CYBERRISKS+LIABILITIES

July/August 2016

IN THIS ISSUE

Crendon Insurance Brokers

Cyber Security in Post-Brexit Britain

As Britain negotiates Brexit terms over the next two years, prudent businesses would do well to comply with the EU's General Data Protection Regulations (GDPR), since even if the government abandons those regulations, businesses must still abide by them if they want to do business or communicate with mainland Europe. Because of this, cyber security experts are predicting that Britain will either retain the GDPR, or adopt very similar, compatible measures.

The GDPR was supposed to come into force in May 2018, and was intended to help Britons regain control of their personal data as well as reduce the amount of red tape that international businesses must get through. One of the chief changes that the regulations will introduce is how personal data can and cannot be exported outside the EU. This requirement is what ensures that Britain can continue to conduct business with EU companies.

Complying with the most up-to-date cyber security regulations is more important now than ever—nearly 2 out of 5 IT professionals are concerned that Brexit will expose Britain to more cyber threats, according to industry research. And, it's easy to see why—from 2014 to 2015, the number of global security threats increased by 38 per cent and the theft of hard intellectual property increased by 56 per cent, according to PricewaterhouseCoopers. Unfortunately, there is currently a shortage of IT professionals in Britain to help shore up cyber security deficiencies, which means that they could worsen, depending on how Brexit negotiations develop.

However, until Britain finalises Brexit negotiations and decides to keep or nullify the GDPR, your company still needs to comply with the regulations. In addition to adhering to the GDPR, your company should at least implement these two practices to bolster your cyber security:

1. Provide all employees with comprehensive data security training to ensure that they know how to identify and manage cyber security threats—such as suspicious email requests and phishing scams.

2. Install security software on each computer in your organisation to detect and stop malicious malware and viruses. In addition, draft a non-work mobile device policy to minimise the potential of a data breach caused by an employee's device.

Recent Cyber Security News and Prosecutions

Cyber threats are the most significant risk for insurance buyers

Cyber threats represent the most significant concern to risk managers, according to a survey conducted by the Association of Insurance and Risk Managers in Industry and Commerce (Airmic). The survey found that the three most prominent areas of concern in regards to cyber threats were business interruptions, loss or theft of personal data, and reputational damage. Overall, the survey revealed that the average UK business owner's concerns are shifting away from physical risks toward more intangible perils—like cyber threats.

Employees working abroad are more likely to be victims of cyber crime

Kaspersky Lab, an international software security group, surveyed nearly 12,000 individuals from across the globe in order to measure how much pressure they experience from their employers to be available online when they work abroad. The study revealed that 3 out of 5 employees in senior roles said that they try to log on as soon as they can. However, that perceived pressure to remain connected places not only the employee at risk, but it places the employer's cyber security at risk as well, as nearly half of employees use unsecured public Wi-Fi networks—effectively sacrificing network security in exchange for logging on quickly. While 2 out of 5 employers expect that their employees will use strong security measures, employees are, in fact, more likely to be victims of cyber crime than of muggings while abroad.

Britons do not trust organisations with their personal information

A recent study conducted by the Information Commissioner's Office revealed that only 1 out of 4 of Britons trust businesses with their personal information. This has made Britons more proactive in protecting their personal information, as 70 per cent routinely check bank and credit card statements for irregular activity and more than 50 per cent have antivirus software installed on their computers. These figures should be treated as a wake-up call for UK businesses to adopt more robust and comprehensive cyber security schemes in order to regain the public's trust.

Learning From the Panama Papers

Published in April of this year, the Panama Papers—a collection of 11.5 million documents with information on the identities of shareholders and directors for more than 214,000 offshore companies—represent the largest data breach in history. The information contained in these documents is concerning, since an offshore company, sometimes called a 'tax haven', can help investors deposit large sums of tax-exempt money. The breach not only highlighted the importance and value of a robust cyber security system, but it also highlighted how cyber criminals are accessing more than just financial information.

The Panama Papers incident is a wake-up call for businesses, proving that cyber security and cyber cover are no longer optional—currently, investigators have still not identified how the information was moved. No matter whether your business is a multinational company or a local small to medium-sized enterprise (SME), no organisation is safe. However, SMEs are increasingly targeted by cyber criminals. In fact, in 2015, 74 per cent of small businesses suffered security breaches—a 20 per cent increase from 2014. These attacks cost the average SME between £75,000 and £311,000, according to the most recent government research. Since SMEs typically do not have robust cyber security, hackers often view them as unguarded back doors into larger, more lucrative organisations.

Fortunately, 80 per cent of all breaches can be stopped by implementing basic cyber security, according to industry experts. However, implementing a cyber security system with antivirus and anti-malware software is an incomplete defence. Your company needs to additionally safeguard itself with a comprehensive cyber cover policy. Unfortunately, 64 per cent of UK companies do not have any cyber insurance and 45 per cent of the companies that do are unsure if it is up to date, according to a study conducted by Mimecast.

The Panama Papers incident dissolved any ambiguity about the value of cyber security—no longer can those defences be seen as optional. No company is too large or small for cyber criminals. That is why it is critical that your company takes the necessary steps to protect itself with cyber cover and cyber security. For more information on how you can bolster your company's cyber protection, contact the experts at Crendon Insurance Brokers Ltd today.

74 PER CENT

of UK SMEs have suffered cyber security breaches within the last year.

Source: PricewaterhouseCoopers

Crendon Insurance Brokers Ltd

The CIB A Building, 146 Hagley Road

Edgbaston, Birmingham B16 9NX

0121 45 45 100

www.crendoninsurance.co.uk