CYBER RISKS & LIABILITIES_
NEWSLETTER

1st Quarter 2015

IN THIS ISSUE

Minding the Gap in Your Cyber Cover

The frequency and severity of cyber-attacks have been steadily growing in the United Kingdom, and even if you believe that your company will not be a target or that your cyber protection is adequate, the extra cover of a cyber-policy would be extremely beneficial. Currently, only 13 per cent of UK firms are covered by some form of cyber security insurance, according to a February 2015 report by the not-for-profit security group Corporate Executive Programme.

Many organisations either opt to add cyber cover to existing commercial insurance policies, or they set aside specific funds for potential cyber incidents. However, if you approach cyber-attacks in this piecemeal manner, there could be dangerous gaps in your cover, leaving your firm underinsured.

New cyber scams are developing at a rapid pace, eclipsing many current defensive practices as they expand their breadth and capabilities. This means that any current gaps in your cyber cover are likely to grow as regulatory and legislative changes fail to keep up with the ever-evolving cyber scams. Maintaining up-to-date, effective cyber cover requires constant vigilance against current and impending cyber-attacks.

Cyber-attacks pose a threat to your company in part because they have far-reaching effects that can manifest themselves in a number of ways, including the following:

- Loss, damage or theft of digital assets, such as software
- Interruption in business caused by attacks that target customer access or services
- Cyber extortion of stolen files, data and/or other sensitive material
- Damage to the firm's reputation brought on by the loss of personal data and intellectual property infringement

However, the effects of cyber-attacks are rarely confined to just your firm—your clients and contacts are impacted as well. You are responsible for contacting and informing clients of a breach, as well as reimbursing them for any personal data that was lost or stolen. Claims could be brought against your firm for breach of privacy, which would mean that any subsequent investigation costs, fines, damages and compensation would all be your financial responsibility.

The digital landscape is growing every day—certain technology that was considered commonplace years ago may be obsolete today. This forces your company to adapt and provide agile solutions constantly in order to protect your digital assets. Contact the insurance professionals at **Crendon Insurance Brokers Ltd** for more information on plugging the dangerous gaps in your cyber cover.

Crendon Insurance Brokers

Cyber Security Boost for UK Firms

In January, the government announced new measures that it hopes will help UK businesses when facing future cyber security challenges. The announcement details several new, free resources designed to help businesses recognise and combat cyber threats, strengthen the government's National Cyber Security Programme and further the work done by Cyber Growth Partnership in order to expand the cyber security sector in the United Kingdom. Included in the announcement are the following measures to help businesses:

- A major update to the 10 Steps to Cyber Security guide that more clearly outlines the cyber risks that businesses face and the most effective methods of mitigating those risks—find the guide here: https://www.gov.uk/government/publications/10-steps-to-cyber-security-advice-sheets
- The publication of a new report from the Government Communication Headquarters, detailing the common cyber attacks used against businesses across all industries and how to stop them
- Improved cyber security information and advice for businesses through the government's Business Support Helpline, the Business Growth Service and www.greatbusiness.gov.uk
- New research from the Department for Business, Innovation and Skills, which shows how top UK companies are improving their cyber defences

With these new measures, the government is cementing the importance of supplying businesses with the knowledge and tools to properly defend against cyber-attacks. If your company does not have an established cyber security programme, you are leaving yourself exposed to potential attacks. The message from the government is clear: Cyber security can no longer be treated as an addendum—it is a necessity. For more detailed information on these new government resources, click here: https://www.gov.uk/government/news/cyber-security-boost-for-uk-firms.

Boiler insurance firm targeted pensioners to sell unnecessary cover

A Croydon boiler insurance firm was fined £90,000 for continually making nuisance calls to elderly individuals. Employees were improperly trained on the Privacy and Electronic Communications Regulations, and they were discovered to be targeting individuals who had registered with the Telephone Preference Service (TPS), the free service enabling people to opt out of receiving unsolicited sales and marketing calls. This resulted in the firm's employees selling boiler insurance to multiple individuals who did not need it. Between 1 July 2013 and 31 March 2014, the firm was the subject of 214 complaints to both the Information Commissioners Office and the Telephone Preference Service.

Festival organisers send mass unsolicited marketing texts

A Manchester festival event planner was fined £70,000 after sending unsolicited marketing text messages to 70,000 individuals who had purchased tickets to the previous year's music festival. The company was not in compliance with the Privacy and Electronic Communications Regulations due to sending spam text messages that were labelled as being sent from 'Mum'. The Information Commissioners Office received 76 complaints from individuals who were distressed by the invasion of privacy as well as the content of the message itself.

Pharmacist fined for unlawfully accessing non-patient medical records

A 50-year-old pharmacist was fined £10,000 and ordered to pay a victim surcharge of £100 as well as £608.30 in prosecution costs after he unlawfully accessed the medical records of family members, work colleagues and local health professionals. The pharmacist was responsible for handling medication reviews for patients with dementia and other mental health issues in local residential care homes. However, the pharmacist used his security pass to access unrelated medical records as well. The breach in security was caught during a routine audit by one of the surgeries where he worked.

CYBERRISKS&LIABILITIES_
NEWSLETTER

Crendon Insurance Brokers Ltd
11 Greenfield Crescent
Birmingham, West Midlands, B15 3AU
0121 45 45 100
www.crendoninsurance.co.uk