Risk Insights

Brought to you by: Schauer Group

Cyber Security for Your Small Business

High-profile cyber attacks on companies such as Sony, Target and Zappos have generated national headlines and have raised awareness of the growing threat of cyber crime. Recent surveys conducted by the Small Business Authority, Symantec and the National Cybersecurity Alliance suggest that many small business owners are still operating under a false sense of cyber security.

The statistics are grim; the vast majority of U.S. 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-resistant, and nearly 40 percent do not have their data backed up in more than one location.

Shockingly, despite these significant cyber-security exposures, 85 percent of small business owners believe their company is safe from hackers, viruses, malware or a data breach. This 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.

In recent years, nearly 60 percent of the small businesses victimized 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 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. The following list of easily implementable security procedures was developed during a Federal Communications Commission roundtable on effective cyber-security strategies for small business owners and is a great place to start:

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.
10. Regularly change passwords.

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

Brought to you by the insurance professionals at Schauer Group.

This Risk Insights 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.