Five Questions With: Colin A. Coleman

According to The Global Risks Report 2018 by the World Economic Forum, 64 percent of all malicious phishing emails sent in 2017 contained malware. Colin A. Coleman, a partner at Partridge Snow & Hahn LLP in Providence, chairs the firm's Cyber Liability and Data Security division. He spoke with Providence Business News about the importance of cybersecurity to businesses, some of the biggest misconceptions and methods used by thieves and hackers.

PBN: Speaking in broad terms, how prevalent is the problem of inadequate cybersecurity in businesses you serve?

COLEMAN: Our insurance and banking clients are regulated and tend to have better cybersecurity practices in place than other businesses. Closely held business owners in other industries are busy, which can lead to an "out-of-sight-out-of-mind" complacency regarding cybersecurity risks. These businesses are most vulnerable to an attack.

PBN: What are some of the biggest misconceptions?

COLEMAN: Many business owners believe they are safe because they have installed software that is designed to offer protection. Unfortunately, this is rarely enough to prevent hackers from getting through to confidential data. The primary risk to most companies is employee behavior – especially when it comes to email communication. Software protections, combined with written policies and ongoing employee training, are the best ways to prevent a breach.

PBN: What would you say to a company that put a cybersecurity policy in place four years ago and is "all set"?

COLEMAN: I would ask the company what they have done since that time to train and educate their team on preventing a cyberbreach. While written policies and procedures are essential, a well-trained and vigilant staff is still the best defense against hackers. Never assume you are safe. Protecting against a breach requires ongoing monitoring, education and good communication.

PBN: What are some of the trends that cyberthieves or hackers use?

COLEMAN: We have seen situations where cybercriminals watch social media and then send emails that look legitimate to try and trick employees into wiring funds, such as when a CEO is heading out of the office on vacation and things are hectic. In other cases, hackers have gotten behind a company's firewall through infected or misleading email communications and planted malware on the company's server that alerts the hacker when certain key words are generated in an employee's email, thereby allowing the hacker to send phony emails and redirect financial transactions to themselves without the company even knowing a breach has occurred. It only takes an instant for a mistake to happen, and the cost to the company can be significant.

PBN: What kinds of companies need cybersecurity most?

COLEMAN: Any company that handles money is a prime target for hackers, especially if the company is frequently wiring money as part of its business. Hacking has become a volume business, evidenced by the fact that any business with data, large or small, can be held up for ransom. In short, no one is safe, and every business owner should keep his or her guard up at all times.

Susan Shalhoub is a PBN contributor. To view this article in Providence Business News, please click here.

Date Created
February 7, 2018