Sure, you can upgrade your accounting system or put money into marketing software or better tools to manage your inventory.  However, before you do, you might want to think about security.

Many small businesses find themselves shut down for days after an attack, some even weeks or months. Is this something you can afford? Probably not.  Every day we hear about new and dangerous cyber threats and 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 month alone, we have seen Macy's, T-Mobile, and Schlotzsky's all suffer data breaches, and these are just the recognizable companies. Most small business owners know that no organization can confidently claim that their customer, employee and company data is 100% secure. Nevertheless, there are practical steps to take to decrease your odds of falling victim to a cyberattack.

Having a good firewall is the best place to start. Many small businesses think the equipment provided by their Internet company is sufficient, but it isn't. Spend money on a commercial grade firewall and have an expert managed services company configure it for you.

Backups! Backups! Backups! 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."

All technology resellers urge customers to make sure they are running the most current operating systems, particularly if they are using Microsoft Windows.  On January 14, 2020, extended support for Microsoft Windows 7 ended, leaving anyone still running the operating system vulnerable and will not be patched by Microsoft any longer. 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 is also the cloud. Some think that moving their data online is less secure, but that is actually not correct.  Managed services firms like CDS Office Technologies provide protection for your IT environment, data and applications.

CDS not only provides a higher level of protection and access from any device, but also ensures that their clients' systems are regularly backed up, updated and protected from data breaches. In addition, let's face it: CDS can afford to hire better people and use more advanced tools than you, right?

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

Why? Because human error – mistakes made by you and our employees - accounted for more than 25% *of* data breaches last year alone. All of the tech experts 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.

Experts recommend talking 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.

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.

Contact CDS Office Technologies for a no-charge risk assessment. It’s one action item you can’t afford to put off…