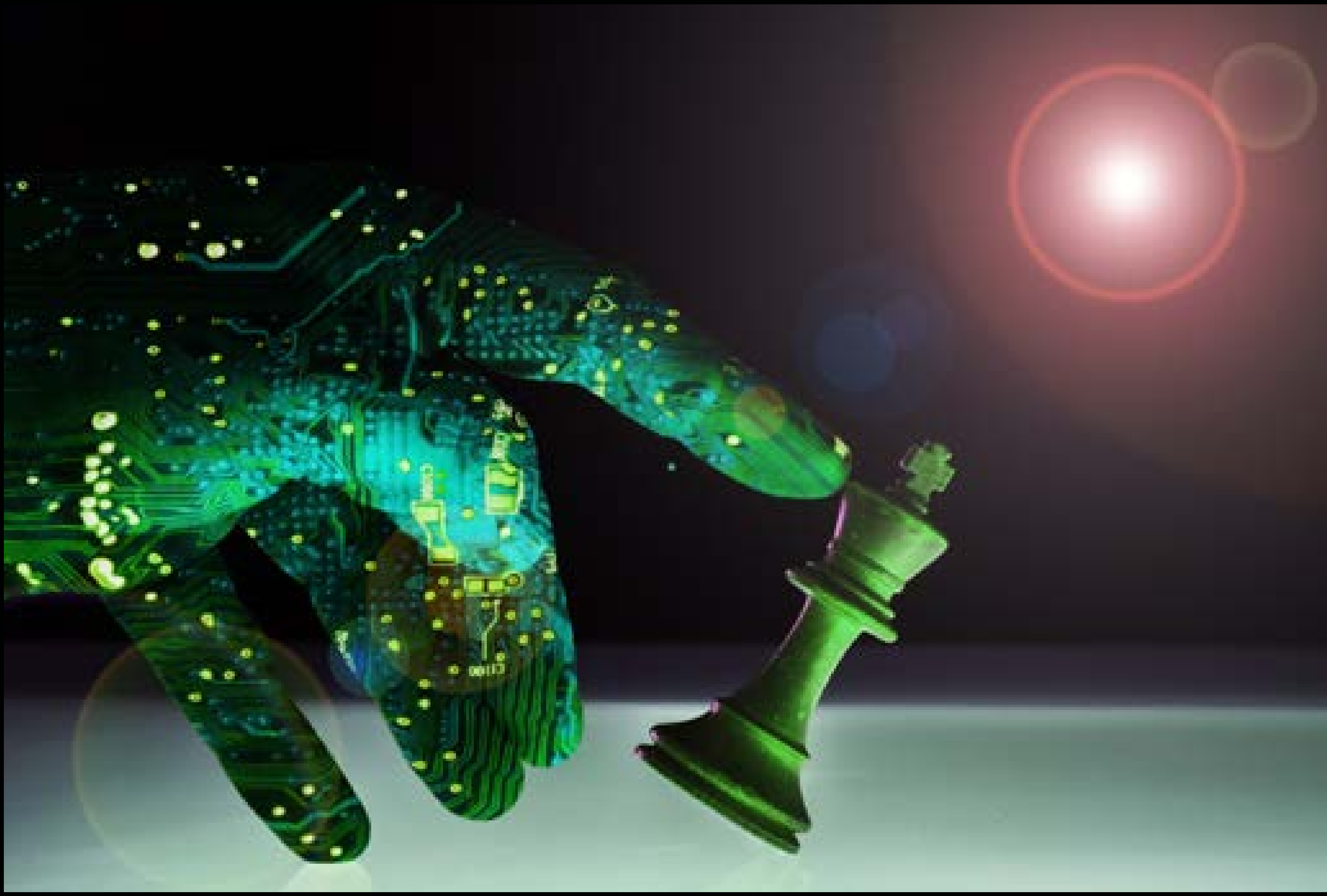
COMCAST
BUSINESS

CYBERSECURITY:

TRACKING THE CURRENT THREAT LANDSCAPE



COMCAST
BUSINESS

CYBERSECURITY:

TRACKING THE CURRENT THREAT LANDSCAPE

Hackers work 24/7, and small business is increasingly at risk. Here's what you need to know to protect your company.

