CYBERRISKS+LIABILITIES

May/June 2016

IN THIS ISSUE

Crendon Insurance Brokers

Half of UK Businesses Are Unprepared for Cyber Attacks

In the last 12 months, two-thirds of large businesses (those with at least 250 employees) experienced at least one cyber-attack or breach, according to the government's Cyber Security Breaches Survey, released in May. Of those businesses, one-fourth experienced a breach at least monthly.

While about one-third of these incidents involved cyber criminals impersonating the organisations and stealing money (ranging from an average of several thousand pounds to a high of £3 million), the majority involved viruses, spyware or malware that were used to steal data or disrupt systems. If businesses are not adequately protected against these cyber threats, they leave their data—including financial and private customer information, bank account numbers and access to social media accounts—vulnerable to cyber criminals.

Yet, while most of these threats could have been prevented using free resources from the government's Cyber Essentials scheme, only half of all UK businesses have taken any recommended steps to address gaps in their cyber security. And, that is a problem made worse by the finding that only 27 per cent of UK businesses consider cyber security training to be an effective method to prevent attacks, according to research from CompTIA, a global IT industry trade association. However, training is absolutely necessary, since 60 per cent of all security breaches last year were the result of human error, general carelessness or IT staff failures.

To help shore up cyber security for all UK businesses, the government will invest £1.9 billion over the course of the next five years to prevent and address cyber-crime. As part of this effort, the government will also develop a new National Cyber Security Centre, which will launch in autumn 2016 and provide UK businesses with cyber security guidance. Also, a new national cyber security strategy, which will outline proposals to improve cyber security, will be published sometime later this year.

In the meantime, there are three simple practices that your business—regardless of size—can implement to bolster your cyber security:

1. Provide all employees with training on how to identify and manage cyber security threats.
2. Implement the guidance outlined in Cyber Essentials.
3. Complete the 10 Steps to Cyber Security, if you are a large business.

Recent Cyber Security News and Prosecutions

Cyber cover may be useless if your employees hack your data

Legal experts are warning that businesses' cyber cover may be invalidated by insurers if employees hack company data. Most standard cyber and data protection policies only provide cover for first- and third-party liabilities, which means that your company may not be covered for incidents that result from deliberate or criminal behaviour by an employee. For that reason, contact **Crendon Insurance Brokers Ltd** to understand the limits of your cyber liability policy.

TalkTalk's profits halved after suffering from cyber attack

This past October, TalkTalk revealed that cyber criminals had gained access to the private information of 1.2 million of its customers. The security breach has cost the company £83 million—£43 million of which is directly related to the cyber-attack. As a result of the breach, the company's profits have been more than halved. However, TalkTalk has reported that it has been recovering quickly as a result of focusing on rebuilding its relationship with its customers.

EU campaign firm fined for sending spam texts

Better for the Country Ltd (also known as Leave.EU) was fined £50,000 by the Information Commissioner's Office (ICO) after it was discovered that it had sent more than 500,000 text messages without recipients' consent. The company was attempting to convince people to support the campaign to leave the EU through text messages, but it did so without following the ICO's rules about sending marketing messages. In its investigation, the ICO discovered that the company had obtained the phone numbers through a third-party supplier. While the numbers were originally obtained from people that had given their consent to receive information on a variety of subjects, they had not consented to receive information on EU politics.

UK Businesses Have Been Increasingly Plagued by Ransomware

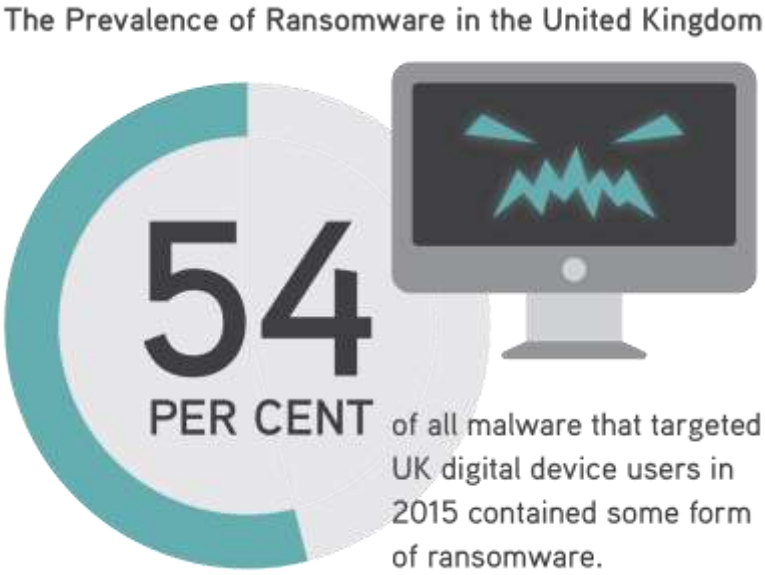
The number of businesses across the globe that reported being the target of ransomware scams rose by almost 170 per cent in 2015, according to a report from Intel Security. And, by some reports, the United Kingdom is getting hit the hardest—UK businesses are among some of the most targeted in Europe, according to network security firm, FireEye. Indeed, the United Kingdom received nearly 1 in 10 of all ransomware-infected emails globally in 2015, according to security firm Bitdefender.

Ransomware is a type of malware that uses encryption to lock users out of digital files until they pay a monetary ransom for a 'key'. Unable to access vital information, businesses are increasingly opting to pay the online extortionists rather than report the crime, according to the Financial Times. But, there is no guarantee that access to the files will be granted once the ransom has been paid. Therefore, the government is encouraging users to report ransomware attacks to Action Fraud by calling 0300 123 2040.

Although it is nearly impossible to plug all the potential gaps in your business' cyber security, you can still make it difficult for cyber criminals to access your information. The most beneficial practice that your business can implement is to establish a robust cyber security programme. While your business' cyber security programme will be unique to your business, be sure to include the following components to protect against ransomware:

- Install security software and ensure it is always up to date to protect against new threats.
- Ensure that all the software on your system is current, including browsers, the operating system and any plug-ins. One of the most common ransomware exposures is a software vulnerability.

For more information on how to safeguard your business from cyber threats, contact **Crendon Insurance Brokers Ltd** today.



Source: Bitdefender

Crendon Insurance Brokers Ltd

0121 45 45 100

www.crendoninsurance.co.uk