Image courtesy of Pixabay

How Better Data Security Can Protect Profits for Small Business Owners

It seems like every day, another company is in the news for a data breach. You might think only the bigger companies are under the gun, but small businesses are falling victim to cybercrime at an alarming rate. Here's how making security improvements at your company can have an impact on your profit margins.

Small potatoes or easy pickings?

We hear all the time about big corporations being hacked and losing time, face, and profits, and it might lead you to believe criminals set their sights on bigger fare than what your company could offer. However, some recent studies show 58 percent of 2018's cyber attacks were targeted toward small businesses. And as a small business, a data breach won't just sideline you. The cost of getting things back under control can devastate an ill-prepared company. And topping it all off, unfortunately, small businesses catch criminals' interests because they often have weak defenses.

Learn from the big dogs

It's important to amp up your security measures to protect your data, and in turn protect your company. One way to determine how to improve your defenses is to embrace SOX compliance practices. SOX refers to the Sarbanes-Oxley Act, which applies to publicly traded companies.

These regulations dictate how bigger companies handle their data. While small businesses aren't required to follow suit, incorporating applicable concepts into your business's routine is a worthwhile endeavor. Exploring this guide to SOX compliance can help you determine the best course of action for your small business.

Follow the rules

Depending on which state you live in, your business may be required by law to follow regulations for customer data protection. In New York, for example, certain businesses — like private bankers and insurance companies — must conform to the NYDFS Cybersecurity Regulation. This law requires all covered businesses to develop and maintain an effective cybersecurity infrastructure. They must also regularly analyze the program, report cybersecurity events, and implement a plan for improving the program. Other cybersecurity regulations are in place for various business types, such as private entities, the healthcare industry, and government agencies — the last of which the National Conference of State Legislatures provides in detail by state.

Friend or foe?

One of the primary ways criminals gain access to your data is through malware. Typically, someone clicks on a link that takes the user to another site, and then the user is asked to enter sensitive information, or the user clicks an attachment, which opens and starts syphoning data from your system. These emails often come incognito, appearing to be from familiar sources. Training your staff to recognize malware is a great first step in protecting your data, as is ensuring they are especially protective of sensitive information, like passwords and client information.

Open, sesame!

Passwords are a common weakness amongst computer users, in both the business and private arenas. All too often, people choose words because they are easy to remember, like "password," then use the same password for every account, and never change them. In these situations, once a criminal hacks in, they can slip into everything that user accesses. It's crucial to lock down passwords, require complex passwords that are changed routinely, and use a password manager to facilitate the ongoing process.

Bolster fences and gatekeepers

When looking for places to make improvements, hardware and software are a couple key players in defending your business. Using outdated equipment and old school applications can leave you vulnerable to hardware failures and data breaches. It's important to keep your systems fully up to date, install well-chosen virus protection, and make sure you have the latest and greatest security patches so your fences are solid.

In addition to solid fences, you need gatekeepers who can recognize threats coming and going from your company. This can come in the form of firewalls, which essentially evaluate the data going in and out of your system, and filters the threats. Take an inventory of your in-house needs then read reviews of recommended firewalls so you can make an informed choice.

Take to the sky

E-3 Magazine International points out it's smart for small businesses to move to the cloud. It's far more secure than trying to maintain your data on-site, and additionally, it can improve your company's bottom line. It's a chance to become more flexible, raises communication and collaboration with team members, and increase productivity. It also cuts down on time spent making all those updates, and having less equipment to purchase, so your overhead is lower.

Small businesses are frequently vulnerable to data breaches, and when losses occur, it can cripple a company. Protect your small business with well-chosen policies, educated staff, and up-to-date equipment. In the end, it's a chance to defend, and even raise, your bottom line.