Need Help Filing Business Tax Returns? Startup-Friendly Accountants Are on Page 16.

January 2016

The Monthly Resource Guide For Startup Businesses

NEW BUSINESS MINNESOTA

Special Report

Fireproof? Protecting Your Business

You've Worked Hard to Launch Your Business. Have You Taken Steps to Protect What You've Built? These Experts Offer Their Solutions: **Bob Weiss,** Computer Integration Technologies, Inc. (CIT); **Cindy O'Donovan and Julie Tschida,** Right4 Your Business; **Kenneth Kunkle,** Kunkle Law PLC; and **Steve Emmer**, ADT Security Systems. Page 4.

Cyber Criminals Put Every Business at Risk

Protecting Your Computers, Network Requires Defensive Measures and Well-Trained Employee.

By Bob Weiss

Computer Integration Technologies, Inc. (CIT)

Hackers, code crackers and cyber criminals of all stripes want your data. More precisely, they want to make money off your data, either by gaining access to your financial resources or selling it to other crooks in online markets.

The urgency and need to protect your office computer, laptop and home computer has never been greater. Last year, the cost of cybercrimes of all kinds in the U.S. was in excess of $400 billion. It is a very profitable line of work that is constantly evolving and expanding.

As the senior cyber security engineer with Computer Integration Technologies (CIT), which provides IT solution for businesses of all sizes, I've been in the thick of this battle, helping companies implement software, hardware and training solutions.

This is a problem that you need to continually address both for your business and for your home.

Email Is Weak Link

Most people have reasonably good security in place from a perimeter standpoint. Most computers have firewalls and have malware/virus protection running programs like Norton Antivirus and Spyware Removal that does regular scans and is updated frequently.

Although firewalls do a good job of preventing attacks from the outside, they aren't the weak link.

Of all successful breaches, 95 percent start as an email. Most of them gain access because someone lets them in with a simple click.

That's how the now infamous data breach at Target happened. The corporation had the most sophisticated cyber security measures in place, making a successful assault nearly impossible.

But that that level of security didn't extend to the ranks of their suppliers. The breach was successful because of an email sent to an HVAC vendor in Ohio who was tricked into providing passwords needed to get past Target's firewall and onto its network where they could do almost anything they wanted.

The lesson you should take from security breaches like Target's is that you are only as secure as your least secure vendor or supplier and your least attentive employee. Or you, yourself.

Most small business owners don't think they're likely targets because they are small. But small companies are being targeted because they are often the easiest way to break into a bigger, better protected company.

Phishing

Phishing is one of the most common techniques for gaining access. An email arrives looking like it came from a major bank or shipping company. It has their logo, their fonts and looks like the real deal.

The email says there is a problem with an account and they have to take action. A link is provided, but it takes them to a fake login page where the unsuspecting person gives up their password.

Another approach is to have an email with an attachment – often a pdf file – that has malicious program embedded in it. When you open it, the program launches, giving them remote access to your computer. They can see everything you're doing. And they can run the computer just as if they were sitting in front of it.

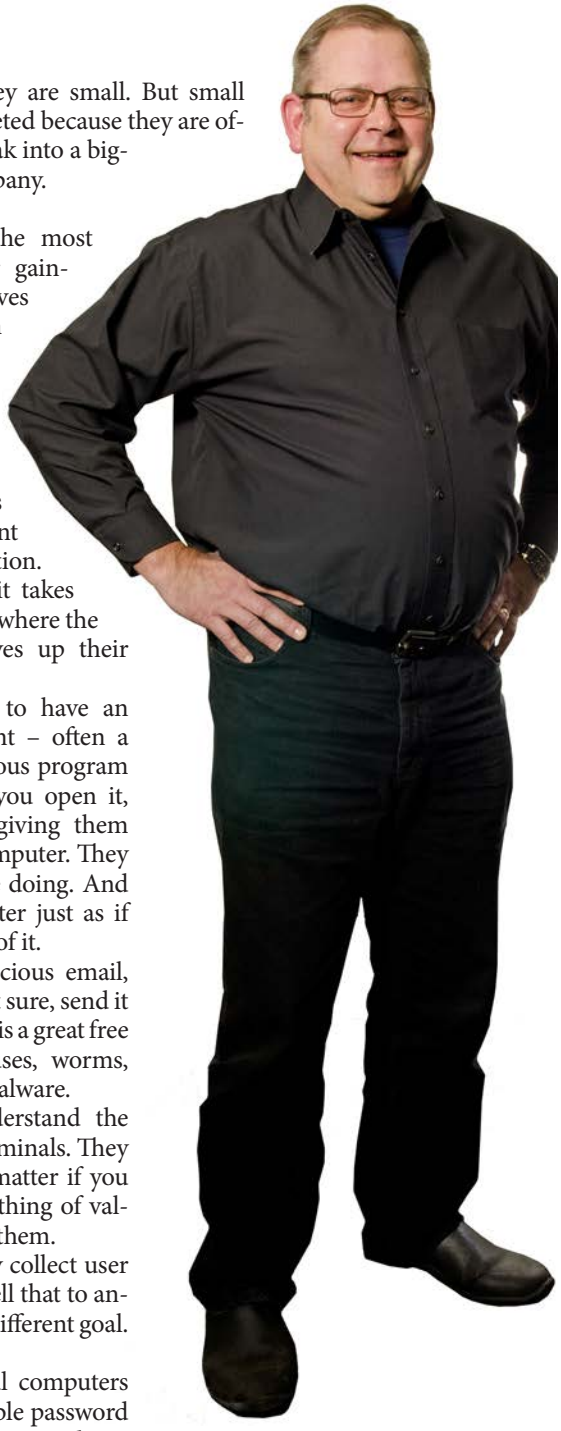
If you receive a suspicious email, leave it alone. If you're not sure, send it to www.virustotal.com. It is a great free service that detects viruses, worms, trojans and all kinds of malware.

