CYBERRISKS+LIABILITIES

March/April 2016

IN THIS ISSUE

Crendon Insurance Brokers

GDPR Emphasises Accountability of Directors and Officers

In January, the European Commission published its draft of the EU General Data Protection Regulation (GDPR). The regulation is expected to strengthen data protection for EU citizens, set clear and modern rules for businesses, and bolster data protection legislation.

Under the new guidelines, the responsibility for reporting serious data breaches and bolstering an organisation's cyber security—including any damages that its customers may experience as a result of a breach—may be placed upon the shoulders of the organisation's directors and officers. Now that organisations will be responsible for reporting data breaches for the first time, directors and officers could be held responsible if they fail to bring their organisation in line with the forthcoming GDPR rules.

In order to ensure that directors and officers comply with the new regulation and provide adequate cyber protection for their organisation and customers, the GDPR has outlined a tiered fine structure:

- An organisation may be fined up to €10 million (roughly £8 million) or 2 per cent of its annual turnover—whichever is higher—for not properly filing and organising its records, for not notifying the supervising authority and data subject about a breach, and for not conducting impact assessments.
- An organisation may be fined up to €20 million (roughly £16 million) or 4 per cent of its annual turnover—whichever is higher—for violating the basic principles related to data security or for violating consumer consent.

The aim of these fines is to illustrate to directors and officers the importance of digital data compliance in their corporate efforts, system maintenance and responses to data breaches. Therefore, to minimise exposure to sizeable potential fines, organisations—regardless of size or industry—need to commit to implementing cyber security measures that effectively address potential cyber attacks in a prompt and thorough manner.

While the GDPR will not be formally adopted until 2018, your organisation should begin implementing the necessary cyber protections and educating your employees on cyber awareness as soon as possible.

Recent Cyber Security News and Prosecutions

Take advantage of the ICO's Data Protection Self-assessment Toolkit

The ICO recently released a comprehensive Data Protection Self-assessment Toolkit which can help your company remain compliant with the Data Protection Act and increase its cyber security. To use the free toolkit, visit www.ico.org.uk/for-organisations/improve-your-practices/data-protection-self-assessment-toolkit.

Cyber criminals are impersonating CEOs in costly new email scam

According to a recent report from the US Federal Bureau of Investigation (FBI), there has been a sharp increase in a new type of email crime known as CEO fraud. The email scam consists of a cyber criminal impersonating a chief executive through email and then directing an employee to wire money to an overseas bank account. On average, businesses lose about £83,500 from the scam, and, over the course of the last two years, the scam has collectively cost businesses across the globe more than £1.4 billion. In its ongoing investigation, the FBI has stated that the scam could be mitigated if companies provided their employees with proper cyber security training.

Record fine for company behind 46 million nuisance calls

Prodial Ltd, a lead generation firm, was fined £350,000 by the ICO for making more than 46 million automated nuisance calls over a period of several months. The firm was operating out of a residential property as well as hiding its identity, which made it difficult for people to report the specific details of the disturbances. More than 1,000 people called to inform the ICO about the calls. In its investigation, the ICO discovered evidence that the firm had been making nuisance calls to people who had not consented to receiving marketing calls. In addition, the firm was also selling people's personal details to claims management companies. According to the ICO, this was the worst case of cold calling that it has ever come across, which is why the firm was fined the record-breaking amount.

Cyber Attacks Targeting SMEs on the Rise

In 2015, cyber crime became the most common criminal offence in the United Kingdom, with about 8 million cases. Despite these findings, 44 per cent of UK business do not believe that they will be a target of a cyber attack, according to industry research, and 71 per cent of cyber attacks are aimed at businesses with fewer than 100 employees. The reason is simple—generally, SMEs think they are too small to be valuable to hackers and thus do not invest in cyber security or cyber awareness training.

The average cost to an SME for a security breach is between £75,000 and £311,000 according to government research. However, that does not include related costs such as rebuilding a destroyed reputation. And, when the EU's new GDPR comes into force in 2018, it could require companies to pay about £16 million or 4 per cent of their annual turnover for customer data breaches.

The good news is that nearly 80 per cent of breaches can be stopped by implementing basic cyber security, according to industry experts. Here are the five most common and dangerous cyber threats to SMEs:

1. **Ransomware:** A piece of malicious software that encrypts all of the data on a company's network and that can only be decrypted after paying cyber criminals a ransom—generally between £500 and £1,000.
2. **Hacking:** A cyber criminal will exploit an unpatched vulnerability within a company's security software to access its data. Generally, the criminals are interested in personally identifiable information (PII) on a company's customers—especially credit card information.
3. **Denial-of-service attack:** A company's website is maliciously overwhelmed by a high volume of data pushed to its servers, which temporarily or indefinitely interrupts services.
4. **Human error:** Information lost or distributed to the wrong person (accounted for 50 per cent of the worst breaches last year).
5. **CEO fraud:** A cyber criminal poses as a senior person within a company, either by hacking or 'spoofing' an email account, and convinces someone with financial authority to transfer money.

Understanding these risks is the first step to cyber security. The second is contacting **Crendon Insurance Brokers Ltd** for helpful guidance on cyber security and to discuss cyber security insurance.

Consumer Reaction to Corporate Cyber Attacks

Source: Deloitte Consumer Review

Crendon Insurance Brokers

0121 45 45 100

www.crendoninsurance.co.uk