The IT Insider

May 2018

IS YOUR CYBERPROTECTION UP TO DATE?

Security Alert! Hackers And Cybercriminals Are Now Concetrating Their Attacks On Your Business. Is Your Cyberprotection Up-To-Date?

Security protocols aren't a set-it and forget-it fix.

It's estimated that 978,000 new malware threats are released with each passing day.

Technology exists in a state of constant flux. The most popular gadgets turn obsolete within a year or two, the sophistication of the hardware and software we use increases exponentially with each passing month and the digital foundations of modern society are almost continuously supplanted. Every day, there's a new device to contend with, a fresh update and an addendum to the already dizzying array of features at our fingertips.

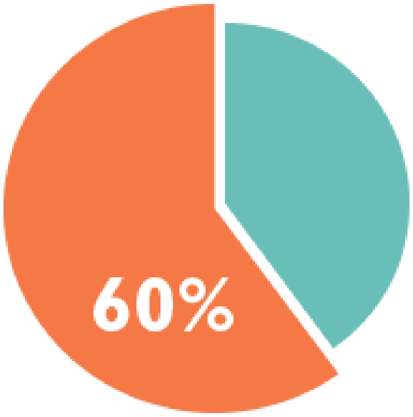
It's a thrilling world full of possibility and potential, but our dependence on these ever-changing technologies comes at a price. The overlay of the Internet on all aspects of our lives is fraught with vulnerabilities that criminals are eager to exploit. Though new protective measures are developed at the same breakneck speed as the software they guard, so are new ways to penetrate and circumvent these defenses. It's estimated that 978,000 new malware threats are released with each passing day. It's clear that "up-to-date" can no longer be an accurate descriptor; it always describes a system one step behind the newest development.

Today, cybercriminals are casting a wider net and catching more hapless victims than ever before. We read about the most costly of these breaches in the news each morning, including Equifax, J.P. Morgan, Home Depot, Yahoo!, Verizon, Uber and dozens more.

But these high-profile incidents don't even comprise the majority of attacks. According to Verizon's 2017 Data Breach Investigations Report, 61% of breaches occurred at small business, with half of the 28 million small businesses across the United States succumbing to a digital strike. Even scarier is the fact that UPS Capital reports that 60% of these businesses shut down within six months of a breach.

It's a bleak reality to come to terms with if you're a business owner. The truth is that it's almost a statistical certainty that hackers will come for your data, and when they do, they'll likely be using techniques nearly unrecognizable from today's malicious flavor of the month. How can you possible prepare for something that is constantly changing?

The answer is sustained attention, vigilance and resources directed toward protecting all that you've worked so hard to build. While it may be impossible to foresee exactly how hackers will try to penetrate your business, it's



UPS Capital reports that 60% of businesses shut down within six months of a breach.

well within the meansof most businesses to implement comprehensive security solutions to give your organization a fighting chance.

It’s vital to realize that, unfortunately, security protocols aren’t a set-it and forget-it proposition. To respond to the evasive and increasingly sophisticated tools being shared throughout the enormous hacker community, you need an equally sophisticated and regularly updating security system. For nearly every one of the 978,000 fresh new malwares developed daily, there are patches and updates designed to address them -- strategies and techniques to outsmart even the most devious of criminals.

Just because you don’t have the resources of a massive corporation doesn’t mean you need to be low-hanging fruit for well-funded and highly organized cybercrime rings. Hackers assume that a business like yours is too tiny and ill-informed to prepare for even a simple phishing scam, and they’re usually right. But if every business owner put just a little more effort into securing their data, you can bet attacks would be curbed. And if every small business pledged to implement a professionally managed security protocol, we would see frequency of these hacks diminish drastically.

There’s a lot for business owners to think about during a year as chaotic as 2018, but your top priority should be the basic security of your company. Invest your time and resources into building a foundational blockade for potential threats, and you can rest assured that your livelihood is safe from digital collapse.

A Brief History of Internet Security

As long as there has been an internet, there have been people who try to manipulate it. The bigger the Internet gets the higher risk it becomes for intrusions, phishing, viruses, worms, and fraud. While the internet as we know it today wasn’t really invented until the late 1980s, computers have been networked into a sort of “mini-internet” for a bit longer. The earliest network ‘hacks’ weren’t malicious in nature as we see them today. Instead, they were experiments or demonstrations to learn more about how computers spoke to one another. Then, we see a shift from education to recreation. Before it became a widespread and vicious criminal activity, it was often used for pranks. While mischievous, it wasn’t meant to do lasting harm. In fact, many hackers in the early 1990s hacked computers just to prove they were smart enough to do it.

AOL was the victim of the first widespread phishing attacks in the 1990s, which allowed hackers to steal usernames and passwords to the popular web portal. The 90s was also the birth of tracking cookies - the start of advertisers monitoring our website browsing behavior (it wasn’t invented by Facebook or Amazon!).