SMALL NO LONGER EQUATES WITH SAFE

If you're lucky, you first heard about WannaCrypt (often better known by the nickname WannaCry) ransomware when it made international news in May 2017. But as a small business owner, you can't afford to trust your luck to hold. While the WannaCry headlines focused on large, high-profile organizations hit by that attack, small businesses' size no longer affords them the security they enjoyed in the past against cybercrime.

The risk to small business is so significant that it prompted bipartisan legislative action in the Senate, which in September 2017 passed the

MAIN STREET Cybersecurity Act. In announcing the legislation, the bill's sponsors cited a 2012 report that businesses with fewer than 100 employees suffer 71 percent of cyberattacks, which can do enough damage to drive small companies out of business.

And the threat landscape has become even more challenging to navigate during the past few years. That's because bots and automation have made it possible to blanket cyberspace with phishing schemes, malware, ransomware, and other means of compromising your company's data security. You no longer have to be targeted for an attack. You don't even have to be on the cybercriminals' radar to be hit.

While targeted attacks still occur, "small business people who think no one's going to phish them are very wrong," says Joel Snyder, senior partner at Opus One, a Tucson, Arizona-based IT consulting firm that specialized in networking, electronic mail, and security. "They're going to discover that they're caught in that same net of hackers trying every single domain in the universe.

You could also find yourself in the company of small business owners whose companies were targeted. That can happen when hackers have a specific interest in some aspect of your business. But it's more common when they attempt to exploit weaknesses in your security to gain access to another organization—to use you as a conduit to get to one of your vendors or your biggest customers. It's worth remembering that each time you celebrate a big new account win, you're also potentially making your company more attractive to cybercriminals.

WHERE ARE THREATS COMING FROM?

This is a cat-and-mouse game in which the cats are particularly devious—and become more so every time you get wise to their latest tricks.

WannaCry was ransomware, which invades computers or servers, seizes all their data, and makes the data inaccessible to the owners until they pay ransom—in this case, in the form of bitcoin currency. FBI crime statistics show that the number of ransomware attacks increased by a third from 2014 to 2015. Complaints filed grew from 1,800 to 2,400, and losses rose from $23 million to $24 million. But that's just reported attacks.

According to the Bureau's 2016 Internet Crime Report, victim losses to cybercrime for the year totaled $1.33 billion.

Snyder notes that ransomware has the potential to be more effective against businesses with poor IT practices. Opting to economize by not updating to the latest operating system is a risk factor. Poor backup processes and practices also make companies more vulnerable. Conversely, those who have their data protected and accessible in the cloud, for example, don't even have to consider paying ransom because they haven't lost anything they can't recover on their own.

Website attacks are another threat. Here, hackers seek "vulnerabilities in major tools" such as WordPress, Snyder says. In these cases, you may be targeted via email, by someone scraping your site or by bot-generated attempts to reset your password.

Among the most familiar schemes are those involving email, where "you should be very, very suspicious of everything, because the attackers are smart," he adds. "Be suspicious of anything you see coming in via email that looks in the least bit out of the ordinary."

Examples include "we couldn't deliver your package" notifications when you weren't expecting a package. Another red flag: a message that appears to be from someone but contains uncharacteristic errors in spelling or grammar. Scammers may purport to be interested in buying your domain name or selling similar-sounding domains. Approach shortened URLs with caution, too, as they're useful for hiding malware evidence. And if you've received something that appears to be spam and includes an "unsubscribe" link, look before you click, because that link may duplicate the sales URL you took care not to click.

"If it's from some company you've never heard of, that you have no relationship with, and particularly in another country," Snyder says, "then probably the unsubscribe link will either get you some malware if you click on it or won't do anything useful."

