JOURNAL *of* PENSION BENEFITS

Issues in Administration, Design, Funding, and Compliance
Volume 25 • Number 4 • Summer 2018

Plan Audits

Cybersecurity Hot Topics for Closely-Held Businesses

Five business IT security strategies relating to data security issues.

By Amanda Iverson and Paz Terry

Amanda Iverson is the Chief Operating Officer and a Partner at Pinnacle Plan Design, LLC, a Third-Party Administration (TPA) firm headquartered in Arizona. Amanda is responsible for managing the firm's internal operations, including accounting, human resources, growth strategy, and efficiency analysis. She is a Professional in Human Resources (PHR) and a SHRM Certified Professional (SHRM-CP). She is also a Certified Public Accountant (CPA). Ms. Iverson speaks on topics surrounding human resources and firm management matters. Amanda received her BA in Business Administration with an emphasis in Accounting from Pacific University and her MBA from the University of Wisconsin MBA Consortium.

Paz Terry is the Director of Technical Services for Silverado Technologies, a Managed Security Services Provider serving businesses throughout the Southwest, with its main office in Tucson, Arizona. Paz has been in the IT industry for over 20 years and has worked in every capacity, from help desk support to virtual CIO for small to midsize companies. He is VMware, Microsoft, SonicWall, and Cisco certified and is responsible for day-to-day operations for Silverado. Paz is an enthusiastic evangelist for simplified and worry-free IT security.

Often, closely-held businesses do not have a designated Information Technology (IT) expert in-house. Instead, the business relies on an owner or office manager to work with an outside IT consultant regarding its data security. And even if a closely-held business does have an IT consultant on staff, cybersecurity is a risk for every business, and not simply a risk that can be handled only by the IT department. Businesses should incorporate a data security plan into their overall business processes. This column covers a couple of common IT data security myths and addresses some relatively simple business

IT security strategies surrounding data security matters.

Common Cybersecurity Myths

Myth #1: Cyberattacks Only Happen to Large (or Small) Companies

Cyberattacks are not exclusively a threat to companies of a particular size. In point of fact, no industry or business is exempt from an attack. Furthermore, not every cyberattack is executed in the same way or affects the same areas of business. Attacks can come as malware infections, mobile device hacks, targeted phishing email, or stolen passwords, just to name a few. In the modern internet- and email-reliant world we live in, no company of any size is without risk. While you have likely read about attacks related to larger companies, such as Target and Equifax, small businesses are just as likely to experience an attack, but we likely will not read about these incidents, as they are numerous and often unreported.

To illustrate the fact that cyberattacks can happen to a company of any size and type of business, we can look at one industry: public accounting. These are just a few of the attacks that happened to companies in that industry last year. In September 2017, a news outlet, The Guardian, reported that Deloitte, one of the four largest accounting firms in the world, was victim to a cyberattack that reportedly gave the attackers access to passwords, usernames, and business and health information related to clients. [*https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyberattack -revealing-clients-secret-emails*] Additionally, in April 2017, Robinson + Cole reported that two small accounting firms in Massachusetts suffered data breaches that affected approximately 8,000 clients. [*https://www.dataprivacyandsecurityinsider.com/2017/04/eight-thousand-clients-affected-by-data-breach-at-two-massachusetts-accounting-firms/*] From one of the largest companies in the industry to two smaller companies in the same industry, each was victim to a unique cyberattack.

No company, regardless of size, is exempt from cybersecurity risks.

Myth #2: IT Security Breaches Only Happen to Companies That Use Cloud-Based Servers (or Physical In-House Servers)

There is no one-size-fits-all solution for servers for every business. For some companies, a cloud-based server provides the best solution. For others, a physical server solution best fits their business. In addition, because cloud-based servers may not be the appropriate solution for all the needs of any given company, many companies use the cloud for some applications and run dedicated hardware within their premises for other applications in a hybrid solution. Virtualization also plays a key role in leveraging hardware costs into a more redundant and inexpensive solution, and, although this method is not inherently more or less secure, adoption of security best practices must be pursued no matter where your resources are kept.

The security of a business' servers, whether physical or virtual, significantly depends on the server configuration, IT knowledge, and the IT environment. These dependent factors can differ substantially based on a company's resources and requirements. Companies using dedicated physical servers need strong and continuously trained IT leadership and expertise to manage the ongoing changes, maintenance, and security of those servers. For some organizations with a limited budget, IT staffing, or the ability to invest in capital expenses, switching to a cloud solution can offer an overall higher level of security protection, but this is not a universal truth.

