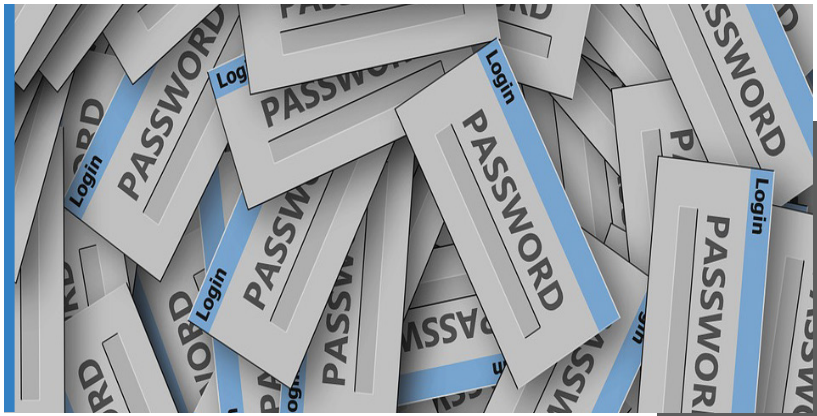
The IT Insider

March 2018

YOUR #1 HACKING THREAT IS INSIDE YOUR OWN ORGANIZATION. DO YOU KNOW WHO IT IS?

As technology advances, the number of potential cyber threats has increased exponentially. Average Joes simply cannot be bothered to keep up.



Make data security a priority among your team.

If your employees haven't been taught to identify threats, how could they possibly avoid them?

Every movie portrays hackers in pretty much the same way. When it comes to crunch time, they crack their knuckles, sit down at the keyboard, and begin tapping away at lightning speed. The timer is ticking down, the music reaches its peak of tension, but the hacker remains cool as a cucumber. Within seconds, they're in, they've "hacked the mainframe" and prompted high fives from their swarm of cohorts waiting in the wings with bated breath.

In reality, hackers are rarely up against some impenetrable digital fortress, digging into the passwords of a megacorporation or the US government. The vast majority of the time, they're nothing more than a ragtag group of bored criminals up against some unassuming small business. And more often than not, netting thousands of dollars from ordinary businesses just going about their day-to-day routines requires little coding at all, and certainly no "mainframe hacking." According to IBM's 2016 Cyber Security Intelligence Index, 60% of the time, all it takes is an unwitting insider to accidentally leave the company's digital front door wide open.

The Dangers Of Human Error

Cybercriminals may be experts in sniffing out the slightest vulnerability in your company's security, but a lot of the time, the data they need practically falls into their laps. Every day, internal e-mails are mistakenly addressed to the wrong people, sensitive info is inadvertently made public and employees unknowingly click on malicious links.

As technology has progressed, the number of potential threats has increased exponentially. Average Joes simply can't be bothered to keep up with hacking trends, and therefore are prone to opening your business up to cyber-attack by simply bumbling through their daily activities. If they've never been taught, how could they possibly know otherwise?

Digital Impostors

One of the easiest ways hackers can gain access to your business's valuable data is by posing as a trusted figure within your organization. This may sound complicated, but in today's world of social media and constant interactions through screens, it really isn't. Hackers can use data pulled from Facebook to either hijack the e-mail accounts and identities of employees or pretend to be them outright.

It's vital that you and your employees gain the knowledge you need to fight cybercrime.

After that, they can send peculiar requests to other members of your team. After all, if your CEO, Controller, or Office Manager sends you an urgent e-mail, you're probably going to open it. In many cases, by gaining access to a particular team member's credentials, hackers can bring down barriers and decrease the effectiveness of your security network, while staying completely invisible.

Smarten Up Your Team

No matter how comprehensive and powerful your cyber security software may be, it's not going to do much if an unsuspecting employee welcomes the bad guys into your network. With that in mind, it's vital that we provide specific training to our teams to truly make data security a priority.

But don't do this alone — after all, you're not the security expert. Instead, ask us (or your current provider) to equip you and your employees with the know-how to stave off digital attacks. We provide comprehensive services for you and your team, including:

- Giving employees a crash course on contemporary hacking strategies. You'll likely be shocked by how many of them don't even know what phishing is. During the training, we will provide specific examples of potential attacks - especially phishing - and how to avoid them.

