RISK INSIGHTS

Crendon Insurance Brokers

Cyber Security for Your Small Business

High-profile cyber-attacks on companies such as Sony have generated international headlines and 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 cyber security.

The statistics 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.

Shockingly, despite these significant cyber-security exposures, 85 per cent of small business owners believe their company is safe from hackers, viruses, malware or a data breach. 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. As more and more large companies get serious about data security, small businesses are becoming increasingly attractive targets—and the results are often devastating for small business owners.

Statistics show that roughly 60 per cent of small businesses will close permanently within six months of a cyber-attack.

In recent years, nearly 60 per cent of the small businesses victimised by a cyber-attack closed permanently within six months. Many of these businesses put off making necessary improvements to their cyber-security protocols until it was too late because

The content of this Risk Insights is of general interest and is not intended to apply to specific circumstances. It does not purport to be a comprehensive analysis of all matters relevant to its subject matter. The content should not, therefore, be regarded as constituting legal advice and not be relied upon as such. In relation to any particular problem which they may have, readers are advised to seek specific advice. Further, the law may have changed since first publication and the reader is cautioned accordingly.

they feared the costs would be prohibitive. Don’t make the same mistake. 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:

- Train employees in cyber-security principles.
- Install, use and regularly update antivirus and antispyware software on every computer used in your business.
- Use a firewall for your Internet connection.
- Download and install software updates for your operating systems and applications as they become available.
- Make backup copies of important business data and information.
- Control physical access to your computers and network components.
- Secure your Wi-Fi networks. If you have a Wi-Fi network for your workplace make sure it is secure and hidden.
- Require individual user accounts for each employee.
- Limit employee access to data and information, and limit authority to install software.
- Regularly change passwords.

Cyber security is a serious concern for all businesses—large and small. Contact ***Crendon Insurance Brokers Ltd*** *to learn how our risk management resources and insurance solutions can help protect your business from cyber-attacks.*

Crendon Insurance Brokers