Is Cyber Insurance Necessary?

By Randolph P. (Randy) Johnston

Cyber-attacks are becoming more frequent, more invasive and more lucrative to bad actors. It is not a matter of if your firm will have a breach of security, it is simply a matter of when this will occur. While experts try to argue the merits and risks of using cloud providers versus premise-based solutions from a security perspective, all types of technology are vulnerable, from your mobile phone to your hosted or SaaS service.

When an attack occurs, the costs of reporting required by compliance regulations, down time and loss of data will be among the losses. Since we can't be sure that all the efforts of your technology teams on cybersecurity will keep the bad actors out, one way to mitigate that risk is to shift the risk of cybercrime to cyber insurance carriers. There are almost 100 providers of these policies today.

Public practice firms, as well as industry businesses, have a variety of regulations that must be followed for computer systems and computer-based records. For example, breach reporting laws exist in 47 states. These laws have driven recommendations to encrypt all data whether in motion over the internet or at rest on a local drive, server or storage device. However, both Tennessee and Louisiana currently require reporting a breach even if the data is encrypted.

There are other regulations that control Personally Identifiable Information (PII), Personal Health Information (PHI) or Payment Card Industry (PCI) that frequently exist in our client records or on our mobile devices. One defense you can implement is multi-factor authentication (MFA). With the March 1, 2018, changes in PCI regulations requiring MFA, the fact that many banks and other financial institutions implement MFA for larger or business accounts, as well as the requirement early in 2017 by the Internal Revenue Service (IRS) to use MFA with tax software applications, it has become clear that the minimal best practice for security is adding MFA for most businesses. If you don't have MFA or encryption, your risks increase; just like in the 1990s when not having a firewall or anti-virus software increased your risks.

Consider having security training at least once per year, but perhaps as often as four times per year. Instruction for team members on what to do, or not, and how to recognize attacks will drive up awareness, and in turn, drive down your risk. This could include simple training like recognizing bad email, not clicking through links, making sure that anti-virus software is running properly, as well as how to report and respond to a suspected issue. You can use services that test your organization with social engineering and use tools that run network vulnerability scans or external penetration tests. Studies have shown that organizations that have security as a priority from the top levels of management have more security awareness throughout the organization and have fewer security errors made.

TSCPA offers a number of CPE programs on cyber risk and cybersecurity. Go to the CPE online catalog at tscpa.org and search on "cyber."

Bad actors, whether they are individual, organized crime or state actors, have discovered that obtaining PII data can be profitable when it allows them to access bank accounts, credit cards, retirement accounts, stock holdings and other monetary instruments. While the perception of many businesses is that the bad actors only target larger players, anyone who is connected to the internet is a potential target. This is made even easier with automated cracking tools that can be obtained for less than $100. Automated tools identify specific targets with vulnerabilities, desirable characteristics for monetary gain and easy targets for infection. Malware, that is malicious software such as ransomware, can be planted that demands payment,

destroys live files and backups, or simply transfers valuable data from your business to the bad actor.

The most effective attacks are the ones that occur and you never detect. If a breach occurs on your data, and you have a reporting incident, industry standards suggest that $250-$500 per person is needed. Consider if you do work for a business and obtain individuals' records as part of that work. One project could result in hundreds or thousands of breach reports required.

Just because your provider claims to have appropriate backups, security and other protections in place, what have you done to confirm this? Have you tested your restore capabilities, business continuity/disaster recovery plan or reviewed your incident response plan (IRP) lately? What about your internal controls? Have you reviewed the strength of your various controls and procedures?

To counter this risk, insurance companies have begun to offer insurance to specifically protect against the threat of digital attacks. Most of you purchase casualty and liability insurance to protect the business from unforeseeable risk. Cyber insurers either offer separate policies or riders can be added to your existing policies to assist in reporting, forensics and litigation. The policies available and related premiums and coverage are still developing. As you review policies, listen to your underwriter, but consider the cost of:

- Downtime,
- Remediation,
- Forensics and litigation,
- Reputation damage,
- Loss of data.

It would be our hope that your business is never attacked or, worse yet, breached. However, with the simplicity of today's attack tools, the value of business data and vulnerabilities in our various hardware and software systems, even if everything is perfectly implemented, there are no guarantees that your protection mechanisms will keep the bad actors out. How can you shift the risk of cybercrime? Cyber insurance. ■

Randy Johnston is a shareholder in K2 Enterprises, LLC, a leading provider of CPE to state CPA societies. He also owns Network Management Group, Inc., a managed services provider that provides support 24x7 from Boston to Honolulu. Concepts for this article were extracted from the Technology Update session produced as part of the K2 Technology Conferences in 2017 and from his own experience working with technology at various firms in the United States.