CYBER RISKS & LIABILITIES_
NEWSLETTER

Brought to You by Crendon Insurance Brokers Limited

June / July 2014

IN THIS ISSUE

Is Your Website Secure?

In the wake of several high-profile cyber security scandals and the widespread Heartbleed security bug, website security is more important than ever. And the stakes have never been higher—according to the 2013 Information Security Breaches Survey, over 78 per cent of large organisations and over 63 per cent of small businesses were attacked by an unauthorised outsider in the past year.

Without a concerted effort to safeguard your business' website, you risk losing money due to relentless cyber attacks. Because hackers are constantly searching for new website vulnerabilities and engineering new viruses, website security should be a round-the-clock concern—the threat will never ebb. The consequences of weakening your stance on website security, even for a second, can be disastrous: loss of revenue, damage to credibility, legal liability and broken customer trust.

Web servers, which host the data and other content available to your customers on the Internet, are the most targeted and attacked components of a company's network. Some specific security threats to Web servers include the following:

- Cyber criminals may exploit software bugs in the Web server.
- Attackers can disable a network by flooding it with information.
- Hackers may secretly read or modify sensitive information on the Web server.
- Criminals could gain unauthorised access to resources elsewhere in your business' network following a successful attack on the Web server.

To avoid similar threats to your website's security, follow the steps listed below:

1. Develop and implement a data breach response plan.
2. Ensure that the Web server operating systems and applications meet your organisation's security requirements.
3. Publish only appropriate information.
4. Prevent unauthorised access or modification on your site.
5. Protect and monitor Web security at all times.

Rely on Crendon Insurance Brokers Ltd for expert, timely guidance on cyber security.

Crendon Insurance Brokers

Remind Your Employees to Be Wary of Online Scams

As the world's football fans are engulfed by World Cup fever this summer, online scammers are hoping to capitalise on the sporting event's widespread popularity by sending a spate of bogus Fédération Internationale de Football Association (FIFA) emails designed to con the recipients out of their money and personal information, or gain access to their computers. If employees fall for these sham emails, they risk infecting your business' computer network by inadvertently granting hackers unauthorised access.

The scams, purporting to represent FIFA, rely on a number of tricks to persuade supposed 'lottery winners' to fork over money in order to receive their huge cash prize. Another tactic is making delivery of the fake prize contingent on recipients divulging personal information. Scammers then use that personal information to commit identity fraud—draining bank accounts and opening fraudulent credit cards.

Due to the barrage of 2014 World Cup promotional material, it can be difficult to separate the real from the fake. To counter this confusion, urge your employees to follow the age-old adage that if something is too good to be true, it probably is. Tell them to remember that if they did not enter a lottery, they could not have won it. Because some scam emails are sent in Portuguese to baffle the recipients into clicking on a malicious link, employees should never click anything unfamiliar.

These and other online scams often take the form of spam, or unsolicited electronic messages. Through spam, scammers can also initiate installation of spyware, which is software installed on a computer without the user's permission.

As a general rule, caution your employees to be suspicious when receiving any unsolicited or unexpected emails, and exercise extreme caution when clicking on links in suspicious emails.

Merseyside council sends records to wrong address

The Wirral Borough Council in Merseyside breached the Data Protection Act by accidentally sending social services records to the wrong address on two occasions in February and April 2013. The records contained sensitive personal information relating to two local families, including details of a criminal offence committed by one of the family members. An Information Commissioner's Office (ICO) investigation found that the council had neither mandatory data protection training for staff nor sufficient checks in place to make sure records were being sent to the correct address. The council signed an undertaking to improve practices, which includes ensuring that all staff completes data protection training.

Kent Police fined £100,000

The ICO fined Kent Police a whopping £100,000 for abandoning confidential information, including copies of police interview tapes, in the basement of its former police station. The highly sensitive information included records stretching back to the 1980s, and is thought to have been left in the basement when Kent Police vacated the site in 2009. A police officer discovered the records when visiting a business owner about an unrelated matter on 27 November 2012. The business owner explained how he found the tapes in the basement of the old police station after purchasing the building two months before. He was planning to watch the tapes for entertainment. The ICO's investigation concluded that the Kent Police had no guidance or procedures to safely remove sensitive information from their premises.

Private investigator slapped with £89,000 penalty

An unscrupulous private investigator was ordered to pay £20,000 in fines and prosecution costs and a confiscation order of £69,000 for relying on illegal methods to obtain personal information. The investigator's Middlesex company worked on behalf of clients to trace individuals, primarily for the purpose of debt recovery. Employees of the company routinely tricked organisations such as utility companies and GP surgeries into revealing personal data, often by claiming to be the individuals they were trying to trace. A subsequent ICO investigation estimated there were almost 2,000 separate breaches of the Data Protection Act between 1 April 2009 and 12 May 2010.

CYBERRISKS&LIABILITIES_
NEWSLETTER

Crendon Insurance Brokers Ltd
11 Greenfield Crescent
Birmingham, West Midlands, B15 3AU
0121 454 5100
www.crendoninsurance.co.uk