Security is one problem that small businesses need to take care of pronto

December 5 2019, by Gene Marks, The Philadelphia Inquirer

Credit: CC0 Public Domain

So where's the best place to spend your company's technology budget next year? The answer may surprise you.

Sure, you can upgrade your accounting system or get that long-desired customer relationship management application. You can put money into marketing software, a new set of point-of-sale devices or better tools to manage your inventory. But before you do, you may want to think about something else: security.

Why? Because your small business is vulnerable—very vulnerable—to an attack. Don't think it won't happen to you. It probably will. More than one in five small businesses reported a data breach within the past 24 months, according to a recent report from Bank of America's Merchant Services. And 41% of those said that a data breach cost them more than $50,000 to recover.

Those are the lucky ones. Many other small businesses find themselves shut down for days — even weeks—from a cyberattack. Is this something you can afford? Probably not.

"Every day we hear about new and dangerous cyber threats," says Rick DeLello of Informed Systems, Inc. in Blue Bell. "Making sure your environment is protected from such threats is paramount to any small business today."

Unfortunately, the risk of an attack is getting worse. In just the past few weeks alone, we've seen brands such as Macy's, T-Mobile and restaurant chains like Moe's, McAlister's Deli, and Schlotzsky's all suffer data breaches, and these are just the recognizable companies that we read about. Most small business owners know that no organization can confidently claim that their customer, employee and company data is 100% secure. But there are practical steps to take to decrease your odds of falling victim to a cyberattack.

Jeff Sumner of TechGuides in Media says that having a good firewall is the best place to start. "Many small businesses think the equipment

provided by their Internet company is sufficient," he says. "It isn't. Spend money on a commercial grade firewall and have an expert configure it for you."

"Backups! Backups! Backups!" Chris Stafford, another local technology consultant, adds. "Every small business should have both onsite and offsite backups with version control. Malware like ransomware can cripple a business without the ability to "go back in time."

Brad Finberg, who owns the tech firm Micro-Innovation in Allentown, urges his clients to make sure they're running the most current operating systems, particularly if they're using Microsoft Windows.

"On January 14, 2020, extended support for Microsoft Windows 7 will end, leaving anyone still running the operating system vulnerable to new security bugs that will not be patched by Microsoft any longer," he warns. "This is very critical for any business and especially those in industries with regulations like healthcare and financial services, to stay compliant and protect their customer data."

There's also the cloud. Some think that moving their data online is less secure, but that's actually not correct. Managed services firms like Right Networks (a client of my company) and local providers Miles Technologies and Waypoint Consulting host both data and applications for tens of thousands of small businesses nationwide.

These companies—and there are plenty of other managed services companies like them—not only provide a higher level of protection and access from any device, but also ensure that their clients' systems are regularly backed up, updated and protected from data breaches. And let's face it: these companies can afford to hire better people and use more advanced tools than you and I, right?

The bottom line? Your 2020 technology spending should prioritize security. But don't stop at just software and services. There's something else that's just as important: training.

Why? Because human error — goofs made by you, me and our employees—accounted for more than 25% of data breaches last year alone, according to a recent study from IBM. All of the tech experts I know agree that an investment in training that enables employees to recognize threats from websites and downloaded files will reduce your company's risk of an attack.

DeLello recommends taking things one step further by committing to a regular tech assessment. "That way a business can make sure there are no security holes in their networking environment," he says.

Can we all agree that most of us have spent plenty on software and hardware over the past few years yet we're not even using what we to have its fullest potential? Rather than spending on more technology, a better use of our 2020 dollars is investing in the tools, services and training to protect the data that we have.