CYBER RISKS & LIABILITIES_
NEWSLETTER

Provided by Crendon Insurance Brokers

August / September 2014

IN THIS ISSUE

Protect Your Email From Prying Eyes

Email has a number of benefits that far outweigh the costs—it's cheap, instantaneous and easy to use. But email can be a huge liability for businesses: It is not inherently secure, meaning anything you or your employees send via email could be intercepted. For normal, everyday email communication, this is no problem. But for emails containing sensitive information such as passwords and customer data, lax email security is a persistent problem, which can generate steep fines and tarnish a business' hard-fought reputation. To protect your business' email from prying eyes on the Internet, follow these top tips:

- **Set up a spam email filter.** Email is the primary method for spreading viruses and malware. Everyone gets those messages promising £1,000,000 or a new gadget under the condition that you disclose your National Insurance number or bank information. To avoid receiving these dubious messages in the first place, use email-filtering services provided by your email service, hosting provider or cloud provider. Regularly review and update filters to ensure you always have the most up-to-date protection.
- **Protect sensitive information sent via email.** Business email often includes sensitive information. Whether it is company information that could harm your business or something personal, it is imperative that you protect that information and ensure that only authorised recipients can see it. Consider encrypting your emails, which is the process of converting data into an unreadable format so that only those with the encryption key can read it. Cloud services also offer secure Web-enabled drop boxes that allow secure data transfer.
- **Implement a sensible email retention policy.** Keeping old, unnecessary emails clutters your inbox and increases your security risk. You should implement basic controls to limit email retention—if an email contains sensitive information, the longer you keep it, the more your risk grows. Consider mandatory archiving at a chosen retention cycle end date and automatic permanent email removal after another set point, such as after 180-360 days in archives.
- **Develop an email usage policy.** Your email policy is important for setting employee expectations and developing company-wide standards. Key areas to address in your policy include what the company email system should and should not be used for, and what data is allowed to be transmitted. Other policy areas should address retention, privacy and acceptable use.
- **Train your employees in responsible email usage.** Technology alone cannot make a business secure—train your employees to identify risks associated with email use, how and when to use email appropriate to their work and when to seek professional assistance. Offer security awareness training for all new employees and refresher courses every year.

Crendon Insurance Brokers

Data Theft by Departing Employees

Data theft by departing employees is costing UK businesses millions of pounds, according to research by London-based law firm EMW Law LLP. The number of High Court cases related to the theft of confidential company information spiked more than 250 per cent from 2010 to 2012, with the average legal bill for settling such cases costing about £30,000, not including the actual cost of data loss.

What is motivating these sticky-fingered employees? For one thing, data theft has become extremely easy as more and more information can be compressed into smaller and smaller quantities. Disgruntled employees, after being sacked, are making copies of company databases and other critical information to give to new employers, to set up their own businesses or to sell to marketing firms. It only takes seconds to copy a damaging amount of data to a cloud-based storage service, which employees can later access from outside the company.

Unfettered remote access to company systems also enables employees' data theft, allowing them to access sensitive information and easily copy it to their home computers. Although the door is wide open for employees to steal data, businesses lack the basic controls to prevent such thefts. Three-quarters of employers surveyed by OnePoll in April 2013 admitted to not having any enforceable systems to prevent employees from gaining unauthorised access.

Smaller companies are more likely to be vulnerable due to their lack of resources. The most commonly affected small companies are financial services firms, estate agents and recruitment firms.

To prevent an embarrassing internal data breach and whopping legal bills, proactively monitor all activity across your business' entire IT network. Rather than relying on reactive security defences, use a dedicated monitoring system to identify data breaches before they escalate. Contact Crendon Insurance Brokers Ltd for a wealth of resources on securing your business' data.

Scottish businesses prime targets of cyber-crime gangs

Russian cyber-crime gangs are increasingly targeting Scottish businesses, according to a BBC investigation. Figures from Police Scotland show a surge in cyber-crimes at the end of 2013, with businesses as the prime target. Businesses of varying sizes across a wide range of sectors have been targeted, but most targets are financial and agricultural businesses with up to 200 employees. Police are stressing the long-term financial and reputational damage of cyber-crime and recommending that businesses invest in additional cyber security measures. The police urge any businesses that were victims of cyber-attacks to come forward—although few commercial attacks are reported due to fears of reputational damage, only by contacting the authorities can the criminals be caught.

Northern Ireland prison service warned

The Information Commissioner's Office (ICO), the United Kingdom's data protection regulator, has warned the prison service in Northern Ireland to bolster security after a filing cabinet containing Maze Prison records was unwittingly sold at auction. The incident occurred in 2004 when a cabinet that officials thought was empty was sold at a public auction. In fact, the cabinet contained files about the prison's closure, including details on staff and a high-profile prisoner. The Northern Ireland Office, which was responsible for prisons at that time, retrieved the sensitive information but failed to report the matter to the ICO. The ICO became aware of the breach when a similar incident occurred in 2012.

Manager who sold customer details to claims company fined

A 29-year-old former manager at a hire car company in Merseyside was fined £500 and ordered to pay a £50 victim surcharge in addition to £264 in prosecution costs after stealing the records of almost 2,000 customers and selling them to a claims management company. The rental company alerted the ICO after its cyber security system showed an irregularity. The ICO then raided the Liverpool-based claims management company, finding a stockpile of records all related to customers who had been involved in recent accidents. The claims management company currently remains under investigation by the ICO.

CYBERRISKS&LIABILITIES_
NEWSLETTER

Crendon Insurance Brokers Ltd

www.crendoninsurance.co.uk

11 Greenfield Crescent

Birmingham, West Midlands, B15 3AU

0121 45 45 100

enquiries@crendoninsurance.co.uk