldridge.com