All IT-related resources are at risk for a cyberattack.

Strategies for Prevention

Many business owners understand that their companies are at risk for a cyberattack but are unsure as to how best to protect against this risk. Now that we have tackled to a couple of myths surrounding IT data security, we will provide a few strategies that can be employed to mitigate against risks.

Strategy #1: Users Can Be Your Greatest Risk or Your Best Security

Cyberbreaches are often a result of human error. Security awareness education is one of the most effective methods to keeping your company secure. Cybersecurity is a team sport. Everyone in your business needs to be involved and informed in keeping your employees, clients, and business safe. You and your staff should all have basic training to avoid risky cyber behavior. Part of that education should include information about online threats and basics about how to protect your company's data, including but not limited to the safe use of social media Websites.

Phishing is a fraudulent attempt to steal data electronically. It is imperative to train your team on how to defend against phishing in order to keep your network and data secure. A majority of your threats will arrive in your team's email inboxes with a link that intends to spread a virus to all those on your network or to plant a program that scans your network for valuable data and sends that information out to malicious players. After educating your staff, continue to send regular computer security hints and reminders to keep security a top priority. The best method for testing your company's end user security education level is to send phishing test emails on a regular basis using a known, reputable vendor.

Strategy #2: Multifactor Authentication and a Password Management Solution Can Help Keep You Secure

Multifactor Authentication (MFA), also known as Two-factor Authentication (2FA), requires additional information beyond one password to gain entry. It requires a two-step sign-in process that adds an additional layer of security and protection to accounts. When using MFA, employees will need to access another device (such as a cell phone) to obtain an algorithm-generated one-time code, or a code sent to an email address, to complete the sign-in process.

Require employees to create strong, long (at least 16-character), and unique passwords that are changed at least annually. Another best practice is to use unique passwords for business accounts that differ from those used for personal accounts. This way, if a personal account is hacked, the attacker will not be able to access business accounts using that same password. Each of us often forgets our passwords. Therefore, a password manager that uses MFA can help protect accounts and keep your business secure.

Strategy #3: Use Security Software and Create Access Barriers

There are many inexpensive software options that will provide firewall, anti-virus, anti-spam, and other useful security technologies. All computers should be equipped with antivirus and antispyware software. Whenever possible, automate software and operating system updates. It is also important to utilize a next-generation firewall and a cloud-based email security service, which stops spam, scans for malicious attachments and embedded links, and quarantines questionable mail. It is important to make sure a separate user account is created for each employee. Some IT administrative rights and access should be given only to IT staff and owners or key employees. No one in the company should share information about their accounts with internal or external parties. Prevent access and use of company computers by any unauthorized individuals through education, network segmentation in which certain systems are locked down for only guest use, and company policies.

Do not forget about cell phones. These devices can create significant security risks. Cell phone devices should have software optimized with security features and should have remote wipe capabilities. Require users to password protect their mobile devices (six-number access codes are much stronger than four-number access codes) and encrypt the phone's data. Most modern email services and mobile devices natively support this functionality.

Strategy #4: Image-Based Backups With an Offsite Copy

The rule of three, as applied to data backup and disaster recovery, says that there must be three copies of your critical data:

1. Live and in production;
2. Backed up to a local repository using an image-based backup solution; and
3. Offsite at a secure location.

Maersk, one of the world's largest shipping companies, had no IT infrastructure for 10 days after a ransomware attack, partially because of ineffectual backups. {*https://www.bleepingcomputer.com/news/security/maersk-reinstalled-45-000-pcs-and-4-000-servers-to-recover-from-notpetya-attack/*} Can your business survive for 10 days or more with no access to IT resources? Can you confidently say that your data is in three places at all times?

Strategy #5: Consider Cyber Liability Insurance

Often standard business liability insurance does not cover cyber liability. Your business may need a separate policy to cover cyber liability. This type of insurance generally covers things related to privacy issues, virus damages, or any other cybersecurity data issue that may be passed along via Internet connections. This insurance can cover everything from lost revenue due to business interruption to the expenses associated with notifying customers of a data security breach. You should check with your insurance provider and review your current policy to ensure you have the appropriate coverage related to cyber liability.

Conclusion

We know there are endless IT security issues to consider. However, having a strong understanding of your risks and a plan surrounding the security tactics can help put small businesses on the path toward increased IT data security and continued business success. ■

Wolters Kluwer