Cyber Liability

Cyber Security for Small Businesses

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

The statistics of these studies 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 proof, and nearly 40% do not have their data backed up in more than one location.

Don't Equate Small with Safe

Despite significant cyber security exposures, 85% 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 43% of attacks are against organizations with fewer than 250 employees.

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 fired employee needs to execute an attack on the business.

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.

According to a recent study by the Ponemon Institute, the average annual cost of cyber attacks for small and medium-sized businesses is over $2 million. Most small businesses don't have that kind of money lying around, and as a result, nearly 60% of small businesses victimized by a cyber attack close permanently within six months of the attack. 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.
10. Regularly change passwords.

In addition to the listed tips, the Federal Communications Commission (FCC) provides a tool for small businesses that can create and save a custom cyber security plan for your company, choosing from a menu of expert advice to address your specific business needs and concerns. It can be found at www.fcc.gov/cyberplanner.

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. We have the tools necessary to ensure you have the proper coverage to protect your company against losses from cyber attacks. Contact us today to for additional cyber risk management guidance and insurance solutions.

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. © 2012, 2014 Zywave, Inc. All rights reserved.