Cyber risk - are you covered?

Recent high-profile incidents, such as the hacked celebrity iCloud accounts in August 2014, have shown that individuals, businesses and public bodies are all at risk of a cyber-attack. However, while awareness of the threat may have increased, recent reports suggest that many businesses are currently unprepared to deal with the financial consequences of an attack.

Cyber risk

The term cyber-risk is used to describe, at its most basic, an attack by one computer on another. The typical purpose of such an attack is to obtain sensitive data from and/or disable the target computer. The level of risk and likely financial consequences of an attack depend on the nature of the assault itself, the complexity of the attacked computer or network and the type of data affected.

While general awareness of cyber-attacks may have increased, a recent report by the Association of Insurance and Risk Managers in Industry and Commerce ("Airmic") suggests that many organisations do not fully understand the threat: Airmic's survey found that 62% of its participants were unaware of whether their organisation had been subjected to a cyber-attack, successful or otherwise.

In contrast, the UK Department for Business Innovation and Skills' 2014 Information Security Breaches Survey found that 81% of large organisations and 60% of small businesses experienced a cybersecurity breach in 2013[1]. Airmic concludes that these figures suggest many organisations have fallen victim to non-material attacks, but remain unaware of them.

Financial implications

Depending on both the nature of the organisation and the attack, the damage inflicted can include any, several, or all of the following: loss of revenue, loss of management time in dealing with the attack, costs of notifying customers, compensation to customers for loss of sensitive data, losses suffered from contractual braches in connection with computer/network downtime, reputational damage, third parties' fees for lawyers and consultants to deal with the fallout, litigation, and fines or penalties for data loss.

The implications of an attack also depend on the type of data that needs to be protected: loss of IP data will be particularly damaging to, for instance, design or engineering businesses. Equally, financial services and health care businesses are typically more at risk as regards sensitive personal data stored on their computers and networks, and may be subject to fines if such data is compromised. It is therefore important for each organisation to identify the type of data it needs to protect.

Getting the right cover

Standard business' insurance cover will usually provide insufficient protection against cyber risk. This is because such policies typically exclude economic loss generally, as well as any losses caused specifically by data and privacy breaches. Similarly, property insurance policies tend to only cover tangible property, not data. Company insurance policies covering theft will also not usually cover third party property, such as customer/client data.

In order to protect against financial losses involved in a cyber attack, organisations will therefore need to consider obtaining a specific policy to cover the risks flowing from such an attack. While such policies have been available for around 20 years, they have only recently become more competitive financially as awareness and consequent demand for protection has increased.

Options available include first-party insurance policies that provide protection against the financial consequences of reputational, software, and data damage, as well as business interruption. Third party insurance policies are also available to cover losses relating to third parties' data, including security and privacy breaches, investigation costs, customer notification expenses and loss of third party data. The right policy will depend on an organisation's needs, including the data that requires protection. It is therefore important to fit the right policy to the risk. A wide range of cover is available, so organisations should consider the options available to their business with their broker.

[1] http://www.airmic.com/news-story/cyber-risk-companies-know-there-issue-still-do-not-fully-understand-it

continued overleaf

Fines and penalties for data loss: uninsurable?

One risk that is still difficult to insure against are fines related to personal data losses. This is because fines and penalties are usually specifically excluded from policies on public policy grounds. The rationale behind this is the principle of *ex turpi causa non oritur actio*, i.e. "from a dishonourable cause an action does not arise". In other words: a party should not be able to pass on liability for a punishment it has received in connection with its own illegal act. While the English courts have yet to hear a case on whether a fine related to data loss from a cyber-attack falls within the principle of *ex turpi causa*, the current leading authorities on this principle (Gray v Thames trains [2009] (manslaughter) and Safeway v Trigger [2011] (breaches of the Competition Act 1998) provide that similar fines are uninsurable. In addition, financial services firms are prohibited by the FCA from obtaining insurance to cover regulatory fines, which can include fines for data protection breaches, under General Principle 6.1 of the FCA Handbook.

The above is particularly significant given that a new Data Protection Regulation is likely to be approved in 2014, which will supersede the UK Data Protection Act ("DPA") currently in force. The Regulation will, if passed in its current form, provide for maximum fines of €100million or 5% of annual worldwide turnover, whichever is greater. This presents a significant increase from maximum fines levied under the DPA (up to a maximum of £500,000) and is a further reason for businesses to review their potential exposure in this area.

Contacts

Kari McCormick
Partner
+44(0)117 902 6620
kari.mccormick@burges-salmon.com

Rebecca Houlden
Associate
+44(0)117 307 6881
rebecca.houlden@burges-salmon.com

BRM0820 09 14