PDFs and Word documents can also be infected, he cautions, because they're created through programming languages that can be embedded with malware. When you open the document, you unwittingly trigger the execution of a code or launch an application.

And this should go without saying, but those phone calls from the Microsoft or Apple security team are not from the Microsoft or Apple security team. None of your operating system or software vendors will contact you by phone about security compromises on your computer or other devices. Anyone who does contact you is seeking access to your system to create, not resolve, a compromise in your security.

ASSESSING YOUR DATA SECURITY SUPPORT

As the old saying goes, there are just two kinds of computer users: those who have experienced a system crash, and those who have not experienced one yet. Do you know how to manage one when it's your company's turn? Do you have a business continuity plan in the event not just of a crash, but also of a power failure, natural disaster, or cyberattack? Can you manage the data recovery process yourself, or will you need support from your security solution provider?

If your company's practice is in line with Snyder's observations, chances are that you don't have a business data continuity plan. "They're complex plans to write, they're hard to test, and they often change over time and so fail when you need them most," he says. "I've stopped trying to tell people to engineer redundant data centers and redundant systems, and instead have them think of continuous data integrity."

That means implementing a system that automatically backs up and, ideally, also restores constantly to a second server (or from your desktop to your laptop). In other words, instead of creating a contingency plan for data recovery, create an

WHERE'S THE THREAT?

Where cybersecurity is concerned, you're not dealing with a landscape as much as a landmine. Threats can be embedded anywhere.

- **Phishing attacks attempt to lure you in via email. Make sure that you know the sender and that the email is legitimate.**
- **Check your inbox subfolders for any mail that's marked "infected," and delete it promptly to ensure that you don't inadvertently click on and open it later.**
- **Set up the right level of junk mail filtering to reduce email inbox clutter and distractions from your business focus.**
- **Make sure your security system includes a means of preventing you from accessing malicious web pages.**
- **Also confirm that your security system is scanning attachments such as Word documents and PDFs for malware.**
- **Exercise caution when sharing media; have photos, videos, and sound files scanned before downloading.**

environment in which you won't need to recover your data. You accomplish that by having your data moved from your data center to a cloud-based data center.

The cloud has revolutionized data security and created a solution that wasn't available a decade ago. "It's backing up your data continuously, with versioning, up to some cloud-based service," Snyder says. "If you do these continuous cloud-based backups, that's a huge win." Remember that you may need a higher bandwidth uplink to execute this level of backup successfully.

DATA BACKUP SERVICES

Off-site backup is imperative if you house your data on your own hard drive or server. But even if you've migrated your data to the cloud, when it comes to data storage, redundancy is never a bad idea. That's where data backup services come in. For comparison-shopping purposes, here are a few to consider:

- **IDrive offers unlimited backup of PCs, Macs, iOS and Android phones and devices into a single account. Features also include point-in-time recovery and a web-based console that enables remote management of data backup and restoration.**
- **SpiderOak also offers remote data management, including the ability to share files with team members, and the ability to restore data to specified historic points.**
- **Carbonite offers plans for single and multiple computers or for one or more servers. Its plans can also be designed in compliance with regulatory requirements.**
- **Mozy touts its budget-friendly plans, which are available for personal, small business, or enterprise use.**

He adds this advice to business owners who are concerned about data vulnerability in the cloud: "Look at the risk of data loss—all the ways you can lose data and not be able to recover it—versus the risk of data theft from a cloud-based service. All these cloud-based services are built from the ground up to be more secure. They have good encryption. They have good authentication. If you balance these risks, the continuous cloud-based backup services are a huge win for small business owners."

For an extra measure of security and redundancy, you can also back up to an external hard drive.

TRACKING EMERGING THREATS AND NEW DATA PROTECTION OPTIONS

Data security is not a "one-and-done" element of business. New threats emerge all the time, and you need to stay on top of them. That said, "it's going to be very difficult for a small business owner or even a small business IT person to filter the information in a way that doesn't distract them from what's most important," Snyder says. "That's not to say they shouldn't try."

