CYBERRISKS&LIABILITIES_

Cyber Security Tips for Small Businesses

High-profile cyber-attacks on companies such as Sony have raised awareness of the growing threat of cyber crime. Recent surveys conducted by Symantec and other cyber-security organisations suggest that many small business owners are still operating under a false sense of security.

The statistics of these studies are grim: The vast majority of small businesses lack a formal Internet security policy for employees, and only about half have even rudimentary cyber security measures in place. Furthermore, only about a quarter of small business owners have had an outside party test their computer systems to ensure they are hacker proof, and nearly 40 per cent do not have their data backed up in more than one location.

Don't Equate Small with Safe
Despite significant cyber security exposures, 85 per cent of small business owners believe their company is safe from hackers, viruses, malware and data breaches. This disconnect is largely due to the widespread, albeit mistaken, belief that small businesses are unlikely targets for cyber attacks. In reality, data thieves are simply looking for the path of least resistance. Symantec's study found that 40 per cent of attacks are against organisations with fewer than 500 employees.

Where is the Attack Coming From?
Outside sources like hackers aren't the only way your company can be attacked—often, smaller companies have a family-like atmosphere and put too much trust in their employees. This can lead to complacency, which is exactly what a disgruntled or recently sacked employee needs to execute an attack on the business. Other attacks could come from failures in technology and processes.

According to the 2013 Information Security Breaches Survey released by the Department for Business, Innovation and Skills (BIS), 65 per cent of small businesses were attacked by an unauthorised outsider in the past year. The survey also found that nearly 50 per cent of the worst breaches were caused by inadvertent human error.

Attacks Could Destroy Your Business
As large companies continue to get serious about data security, small businesses are becoming increasingly attractive targets—and the results are often devastating for small business owners.

The cost of an individual security breach can vary, depending on the type of data compromised and the amount of data taken. However, cyber attacks can cost hundreds of thousands of pounds, and most small businesses don't have that kind of money lying around. Businesses are required to keep personal and sensitive data safe in order to comply with the Data Protection Act, and violations of the Act can result in substantial sanctions from the Information Commissioner. However, many businesses continue to put off making necessary improvements to their cyber security protocols until it is too late because they fear the costs of security would be prohibitive.

10 Ways to Prevent Cyber Attacks
The BIS survey found that 83 per cent of small businesses believe security is a high priority, but that many find it difficult to keep up with the constantly changing risks and to know what actions to take to mitigate those risks. Even if you don't currently have the resources to bring in an outside expert to test your computer systems and make security recommendations, there are simple, economical steps you can take to reduce your risk of falling victim to a costly cyber attack.

1. Train employees in cyber security principles.
2. Install, use and regularly update antivirus and antispyware software on every computer used in

CIAT Insurance Services
Administered by McFarland Finn Ltd

your business.

3. Use a firewall for your internet connection.
4. Download and install software updates for your operating systems and applications as they become available.
5. Make back-up copies of important business data and information.
6. Control physical access to your computers and network components.
7. Secure your Wi-Fi networks. If you have a Wi-Fi network for your workplace, make sure it is secure and hidden.
8. Require password-protected individual user accounts for each employee.
9. Limit employee access to data and information, and limit authority to install software.
10. Regularly change passwords.

Your Emerging Technology Partner
A data breach could cripple your small business, costing you thousands or millions of pounds in lost sales, damages or sanctions. Contact CIEEM Insurance Services today. We have the tools necessary to ensure you have the proper cover to protect your company against losses from cyber attacks.