CYBERRISKS+LIABILITIES

4th Quarter 2015

IN THIS ISSUE

Crendon Insurance Brokers

Cyber Security: From IT to the C-Suite

A 2015 government survey revealed that an estimated 90 per cent of large organisations and 74 per cent of SMEs had suffered a cyber attack within the past year. The average cost of an attack varied widely—from £115,000 to £1.46 million—depending on the size of the organisation and the nature of the attack.

Despite the frequency of cyber attacks and the damage they can inflict, more than one-fifth of SMEs do not believe that they are a target for cyber criminals. However, those SMEs are seriously mistaken—while SMEs generally possess far more data than the average person, they often do not have any considerable preventative measures in place to protect themselves against cyber threats, and, thus, are particularly attractive targets to cyber thieves.

As cyber crime is generally a faceless and almost phantom-like risk, knowing how to effectively address the potential cyber hazards that your organisation could be exposed to can be difficult. However, even the most effective and comprehensive cyber security schemes are rendered moot if they are not implemented throughout the organisation—from apprentices all the way up to the C-Suite. Therefore, to help prioritise cyber protection throughout your organisation, rely on these resources and pieces of guidance:

1. **Be Cyber Streetwise:** A cross-government campaign which provides SMEs with cyber security guidance and resources. (www.cyberstreetwise.com)
2. **Cyber Essentials:** A government scheme which outlines the basic cyber protections that should be taken by your organisation. Upon completing the requirements, your organisation becomes eligible to apply for government accreditation. (www.cyber-essentials-scheme.co.uk)
3. **Mobile device guidelines:** One-third of all reported UK cyber security incidents were due to mobile devices being exploited. Develop guidelines on whether employees can use their personal mobile devices and what precautions they need to take in order to safely use their devices.
4. **Staff training:** In the past year, three-fourths of security breaches were the result of human error. For that reason, properly train your staff on identifying and managing cyber threats. The government offers bespoke courses which can be found at www.nationalarchives.gov.uk/sme.

Recent Cyber Security News and Prosecutions

TalkTalk hit by significant cyber attack

TalkTalk, a phone and broadband provider for more than 4 million Britons, was hacked this October. The cyber criminals were able to acquire the personal information—such as names and addresses, birthdates, email addresses, and credit card and bank details—of nearly 1 million customers.

Personal information is usually traded or sold online to other criminals, who use it for email and phone scams. Pensioners over the age of 65 are especially being targeted, as they are viewed as being more vulnerable.

Lead generation company fined £120,000 for making automated nuisance calls

Oxygen Ltd, a South Wales lead generation company, was fined £120,000 after making more than 1 million unsolicited automated marketing calls. The calls resulted in at least 214 complaints to the Information Commissioner's Office (ICO) and prompted an investigation. Upon completing its investigation, the ICO determined that, due to the nature of the calls, the company was in violation of the Privacy and Electronic Communication Regulations.

Crown Prosecution Service fined £200,000 for failing to secure recorded police interviews

The Crown Prosecution Service was fined £200,000 after laptops containing videos of police interviews pertaining to 31 investigations dealing with violent or sexual crimes were stolen from a private film studio. A Manchester-based film company had possession of the laptops in order to edit the videos to be used in forthcoming criminal proceedings. In its investigation, the ICO found that the company had insufficient building security and failed to encrypt the information that was on the two laptops. While the police were able to recover the two laptops and none of the information had been tampered with, the ICO ruled that the Crown Prosecution Service was negligent in ensuring the safety of the information contained on the two laptops.

In 2014, **45 per cent of small businesses** had their digital systems infected by viruses or other malicious software. The average cost of a security breach is between **£65,000 and £115,000.**

SOURCE: SME Insider

Cyber Crime is the Most Common Criminal Offence

Cyber crime—which includes the theft of personal information, online harassment or bullying, and disruption of trade—was recognised as the United Kingdom's most common criminal offence by the Office for National Statistics. Within the last year alone, there were nearly 8 million cases of cyber crime—costing the UK economy more than an estimated £16 billion.

Between May and August of this year, an estimated 2.5 million computers were hacked. As a result, cyber criminals were able to gain access to home addresses, credit card numbers, bank account details and other personal information. To protect your organisation from cyber criminals, keep in mind the following three pieces of advice:

4. **Install security software:** Security software provides you with multiple layers of defence:
    - **Firewalls** control who and what can communicate with your computer online—allowing communications that it knows are safe and blocking those that could be potentially hazardous.
    - **Antivirus software** monitors all online activities—including email and Web browsing—and protects your computer from viruses, worms, Trojan horses and other types of malicious programs. Included in some antivirus software programs is antispyware, which can protect from spyware and potentially unwanted programs, such as adware.
5. **Choose a strong password:** Create a password that is at least eight characters long and is a mix of lower and upper case letters, numbers and symbols. Avoid using things like birthdays or other important dates, the name of loved ones or pets as well as other personal details such as your favourite sports team. Additionally, you should choose a new password every 90 days.
6. **Encrypt your hard drive: E**ncryption translates your data into a code that only you (and anyone you choose to share it with) would be able to understand.

To find out more about how you can protect your information from cyber criminals, contact Crendon Insurance Brokers Ltd today.

Crendon Insurance Brokers Ltd

The CIBA Building, 146 Hagley Road

Edgbaston, Birmingham B16 9NX

0121 45 45 100

www.crendoninsurance.co.uk