CYBER SAFETY

Evading hacker attacks on small business

When a company relocates or offers to relocate a new or current employee, they're most likely not moving all those belongings themselves. They're probably calling a company like Plus Relocation.

The Minneapolis-based firm has offices here, in London and Hong Kong, and it's helping employers and employees move in more than 150 countries, providing local support in each of them. Some of the company's clients are large technology companies with workers in many offices in many states and countries all over the world.

All of which is to say that Plus Relocation has a lot of people's and businesses' important private data in its possession and a significant incentive to make sure that data stays safe. The company meets regularly with Atomic Data, its managed service provider, to talk about security and compliance requirements, new best practices and other issues.

"Our reputation is only as good as we maintain it," says Andrew Kubitschek, chief information officer at Plus Relocation. "We haven't had an issue, thankfully. But definitely, if we were compromised, it'd be a big deal. That's what makes us a target of an attack."

Tyler Olson, founder of **Shyld Academy,** helps train companies on what steps they can take to protect themselves from cyber hackers.

by Andrew Tellijohn

Training and communication help

Kubitscheck worked at Atomic Data before joining Plus Relocation. Atomic Data uses many strageies to help Plus Relocation know where it's vulnerable, including the simulation of phishing attacks and sending of spoofing emails to test employees. Such actions provide instant feedback on issues where workers may need some additional training.

The company also offers regular training on securely transmitting and destroying sensitive information in compliance with government rules.

"For me, it's a kind of continuous improvement," Kubitschek says. "We can implement one thing and three months later, we have to find another, the next best thing to implement to continue to keep us safe."

Last year, with COVID-19 bringing about a largely remote workforce, the company faced further challenges ensuring its phone systems, meeting platforms and other technologies were secure.

"Hackers are out there ahead of things, and it's sort of a catch-up game, trying to implement anything and everything you can that will keep you as up to date or as secure as possible," he says. "Obviously, they find ways that beat you to the punch, but that's really been a significant focus."

Small businesses may not be able to afford all the best software and hardware associated with cybersecurity, but experts say they can't afford to risk doing nothing at all.

Training starts with internal policies

Mark Gamm, director of technology, architecture and compliance at Atomic Data, agrees that one of the most valuable things a company can do is train its employees, because often times, the threats aren't complex, sophisticated efforts to break into computers, but rather simply sending well-rehearsed emails asking for information that will gain them access.

That takes some work internally, as well. Companies need to decide in advance what their policies will be on employees using their own devices or on what software can and can't be installed on company machines.

"Everybody wants to talk about what solutions do I need to buy," Gamm says. "What tools do I need to buy. Before you can really do training, though, one of the things that most small businesses don't take the time to do is policies, determining things like your incident response plans. … In order to really get to the training

Atomic Data meets regularly with clients to go over vulnerabilities and discuss best practices.

aspect, you have to start with policy, so you know what you're training about."

CyberNINES President Scott Singer agrees. He says ransomware is one of the chief threats to small businesses right now. He worked with one financial firm in the Midwest that got a legitimate-looking request to change a direct deposit account.

"Instead of having a policy or procedure in place, a work process that says you verify this by a phone call or some other process, they just changed it and that client lost some money," he says.

The ransomware emails and, now, gift card scams, are not sophisticated. They're higher in quality than they used to be — usually with all the words actually spelled correctly — and they are sent to large quantities of people in hopes of landing a few unsuspecting respondents.

"It's really a numbers game," Gamm says. "If I send out a million emails and I get two people to click, maybe it's worthwhile. Maybe I get something from it."

Unsuspecting targets

Cybersecurity experts say one of the reasons small businesses need to worry is that they … don't worry enough. Despite well publicized attacks on companies large and small, small businesses still let simple things slide that could help keep them significantly safer.

"We're seeing more and more small businesses being targeted with hacks and ransomware and various forms of data breaches," says Tyler Olson, founder of Shyld Academy, which does training for businesses on what to watch for from hackers.

