HR Insights

Brought to you by: Garland-Sturges & Quirk

GARLAND STURGES & QUIRK
INSURANCE BROKERS
MINIMIZE THE UNCERTAINTY OF LIFE.

Cyber Security

According to the Identity Theft Resource Center, data breaches increased 40 percent in 2016, with a total of 1,093 reported breaches. This trend continued in 2017, with over 1,120 cases reported by October. 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 shutdown.

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. According to historical claim data analyzed by Willis Towers Watson, 90 percent of all cyber claims stemmed from some type of employee error or behavior. The high-profile Equifax, Snapchat and Chipotle data breaches were all caused by employee error or behavior.

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
- 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 (DoS) attacks on websites in which the site is overloaded by the attacker and legitimate users are then denied access.

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

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

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 (FCC) 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 Your Company

Cyber security should be a company-wide effort. Consider implementing the following suggestions at your organization:

• 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. • 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 anti-virus programs.

Security Tips for Employees

- Use strong passwords, change them periodically and never share them with anyone. Never repeat a password across accounts.
- 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.

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. 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.

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 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.

A data breach could cripple your small business, costing you thousands or millions of dollars in lost revenue, sales, damages and reputation. Contact Garland-Sturges & Quirk today. We have the tools necessary to ensure you have the proper coverage to protect your company against losses from cyber attacks.

This HR Insights is not intended to be exhaustive nor should any discussion or opinions be construed as professional advice. © 2016, 2018-2019 Zywave, Inc. All rights reserved.