CYBERRISKS+LIABILITIES

3rd Quarter 2015

IN THIS ISSUE

Crendon Insurance Brokers

10 Government Tips for Cyber Security

In the 2015 Information Security Breaches Survey, the Department for Business, Innovation & Skills reported that 90 per cent of large organisations had experienced a cyber breach in 2014. The worst security breach of the year cost each company, on average, between £1.46 million and £3.14 million. Small businesses did not fare much better—74 per cent experienced a security breach in 2014, costing on average between £75,000 and £311,000 for their worst breach.

Regardless of the size of your organisation, cyber security provides invaluable protection. To help your company develop thorough cyber risk management, the government has laid out 10 beneficial tips.

1. Keep directors and officers informed about what preventative measures your company has taken to manage cyber-attacks. This may include reports detailing current and new initiatives.
2. Produce a user security policy that covers the acceptable use of your organisation's systems. Additionally, establish a general staff training programme on how to manage cyber risks.
3. Develop a mobile working policy.
4. Apply any security patches as soon as they become available, and ensure that the configuration of all information communications technology (ICT) systems is secure and maintained. Additionally, create a system inventory and define a baseline for all ICT devices.
5. Create a policy for all removable media—such as thumb drives and external hard drives. Include the requirement that all media be scanned for malware before importing it on the corporate system.
6. Establish online and cyber account manager processes, and monitor user activity for potentially hazardous or malicious behaviour.
7. Establish a cyber-incident response and disaster recovery policy. This should include testing incident management plans.
8. Establish a general employee monitoring strategy to identify potential malware and hazardous online behaviour.
9. Establish anti-malware defences to protect against hackers and viruses.
10. Protect your organisation's computer and online networks against external and internal attacks by managing the network perimeter and filtering out unauthorised access and malicious content.

Through the implementation of these 10 tips, your organisation should be able to effectively shore up any deficiencies in your cyber risk management scheme.

Recent Cyber Security News and Prosecutions

Hackers target Samsung Galaxy devices

A vulnerability in Samsung's digital shortcut keyboard program (which is pre-loaded on all Samsung phones) can provide hackers with easy access to users' information. Once a hacker has gained access, he or she can look through the phone's camera, listen through the microphone, read incoming and outgoing texts, and even install apps. Unfortunately, until Samsung fixes the problem, there is nothing users can do to protect themselves. Even if users do not use the keyboard, their phones still will make the request for an automatic update to the program—which provides the opportunity for hackers to access the phone. Until a solution is presented, Samsung Galaxy users are urged to stay away from unsecured Wi-Fi networks to minimise exposure to hackers looking to exploit the vulnerability.

'Stagefright' bug threatens all Android phones

'Stagefright', a computer bug, is being used to exploit a vulnerability in the operating system of 95 per cent of all Android phones. In order for a cyber criminal to gain access to a device, he or she often needs the victim to take some action, like clicking on a link in an email. However, what makes 'Stagefright' so dangerous is that a hacker only needs the user's phone number to gain access to his or her private information.

The bug gets its name from an Android media playback tool called Stagefright. Stagefright 'previews' multimedia messages (MMS) to reduce load times for users. So, a hacker can just embed the bug into a video file and send it to someone in an MMS. Even if the recipient does not watch the video, Stagefright will still preview it. Once a phone has been infected, the hacker can access photos, Bluetooth radios and other personal information. Currently, patches are in development to fix the massive vulnerability.

The Money Shop hit with huge fine over unsecured data

The Money Shop, a payday lender, was fined a civil monetary penalty of £180,000 after the company lost two computer servers, which contained the personal information of several thousand customers, during transport to a new location. Neither server was properly encrypted to protect the confidential information. In its investigation, the ISO found that the company regularly exposed sensitive customer information by not encrypting it, along with using unsecured transport methods for its servers.

Cyber Security Grants Up for Grabs

Despite 2015 government research showing that SMEs are risking one-third of their revenue by falling for some of the common misconceptions around cyber security, two-thirds of SMEs do not actually consider themselves vulnerable to cyber-attacks. To address the considerable deficiencies present in SME cyber security, the government has launched the Cyber Security Innovation Voucher scheme. If approved, a SME could receive up to £5,000 that can be used to obtain specialist advice on how to improve its cyber security and help it acquire Cyber Essentials certification. A Cyber Essentials certification can be beneficial for your business as it is a requirement for all government contracts.

In order for your business to qualify for the Cyber Security Innovation Voucher, it must meet these four criteria.

1. You must be starting up or running a micro, small or medium-sized UK business.
2. You can't have worked with a cyber-specialist before.
3. You must need help with something that is a real challenge for your business and not just a small improvement or change.
4. You can't have received an Innovation Voucher from Innovate UK or the Technology Strategy Board before.

The scheme will award Innovation Vouchers once every three months to eligible SMEs, which will be chosen at random. To apply, your business must register online with _Connect at www.projects.innovateuk.org. After registering, you will need to answer a few short questions about how the grant would impact your business.

For more information about the Cyber Security Innovation Voucher scheme, including how to apply, visit: www.interact.innovateuk.org/competition-display-page/-/asset_publisher/RqEt2AKmEBhi/content/cyber-security-innovation-vouchers-round-13

Crendon Insurance Brokers Ltd

0121 45 45 100

www.crendoninsurance.co.uk

enquiries@crendoninsurance.co.uk