- Putting systems in place empowering employees to alert the organization of vulnerabilities. For example, if John in manufacturing receives a suspicious e-mail, the entire company should be on the lookout within minutes.

- Teaching your employees that software updates and patches are more than just a nuisance, they're a necessity for up to-date security. When a new patch for a key program is released, we'll make sure your team knows it's available and that they shouldn't avoid installing it until later, and provide them with the tools to make it happen.

Cybercriminals are experts at what they do.

- Testing your team on what they've learned, such as sending out false suspicious e-mails containing shady links. If anybody fails the test, there's still work to do.

Your people are your greatest asset, but they can also be your biggest liability. In the modern world, it can feel impossible to protect yourself from data breach. Luckily, when it comes to your team, there's one potential avenue for hackers you can fix with a little perseverance.

Empower your employees.

4 BENEFITS OF A HYBRID CLOUD SOLUTION

A Hybrid Cloud Solution refers to having both an onsite backup device, and cloud storage in an off-site data center. This type of solution is commonly provided by a Managed Service Provider, which means that a small business does not have to bear the responsibility of maintaining and managing it. Typically, these types of solutions are paid for on a monthly or yearly subscription.

1. Superior Business Continuity
For small businesses, protecting your data is a must. Small businesses are more dependent on technology than ever before, and if they can't access their customer or operational data, they can't do business. Every minute of downtime costs you money. An extended period of downtime could put you out of business. With a hybrid backup, you can be assured that your valuable data is being backed up in two places – one inside your office, and one in a secure data center.

2. Adaptable Capacity
The amount of space you need for your data is not the same as your neighbor's. So why should you pay the same amount? Your on-premise device allows for virtualization, which means it can be adaptive and incrementally add capacity as needed. Off-premise storage can give you as much, or as little, space as you need, without forcing you to purchase an excessive capacity.

3. Optimized Pricing
Because you only pay for the amount of space you need, the cost of cloud-based storage is relatively cheap. With a month-to-month subscription, you can be sure you are only paying for what you use.

4. Confident Compliancy
If your business is subject to regulatory mandates such as HIPAA and PCI that require you to protect specified data from loss or corruption, retain specified records for a period of time, and document successful testing of your data recovery mechanisms – a hybrid cloud solution is perfect for you. A hybrid cloud backup, along with a proper managed service provider, will make sticking with these mandates headache-free.

PREFERRED IT SECURITY SPOTLIGHT

Protect Yourself From Cybercrime With These Questions

Cybercrime is at an all-time high, and it is only going to get worse. Every week, every month, new threats make themselves known. Unfortunately, there isn't a cure-all for these threats, but it is possible to stay ahead of the cybercriminals if you stay alert and pay attention.

Small businesses are the biggest target for cyber threats. Because small businesses are less likely to be secure than a large corporation, hackers can steal a ton of money by infiltrating hundreds of small businesses at once. "Small businesses typically have a moderate amount of data with minimal security. Hackers can use the stolen information to steal from many others."

Hackers won't only steal your money, either. They can steal customer data, employee details, and other private information. A data breach like this will cause your clients and your employees to lose your trust – it will damage your business relationships instantly.

Do you want to improve your cybersecurity? Ask yourself these questions:

1. Are your employees trained?
2. Do you have a password policy?
3. Are your workstations and devices updated?
4. Do you have two-factor authentication?
5. Do you have a disaster recovery plan?
6. Do you have a managed service provider?

Read more about this on our blog.

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

It's that time of year again! Our Charity Golf and Poker Event to benefit the local Children's Sanctuary is on May 5th - 6th.

Every year, we host a charity poker game with a silent auction of some pretty awesome items. This year, we've added a golf tournament, too!

Last year, we raised over $5,000 for local foster children and their families. We want to do even better this year.

Ticket sales are now OPEN!

Visit the website below for more info.
preferreditgroup.com/charity

Give Courtney at our office a call if you'd like to donate to our 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.