CYBER RISKS & LIABILITIES_
NEWSLETTER

2nd Quarter 2015

IN THIS ISSUE

Cyber Cover to be Mandatory in a Decade

Cyber cover will become a business essential within ten years, according to the Association of British Insurers (ABI). Already cyber-attacks are a huge financial drain—annually they cost the UK economy an estimated £620 million. Yet, in spite of the growing threat of cyber-attacks to both the public and private sectors, only about 10 per cent of large businesses have any form of cyber cover, according to the ABI. This small figure reflects businesses' widespread ignorance of cyber cover's benefits, despite the general acknowledgement that cyber-attacks are one of businesses' biggest threats. This lack of cover can be quite costly—both financially and for a business' reputation.

Cyber-attacks can vary in severity and type—ranging from the theft of personal customer information to the theft of money or property. An average of 68 per cent of funds lost as a result of cyber-attacks are declared as unrecoverable, according to industry research. For that reason alone, businesses should fortify their defences with cyber cover. Here are five additional reasons why cyber cover will become a necessity for doing business within the next decade, according to the ABI:

1. Requiring only an Internet connection, cyber-attacks are one of the fastest growing forms of crime in the world.
2. Cyber threats are evolving alongside digital and wireless technology, which makes it difficult to develop matching defences.
3. With the expanding relevance of digital technology in day-to-day operations, businesses are increasingly dependent on IT for their success.
4. Depending on the severity of the cyber-attack, a business may be forced to close or to dramatically change how it operates.
5. The British insurance market is already able to offer businesses the innovative cyber protection that they need.

The threat of cyber-attacks has already become commonplace for businesses, regardless of size and industry. With the potential financial damage that cyber-attacks can inflict, financial experts warn that, depending on the size of the business, £1 billion in cyber cover may be required to adequately protect a large organisation. While that may seem like an exorbitant amount, the damage caused by cyber-attacks has far-reaching effects beyond just the immediate financial loss. Cyber-attacks can threaten your customers, whose private information may have been compromised, and damage the trust of both the public and your investors. Indeed, 79 per cent of investors said they would be discouraged from investing in a business that was hacked, according to a recent global survey conducted by professional services firm KPMG.

Insuring your business with cyber cover demonstrates that you are committed to safeguarding valuable data and ensuring compliance. Contact *Crendon Insurance Brokers Ltd* today to defend your business against the increasing risk of cyber-attacks.

Crendon Insurance Brokers

Take Advantage of Cyber Essentials

Cyber Essentials (CE), a government-backed and industry-supported scheme, provides organisations of all sizes and industries with free guidance to protect data from cyber threats. By following CE guidance, organisations can defend against a wide range of cyber threats through computers, tablets, smartphones, email and web servers.

The CE scheme focuses on controlling these five cyber security elements:

- **Secure configuration:** Installing cyber security measures in all new and existing computers and network devices
- **Boundary firewalls and Internet gateways:** Providing protection to safeguard against cyber threats
- **Access control and administrative privilege management:** Safeguarding user accounts and ensuring that privileged accounts are not misused
- **Patch management:** Installing updates for network devices
- **Malware protection:** Supplying malware protection and removal software for all computers and network devices

Depending on the success of an organisation's use of CE guidance, it can earn one of two levels of certification. The first level, **Cyber Essentials**, is awarded to organisations that complete a self-assessment questionnaire which is verified by an independent party. The second level, **Cyber Essentials Plus**, is awarded to organisations that have their systems independently assessed and have incorporated CE guidance into their information risk management schemes. Earning either certification allows organisations to advertise the fact that they adhere to a government-endorsed standard, boosting their credibility and bolstering their reputation.

By following CE guidance and earning a certification, organisations can demonstrate to their customers, investors and the public that they are committed to cyber security and the safeguarding of sensitive personal data. For more information, click here: www.cyberstreetwise.com/cyberessentials.

Changing jobs but keeping employer information is a criminal offence

A former Birmingham salesman for a communications service provider was fined £358,968.25 after he unlawfully downloaded customers' records onto memory sticks that he then removed from the workplace. He used those records to win business for his employer's competitors during and after his employment there. Failing to relinquish his employer's sensitive, proprietary information was not worth it—he was prosecuted under section 55 of the Data Protection Act 1998 because the use of personal information outside of its sanctioned domain, such as a previous employer, is a criminal offence. The amount of the fine only represents the judge's valuation of the communications service provider's lost business—not the attendant costs of lost reputation and breach of contract.

Individuals can be compensated for data breaches even when they suffered no financial loss

A landmark UK Court of Appeal case found that individuals may receive financial compensation for data protection breaches even when they suffered no financial loss. In the case, Google was accused of integrating tracking cookies into Apple's Safari browser to gather data on users' online behaviour that could then be used for targeted marketing. However, this integration violated Apple's policies and caused users to experience anxiety and distress. The UK Court of Appeal established that individuals could be awarded compensation for breaches of data protection laws even in cases where no financial damage took place. This decision leaves Google poised to owe millions to UK Safari users from September 2011 to February 2012.

Serious Fraud Office fined after mishandling evidence

The Serious Fraud Office was fined £180,000 after mistakenly sending the incorrect evidence in a major fraud, bribery and corruption investigation to a witness in that same case. Contained within the materials was personal data on 6,000 individuals—some of whom are well-known public figures. The error occurred when the Serious Fraud Office failed to properly train and supervise the individual responsible for packaging and mailing the evidential materials.

CYBERRISKS&LIABILITIES_
NEWSLETTER

Crendon Insurance Brokers Ltd
www.crendoninsurance.co.uk
0121 45 45 100
enquiries@crendoninsurance.co.uk