He recommends familiarizing yourself with the security bulletins and alerts offered by your operating system vendor and major application vendors.

Some examples:

- Microsoft's Security Help page provides links to news about the latest threats, information about "tech support" scams and trends, and protection, detection, and troubleshooting strategies.

- Adobe's Security Bulletin provides information on the latest updates and the security threats they address.

- Symantec's 2017 Internet Security Threat Report is the latest in its annual series. The company also publishes a Monthly Threat Report, hosts a library of white papers on Internet security topics, and maintains an A-Z database of viruses, worms, adware, Trojans, and other threats and risks.

- Apple's security support page covers such issues as account compromises and phishing. Resources also include the Apple Security Updates page and the iOS Security Guide.

ANTI-HACKING HACKS

✔ **Keep your system patched and your operating system upgraded. "What's absolutely incredible," Snyder says, "is that the top five to ten problems they find on people's PCs are inevitably things that were patched at least six months before."**

✔ **Maintain end-point security on your system, and keep it turned on. "That means some kind of anti-malware with scanning of attachments, scanning of URLs, looking for malware, and any other kinds of protection that are available from the tool," Snyder says.**

✔ **Make sure you have a full security suite that protects against the complete range of malware scanning and has fitering and blocking capabilities.**

CYBERSECURITY RESOURCES

Explore these online references to learn more about protecting your company, its data, and its reputation.

Hacking never takes a vacation or even a coffee break. But it doesn't have to keep you up at night. With the right information and preparation, your company can stand strong against cyber attacks and minimize the risks they pose to your business. These online resources can help you keep track of the threats and the best practices for avoiding becoming a victim of cybercrime.

BizTech Magazine: Joel Snyder article archive. Snyder writes for the magazine about networking, the digital workspace, the cloud, and data centers in addition to security. Among the security topics he has covered are:

- **5 Cybersecurity Priorities for Every SMB in 2017**
- **6 DNS [Domain Name System] Must-Do's for Protecting Your Networks in a Hostile World**
- **4 Tips to Give You Greater Network Visibility and Prepare You to Survive a Breach**
- **How to Fight Off Attacks from Inside the Network**
- **Staying One Step Ahead of Modern Hackers**

***Adobe*. The company provides advice and guides designed to enhance PDF security, including:**

- **Overview of Security in Acrobat and PDFs**
- **Enhanced Security Setting in PDFs**
- **Security Warnings When a PDF Opens**
- **Protect PDF Files with Permissions**

***Federal Bureau of Investigation*. As "the lead federal agency for investigating cyberattacks," the FBI publishes information and resources for individuals and business, including:**

- **What we investigate: Cybercrime**
- **Incidents of Ransomware on the Rise: Protect Yourself and Your Organization**
- **Ransomware: Latest Cyber Extortion Tool**

These strategies are designed to help you keep track of threats, remain aware of how cybercrime is evolving, and take steps to protect and ensure your uninterrupted access to your business data. But the benefits of engaging in these practices extend beyond keeping your system malware-free and your intellectual property available. The protections you create for your business also protect your vendors, partners, and customers—and so, by extension, your company's reputation.

By playing an active role in safeguarding your small business against the dangers of cyber threats, you foster increased trust and stronger relationships with all your company's stakeholders. This, in turn, positions you for competitive advantage, prospects for continued growth and expansion, and optimal productivity, profitability, and sustainable success.

COMING UP:
KEEPING DATA COVERED: CREATING A "BREACH-FREE" BUSINESS

Your company's reputation is its most precious asset, and once its customer or vendor data security is compromised, it can be difficult to reestablish trust. The best way to keep your customers' and vendors' confidence in your security plan is to avoid losing that confidence in the first place, and that means creating a comprehensive data policy and action plan.