Protect Your Business from Cybersecurity Concerns

mscpaonline.org/news_and_resources/publications/793/view

Massachusetts Society of CPAs

06/18/2018

In Financial Literacy

Whether you're a long-standing community business or a new web-based start-up, many of your transactions will be conducted online. While digital transactions and communications can expand your marketing reach and enhance efficiency, they can also expose you to the same types of security breaches many larger organizations experience. What's a small business to do? The Massachusetts Society of CPAs offers this advice.

Recognize You're a Target

Equifax, Kmart and Verizon are just a few of the companies that have suffered high-profile breaches recently. While we often see reports of hacking at large organizations, many owners of smaller companies incorrectly assume they're immune from the danger. In fact, small companies are also vulnerable—and many have been victims already. A study by the Ponemon Institute found that more than 61% of small and medium-size businesses had security breaches in 2017, up from 55% in 2016. Being aware of the problem—and the need to address it—is a critical first step.

Get Employees on Board

How many of your employees use the word "password" as their password? It's up to the organization to educate their people about the dangers security breaches can pose and to set clear tech policies. That includes requiring staff to take steps that include using strong passwords and changing them often, encrypting data properly, recognizing and avoiding phishing attempts and to initiating automatic locking on computers when they're not in use. All new staff should be trained in your computer security procedures, and it's a good idea to regularly conduct updates for existing employees.

Monitor Mobile Devices

Your security procedures should encompass rules for employees' mobile devices, such as cell phones, tablets and laptops. Many organizations now allow workers to bring their own devices (BYOD), meaning they can use personal technology for work. Carefully consider guidelines for what kinds of data can be accessed or used on these or any other devices used in your

business. Hacking or theft is of particular concern when devices are used remotely and connected to the Internet through unsecured Wi-Fi. Employees should be trained on the importance of protecting confidential company or customer data. In addition, employees should be aware of how to report the loss or theft of a mobile device that contains business data or that connects to the organization's systems.

Keep Your Security Up to Date

Make sure you have the latest version of security software and you download all necessary updates for all your software as they become available. Install a firewall that prevents access to your data or systems by outsiders. Technology used by employees who work from home or other remote locations should also be protected by a firewall. Be sure, as well, to secure and password protect your organization's router.

Set Sensible Limits

Employees should have access to data or systems that relate to their jobs, and no more. That's particularly true of confidential, personal employee or customer data in your systems, but don't stop there. An IT staff member's login may allow him or her to make changes to the system, but other workers should have separate logins that prohibit that access. In addition, workers shouldn't be allowed to load their own software onto company computers.

Turn to Your CPA

Worried about the many challenges a small business may face? Whether you're concerned about technology issues, the need to raise capital, marketing or any other challenge, your local CPA can help. Turn to him or her for expert advice on all your business issues. To find one near you, visit mscpaonline.org/findacpa.

View other publications in Financial Literacy