HR INSIGHTS

Brought to you by the insurance professionals at
Insight Risk Management, LLC

Cyber Security

Every day, more than 1 million people become victims of cyber crime, according to a study by Symantec, a computer security software company. Businesses, both large and small, are increasingly reliant on the Internet for daily operations, creating attractive and potentially lucrative targets for cyber criminals.

With such heavy use of and reliance on computers and the Internet by both large and small organizations, protecting these resources has become increasingly important. Learning about cyber attacks and how to prevent them can help you protect your company from security breaches.

Cyber Attacks Compromise Your Company

Cyber attacks include many types of attempted or successful breaches of computer security. These threats come in different forms, including phishing, viruses, Trojans, key logging, spyware and spam. Once hackers have gained access to the computer system, they can accomplish any of several malicious goals, typically stealing information or financial assets, corrupting data or causing operational disruption or shut-down.

Both third parties and insiders can use a variety of techniques to carry out cyber attacks. These techniques range from highly sophisticated efforts to electronically circumvent network security or overwhelm websites to more traditional intelligence gathering and social engineering aimed at gaining network access.

Cyber attacks can result directly from deliberate actions of hackers, or attacks can be unintentionally facilitated by employees—for example, if they click on a malicious link.

A breach in cyber security can lead to unauthorized usage through tactics such as the following:

- Installing spyware that allows the hacker to track Internet activity and steal information and passwords
- Deceiving recipients of phishing emails into disclosing personal information

Every day, more than 1 million people become victims of cyber crime. Cyber criminals look for the weak spots and then attack, no matter how large or small the organization.

INSIGHT risk management

- Tricking recipients of spam email into giving hackers access to the computer system
- Installing viruses that allow hackers to steal, corrupt or delete information or even crash the entire system
- Hijacking the company website and rerouting visitors to a fraudulent look-alike site and subsequently stealing personal information from clients or consumers

Cyber attacks may also be carried out in a manner that does not require gaining unauthorized access, such as denial-of-service attacks on websites in which the site is overloaded by the attacker and legitimate users are then denied access.

Securing Your Company's Mobile Devices

Gone are the days when contact names and phone numbers were the most sensitive pieces of information on an employee's phone. Now a smartphone or tablet can be used to gain access to anything from emails to stored passwords to proprietary company data. Depending on how your organization uses such devices, unauthorized access to the information on a smartphone or tablet could be just as damaging as a data breach involving a more traditional computer system.

The need for proper mobile device security is no different from the need for a well-protected computer network. According to computer security software company McAfee, cyber attacks on mobile devices increased by almost 600 percent from 2011 to 2012 with no signs of slowing down. Untrusted app stores will continue to be a major source of mobile malware which drives traffic to these stores. This type of "malvertising" continues to grow quickly on mobile platforms.

The Vulnerable Become the Victims

The majority of cyber criminals are indiscriminate when choosing their victims. The Department of Homeland Security (DHS) asserts that cyber criminals will target vulnerable computer systems regardless of whether the systems belong to a Fortune 500 company, a small business or a home user.

Cyber criminals look for weak spots and attack there, no matter how large or small the organization. Small businesses, for instance, are becoming a more attractive target as many larger companies tighten their cyber security. According to the industry experts, the cost of the average cyber attack on a small business is increasing exponentially and shows no signs of slowing down. Most small businesses don't have that kind of money lying around, and as a result, nearly 60 percent of the 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 is too late because they fear the costs would be prohibitive.

Simple Steps to Stay Secure

The DHS, which issues bulletins and alerts that provide information on potential cyber threats, has issued more than 5,000 alerts and advisories in a single year. With cyber attacks posing such a prominent threat to your business, it is essential to create a plan to deal with this problem. Implementing and adhering to basic preventive and safety procedures will help protect your company from cyber threats.

Following are suggestions from a Federal Communications Commission roundtable and the DHS's *Stop.Think.Connect.* program for easily implemented security procedures to help ward off cyber criminals. These suggestions include guidelines for the company as well as possible rules and procedures that can be shared with employees.

Security Tips for the Company

- Install, use and regularly update anti-virus and anti-spyware software on all computers.
- Download and install software updates for your operating systems and applications as they become available; if possible, choose the automatic update option.
- Change the manufacturer's default passwords on all software.
- Use a firewall for your Internet connection.
- Regularly make backup copies of important business data.
- Control who can physically access your computers and other network components.
- Secure any Wi-Fi networks.
- Require individual user accounts for each employee.
- Limit employee access to data and information, and limit authority for software installation.
- Monitor, log and analyze all attempted and successful attacks on systems and networks.
- Establish a mobile device policy and keep them updated with the most current software and antivirus programs.

Security Tips for Employees

- Use strong passwords (a combination of uppercase and lowercase letters, numbers and special characters), change them regularly and never share them with anyone.
- Protect private information by not disclosing it unless necessary, and always verify the source if asked to input sensitive data for a website or email.
- Don't open suspicious links and emails; an indication that the site is safe is if the URL begins with https://.
- Scan all external devices, such as USB flash drives, for viruses and malicious software (malware) before using the device.

Most importantly, stay informed about cyber security and continue to discuss Internet safety with employees.

Don’t Let it Happen to Your Company

According to the DHS, 96 percent of cyber security breaches could have been avoided with simple or intermediate controls. Strengthening passwords, installing anti-virus software and not opening suspicious emails and links are the first steps toward cyber security. 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. Contact Insight Risk Management, LLC today. We have the tools necessary to ensure you have the proper coverage to protect your company against losses from cyber attacks.