CYBERRISKS&LIABILITIES_

Cyber Security for Small Businesses

High-profile cyber attacks and data breaches at Sony, Honda Canada and HRSDC have raised awareness of the growing threat of cyber crime—but recent surveys conducted by Symantec suggest that many small business owners are still operating under a false sense of cyber security.

Don’t Equate Small with Safe

The statistics are grim: The majority of Canadian small businesses lack a formal Internet security policy for employees, and only about half have even rudimentary cyber security measures in place. Despite significant cyber security exposures, 50 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. Symantec’s study found that 40 per cent of attacks are against organizations with fewer than 500 employees.

Hackers and data thieves aren’t the only threats. Smaller companies often boast of an almost family-like work environment and have a tendency to put a lot of trust in their employees. This can lead to complacency when it comes to data security, which is exactly what a disgruntled or recently fired employee needs to execute an attack on the business.

Attacks Could Destroy Your Business

Large companies are devoting more resources towards data security, making small businesses increasingly attractive targets. The results can be devastating for small business owners.

According to Symantec, the average cost of a cyber attack on a small or medium-sized business is nearly $200,000. As a result, nearly 60 per cent of the small businesses victimized by a cyber attack permanently close their doors within six months. Many of these businesses put off making necessary improvements to their cyber security protocols until it was too late because they feared the costs would be prohibitive.

10 Ways to Prevent Cyber Attacks

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 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 backup 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 individual user accounts for each employee.
9. Limit employee access to data and information, and limit authority to install software.

This Cyber Risks & Liabilities document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice.

10. Regularly change passwords.

Your Emerging Technology Partner
A data breach could cripple your small business, costing you thousands or millions of dollars in lost sales and/or damages. Contact ABEX to discuss our Cyber Risk Management program designed to protect your company against losses from cyber attacks.