Small businesses need to protect from hackers, too

Cyber Security is the latest IT-related buzz word. As is often the case, this covers a huge range of topics, but our focus is always the small- to medium-sized business and their IT needs, so that's where I'll start.

The threats, attacks, and the onslaught of social engineering efforts against businesses has become staggering. It used to be that an up-to-date anti-virus software, a firewall, and anti-spam for inbound and outbound email was all you needed to be fairly secure, especially if you were a "small" company.

There's a strong perception that a small business is just too small for hackers to bother with — that is absolutely not true. So is this threat real, or are we just exaggerating and creating fear? I'm confident that if you check the news in whatever medium you like, you will hear of small, medium, and large companies being compromised. I've visited new clients only to hear they've paid the ransom several times.

So where to start? The best starting place is the basics; a good anti-virus software that is up-to-date; a firewall with country blocks and specific port configurations; anti-spam filtering, both inbound and outbound.

Next, educate your staff and arrange ongoing educational opportunities. The number one reason hackers get in is the human factor! This can include weak passwords, shared log on

CATHERINE WENDT

> There's a strong perception that a small business is just too small for hackers to bother with — that is absolutely not true.

credentials, and walking away from your computer but staying logged in. Social Engineering in this venue is the process of determining what types of "hooks" a user will fall for such as email that looks like it came from your bank, a package that is trying to be delivered, or a document that needs to be signed. When you look at these messages, the sender might have the wrong domain name or it is misspelled; they often include requests to provide the user name and password, something your staff should never provide. Be skeptical!

Helping your staff approach email with a critical eye will go a long way in protecting your network. Who sent the email? Is there a link to click on — who knows where that actually goes? Is this a bank you don't even do business with? Is it about your Office 365 email box, but you use Outlook? If

there's a package to be delivered, call them instead of clicking on these links.

The other critical computer-related component is your backup. All backup solutions are not created equal! Be sure it is image-based with regular incremental updates. Don't skimp on what is backed up — if it's just the data, that means the entire computer has to be rebuilt before the data can be copied back, and you have to have the right software (and version) installed; very time-consuming. If you were infected yesterday or the day before, pulling the last backup might not be good enough because it may have been infected, too. For cloud-only solutions, consider how long it would take to download all that data. One company downloaded only the critical accounting data after an attack, and although it was all there, three days later they were stilling waiting for it to finish. There are many options here, so think through the recovery process, as well as the backup process.

Does this feel overwhelming? This is why you need to have a trusted professional IT group as a partner. They can help you navigate this changing landscape and educate your staff. Even within the last two years, many things have changed, so lean on them to take care of your computers so you can take care of your customers!

• *Catherine Wendt is owner of Syscon Inc. in Hinsdale. Contact her at cwendt@syscon-inc.com.*