The 2000s is when we see cybercrime turn into a major criminal enterprise targeted at monetary gain. Security flaws are found in Microsoft computers and new worms are created to manipulate those flaws.

In 2007, smartphones were created. They weren’t much like we have today, but it was the start of the internet infiltrating everyone’s pockets. This ushered in a brand new era of privacy intrusion and snooping from everyone - police to jealous spouses.

Today, cybercrime is constantly in the news. It’s unavoidable. Cybercrime is so complicated and sophisticated that it is impossible to prevent. The emphasis is now on prevention and recovery instead of finding and reprimanding the criminals behind the crime. No one can prevent every accident, but we can control how we manage the aftermath. Every company, large and small, must be prepared (and practiced) in the disaster recovery response
process.

4 STEPS TO FINDING YOUR COMPANY'S DIAMONDS IN THE ROUGH

Executives are always looking to inject “fresh blood” into their teams. They're on the hunt for shiny new talent to be that secret ingredient their organizations are missing. Businesses should look internally for hidden, untapped assets within the company. Here are four steps to start uncovering your diamonds in the rough.

1. DON'T HIRE TO FIT A TITLE.

It may be the way business has been done for half a century, but that doesn't mean it's right. You need to look at the individual strengths of each candidate and determine if he or she is right for your company and culture. Make sure that you have a process in place to make hiring efficient. And as part of that process, take time to identify those creative and out-of-the-box individuals you already have on your team.

2. MINE FOR THE GEMS.

As you refine your hiring methods, you'll likely discover that the talent you're looking for might be right under your nose. Dig into your roster of existing team members. Create a company wide survey for those interested in taking on creative or challenging initiatives, and give them the opportunity to be considered. If you give them the opportunity to shine, they'll come forward.

3. REFINE AND POLISH.

Once you've identified your gems, spend some additional time with them. Find out what inspires and motivates them. You may decide to modify your team member's role or transfer some responsibilities to others in order to better utilize your talented individual's strengths and unleash their creative prowess.

4. FORMALIZE YOUR PROCESS TO FIND MORE GEMS.

This isn't a one-and-done process. It's important to meet regularly with people to find these hidden assets. Consider handing out surveys and holding brainstorming sessions regularly as part of your company culture. That way, new team members will come on board knowing there's an opportunity to shine in new ways, even if it's not what they were originally hired to do.

Focus on embracing and developing internal individuals with relevant skill sets before hiring. I guarantee there is a huge number of underutilized assets within your organization. Give them space to shine brightly.

PREFERRED IT SECURITY SPOTLIGHT

Two-factor authentication (2FA for short) is a system in which you must verify your identity in two separate ways to access an account. Sound confusing? It's not. Here's an example:

After enabling 2FA on a Gmail account, you have to enter your password each time you log in. Then you are asked to enter a six-digit code that you pull from your phone, a jump-drive sized key fob or a program on your computer.

Only then do you have access to your account. That way, if someone steals your password, they still can't get in.

If you aren't currently using two-factor authentication with your most sensitive data and systems, look into whether it might be an option. The extra 15 seconds it takes to pull up that second code is laughably short compared to the time you'd spend dealing with a hacked account.

At Preferred IT Group, we use a two-factor authentication software called Duo. It's so easy to use, and costs pennies. With Duo set up on our computers, we have an extra step in the morning.

Instead of logging directly into our computers as soon as we enter our password, Duo sends a message to our smartphone (or key fob, or a landline) and lets us know that someone is attempting to log into our account. We hit “yes that's me!” and we're ready to work.

If you'd like a demonstration of Duo, give us a call. We'd be happy to discuss the benefits of a little extra security with you.

Free Guide:
What Every Small-Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems

This report will outline in plain nontechnical English common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills, as well as providing an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Download your FREE copy today at http://www.preferreditgroup.com/protect or call our office at 260-440-7377.

PROTECT YOUR NETWORK

"What Every Business Owner Must Know About Protecting and Preserving Their Network"

Don't Trust Your Company's Critical Data And Operations To Just Anyone!

OUR COMMUNITY

Last weekend, we held our annual charity event. This year, we sponsored a golf scramble as well as a poker game. It was a gorgeous day outside, and our golfers had a blast.

Our very own Matt Hart won the poker game, and he, along with the second place winner Chad Tudor, generously donated their prizes back into the charity.

Over all, we raised about $5,000 for Children's Sanctuary!

Thank you to all of our sponsors, our silent auction donators, and every single person who participated in the event.

preferred IT group

CONTACT US

Fort Wayne **260.440.7377**	Warsaw **574.306.4288**
Columbia City **260.213.4266**	Indianapolis **317.426.8180**

www.preferreditgroup.com

6333 Constitution Drive
Fort Wayne, IN 46804

Subscribe to our blog and follow us on social media.