It's important to understand the end game of the cyber criminals. They all want data. It doesn't matter if you don't think you have anything of value, all data has a value to them.

One bad guy may only collect user IDs and passwords and sell that to another bad guy who has a different goal.

Passwords

Using hugely powerful computers to grind away at all possible password combinations, they break yours down



Computer Integration Technologies Continued on Next Page

and sell it.

If you have a seven-letter password, they can break it in less than five minutes. Passwords of fewer than 10 characters might take a day. The simpler and easier a password is for you to remember, the easier it is for them to crack. Longer passwords are better.

A 12-character, lower-case password would take about three years to break. Include a single capital letter and it will take 12,000 years. Including symbols or numbers geometrically increases the security.

Pass phrases are becoming a good alternative to passwords. They are both long and easy to remember. The pass phrase "lassiecomehomenow" -- all lower case -- beats the short and complex password "$sale%12".

Of course if the hackers just send you a nice email, you might unwittingly give them what they want and save all that letter crunching.

I use two-factor authentication for things like Google, Facebook and my Amazon account. Enter the username (I avoid using my email address if possible) and enter the password. An app sends a message to my smartphone and I have to confirm. Very secure.

Another mystery to most people I consult with is why medical records seem to be so important to the data thieves. On the black market, they are 10 times more valuable than credit card information.

The reason is that medical records are so very complete, making it easy to create a fake identity with a full back story. They'll know about your moles, tattoos, next of kin, social security numbers, and more. They can become you.

In recent years, ransomware has hit computer owners hard. Once the bad guys infect your computer through email or a website you may have visited. Your computer will lock up and you'll be invited to pay fees as high as $1,000 to have it set free.

This blackmailers actually offer "customer service." If you have trouble unlocking, they have tech people who will help. How considerate.

Vulnerability Assessment

The first thing we do for our new clients is a vulnerability assessment. Part of that includes sitting outside their system so we can see it the way an attacker would. Then we mimic an attack and document how their defenses work.

And we do it from inside the system as well to uncover vulnerabilities like open file sharing with no authentication required or the presence of expired operating systems like Windows XP within the system.

We make recommendations for the best way to fix the weaknesses we find and look at procedures and training for employees.

It is becoming more common for companies to send security surveys to their suppliers, this is often called a Vulnerability Assessment Request. They want proof you are secure and can be trusted.

If you run credit cards through your computer, you have to prove Payment Card Industry Data Security Standard (PCI DSS) compliance by completing a questionnaire on technical issues and then pass an online security check.

Since the software needed for these assessments can cost upwards of $15,000 and in-house IT staff is already focused on other priorities, companies rely on Computer Integration Technologies' expertise to complete the assessments.

Some of our clients get six or seven such requests a year. The assessment we do can often be used to satisfy other assessment requests they get.

Another big security compliance regulations is HIPPA for medical records. Most big medical organizations already have outstanding compliance and procedures in place, but smaller practices need to conform as well and they often don't know if they are doing it right. With fines of $25,000 per instance, they need the help of Computer Integration Technologies Inc. (CIT).

HIPPA sets a minimum security standard. We try to get our clients to a higher standard. For example, HIPPA requires patient information to be encrypted only during transmission from end to end, but not in storage. We advise clients to have it always encrypted.

If patient information is on a laptop, everything on the laptop, even the operating system, needs to be encrypted.

Training and documentation are extremely important for maintaining security. After our initial assessment, we provide all the documentation to maintain the process and offer cybersecurity awareness training for all their employees.

We also review how employees are using the internet professionally and personally. We have a managed services product for controlling internet access. It can keep employees from going to sites where malware lurks.

Conclusion

Strong security protections require everyone in the organization to be part of the solution. The right technology solutions have to be in place and constantly updated. And you need to constantly be alert for your weak links, whether it's the new hire who isn't fully adjusted or the executive who likes to take shortcuts.

The bad guys aren't going to rest and neither can you.

NBM

Bob Weiss is a senior cyber security engineer with Computer Integration Technologies, Inc. (CIT), which provides a one-stop IT solution for businesses of all sizes to keep their technology up-to-date, up-to-speed and secure. He can be reached at (651) 255-5780 or sales@cit-net.com www.cit-net.com

Call To Action

For more useful information on how to secure your business or home computer environment, check out Bob Weiss' blog at www.cit-net.com/security.