He's heard of businesses that have lost access to their operations when someone took control of their networks, listened as another client learned that all of his customers had been asked to send their payments elsewhere one month and agonized as yet another found out his entire staff's personal information was compromised.

"For some small businesses this could put them out of business," Olson says. "That can become devastating for small businesses especially."

"Small businesses are especially at risk for data breaches that are out there," he says. "I feel bad because many people will reach out to me after they've had a data breach versus before. We can certainly help reduce the chances of that next data breach, but I want to protect from the first ones, as well."

Do something

While they may not have internal IT staffs or massive budgets for all the latest software or hardware fixes, security experts agree that small business owners should at least do something. One option for familiarizing themselves with the risks and solutions is attend one of the cybersecurity forums available in the Twin Cities.

Among them:

- **Cyber Security Summit,** which has a small business track, coming up October 25-27
- **Government IT Symposium,** with its cybersecurity component, November 15-18
- **Secure 360**, next scheduled for May 10-11, 2022

While small businesses may not have all the resources, they also often can't afford the costs associated with not doing anytihng and then trying to fix the problem when they get hacked. If they can't afford a lot of software and hardware, there are many less expensive steps they can take to mitigate risk, Gamm says, including regularly scheduled backups of their data,

"One of the first things that small businesses tend to not think about or ignore is backups," he says. "If you get

> Training employees is one of the best — and least expensive — solutions for keeping a company safe from ransomware and phishing emails.

compromised, the first thing you are going to want to be able to do is restore your backups. A lot of small businesses say 'yeah, we've got backups,' but when is the last time you actually tested the restart process? When was the last time you actually went through and made sure you can actually recover from a backup? It's a really easy first step."

Gamm and others also recommended multi-factor authentication, or requiring more than just a single password, for accessing logging in to key systems.

"It's becoming more and more prevalent that people are getting passwords that are compromised," Gamm says. "Multi-factor authentication gives that second assurance that you're protected."

Nearly 95 percent of data breaches are caused by an employee doing basic "cyber-hygiene" poorly, says Olson, who suggests that unique passwords on all accounts, multi-factor authentication on as many accounts as possible and simple training are low-cost ways of protecting businesses from attacks.

Olson suggests business owners interview some potential partners to find someone, preferably local, to help deal with these issues. He, for example, works with a lot of companies spcifically on training of employees on cybersecurity issues and has partners he can put clients in touch with if they desire more detailed software or hardware solutions.

Singer, from CyberNINES, also is used to working with other companies in tandem. He often partners with managed service providers hired by small businesses to run their information technology departments. Those partners generally do fine with most general technology, but often don't have cybersecurity backgrounds, he says.

Compliance required for contracts

On a side note, if companies won't guard against being hacked for their own well-being, they sometimes have to anyway in order to land certain deals like government contracts.

The U.S. Department of Defense, for example, has highly complex security requirements with which it is often difficult for small business owners to comply.

Singer works primarily right now with small manufacturing companies in Minnesota and Wisconsin and with some financial services and medical firms to help in that area. He spent 30 years in the Navy and he's familiar with such requirements.

"Small businesses don't have purchasing departments, they don't have regulatory departments, they don't have compliance people, they haven't gone to classes on government contracting," he says, "They're really at a disadvantage when it comes to this. We're trying to help all these businesses meet those requirements."

CONTACT:

MARK GAMM is director of technology, architecture and compliance at Atomic Data: 612.466.2000; info@atomicdata.com; www.atomicdata.com.

ANDREW KUBITSCHEK is chief information officer at Plus Relocation: 888.251.2825; akubitscheck@plusrelocation.com; www.plusrelocation.com.

TYLER OLSON is founder of Shyld Academy: 651.603.4567; tolson@shyld.academy; www.shyld.academy.

SCOTT SINGER is president of CyberNINES: 608.512.1010; inquiry@cybernines.com; www.cybernines.com.