The IT Insider

1

December 2018

THE #1 THREAT TO YOUR SMALL BUSINESS IS INSIDE YOUR OFFICE

When disaster strikes, it's human nature to look for something or someone to blame. The world of cybersecurity is no different.

90% of all cyber claims stemmed from some type of human error or behavior.

You can do better. You just don't want to.

When disaster strikes, it's human nature to look for something or someone to blame. The world of cybersecurity is no different. Cybercriminals are everywhere and in high numbers. Given the opportunity, they can steal in five minutes what your company built over five years - and they won't even blink an eye. To them, this is their job, their lazy livelihood, and your company means nothing to them. While threat management tools like anti-virus and ransomware protection get more impressive every day, they still cannot account for one thing: human error.

90% of all cyber claims stemmed from some type of human error or behavior.

Crazy, right? Nope. Computers aren't infallible, but they are programmed to do exactly what we ask of them - which includes blocking hackers from directly infiltrating our systems. However, a computer can't make up for a human's mistakes or outright dumb choices. It's vitally important that people work with their threat management tools in order to keep their business safe.

Think of it like this: You wear a seatbelt when you sit in a car. It's not necessary to operate the vehicle - but it's an extra step you take for safety reasons, right? Adding this split second task to your morning commute is a habit, by now. Even if you've never been in an accident, and are a careful driver, you still wear your seatbelt. Why? Because one day it may save your life. You may go your entire life without ever getting into so much as a fender bender, but because you can't control other drivers, you're going to continue wearing that seatbelt every time you get into a car.

The same goes for protecting your business. The chances of getting a virus (or a more serious breach) are exponentially higher than that of getting into a car crash yet people still insist on practicing bad habits when it comes to cybersecurity. The truth is, you can do better. You just don't want to. Tough luck, my friend. Cybercrime is here to stay, and it's your responsibility

Half of your employees think it's not part of their job to keep your company's data secure.

to protect your business, your employees, and your customers.

It's necessary to preach the importance of hyper-vigilance to your employees (and yourself). What may seem like an unnecessary nuisance (like seatbelts in the '80s), could one day save you from massive fines or a life-ruining bad reputation.

In a recent survey, 8,000 employees were asked about their organizations' security policies. Only 12% of them said they "fully understood" them (I bet those were IT support staff). Plus, 24% of those 8,000 said they weren't aware of any security policies. An astounding 49% felt that security policies weren't their responsibility.

These are scary statistics. If half of your employees think it's not part of their job to keep your company's data secure, even if you have security policies in place - you're not protected in the slightest. If a quarter of them don't even know how to adhere to the policies or didn't even know about them to begin with - you're not protected in the slightest. It only takes one employee to make a mistake that could cost you your business.

Weak Password Security

This is something we see too much for comfort. Passwords are so easy to crack. Hackers merely need to set up a computer program to cycle through the most commonly used passwords (or even information like names and places the program finds on your social profiles) and BAM! They're in. Preferred IT Group has a strict password policy for our clients, but you can use the same policy for home and office.

At least 8 characters, 1 number, 1 symbol, and 1 capital letter. Rinse and repeat every 90 days.

It's even a good idea to pick a phrase and replace letters in the phrase with symbols or numbers. Preferred(1T)Gr0upRoCk$, for example. However, the most important thing to remember is that you cannot share this password with anyone.

Does Your Business Have a Disaster Recovery Plan?

What is your strategy for the aftermath of a terrible storm or aggressive ransomware attack? Likely, you have insurance on your building and your physical belongings like desks and computers and the coffee maker. But what about your data? What about the information stored on your server? Believe it or not, while the server itself may be covered by your insurance policy, everything it contains within its drives is not. For that, you need cyber insurance, which we do recommend, but even that won't help you recover lost data that you need to run your business. While a cyber insurance policy may provide a much-needed payout, it won't magically bring back all of those vital files, information, and software you need to run to your business every day.

For help crafting a disaster recovery plan within your business continuity plan, head over to preferreditgroup.com/thank-you-get-a-free-ebook/ and we'll give you our **Simplified Business Continuity Guide**.

Careless Handling of Data

This is another rampant problem. Your data = Your business. Without the information you store in your computers, you cannot run your business. You wouldn't have access to customer phone numbers, your payroll software, your orders, your emails. So why in the world would you put this data in unencrypted emails or Dropbox? Instead, keep this data as secure as you can. Make sure it's saved locally and in the cloud by using a hybrid backup system. Don't violate compliance laws by emailing sensitive information to inside or outside colleagues. If you wouldn't stand on a table in a busy airport and scream your data's content out into the crowd, don't put it places where unwelcome eyes can find it.

Inadequate Hardware or Software Security

When was the last time you updated your hardware or software? Are you consistently installing the most recent Microsoft patches and updates? Is your anti-virus or ransomware protection software on the latest version with the most recent defenses against the newest threats? If you aren't or don't know for sure - contact your IT support team and verifying. They should also be automating the updating process, too, so that you don't need to worry about it. This isn't an easy thing to keep track of - even your IT support team uses a software program to generate reports on the required updates and patches.

Low Security Awareness

What this entire article comes down to is low security awareness. You and/or your employees just don't know or remember the necessary security policies. This is where training comes in. It's vital that you train yourself and your employees on how to prevent cyberattacks. They need to become a 'human firewall'. Educate them on how to avoid phishing emails, creating solid passwords, and handling data properly. Small businesses are the biggest target for cyberattacks. Their employees aren't expected to follow strict security policies like, say, a hospital. Therefore, small businesses are much easier to attack. Stay one step ahead of cybercriminals. Adapt and stay educated.

With interactive and engaging training courses, we use our security awareness training to highlight common traps. This simultaneously allows us to tailor security policies to fit the needs of your company as well as educating specific employees on their weak points.

PREFERRED IT SECURITY SPOTLIGHT

What is cybercrime?

Cybercrime, at its most basic definition, is criminal activities carried out by means of computers or the internet. It is sometimes referred to as cyber attacks. It is constantly changing, just like technology, and is impossible to totally keep up with. By the time anti-virus software has been updated to include the newest virus attacks, cybercriminals have already moved on to something else.

The most common types of cybercrime are viruses and social engineering. We will discuss both in this guide, as well as ways to prevent them.

What is the purpose of cybercrime?

Typically, cybercriminals are after money. While there are the occasional chaos seekers and harassers, cybercrime is a booming business -- and there is plenty of money to be made in fraud and identity theft.

Who is the target for cybercrime?

We hear about big corporations becoming victims of cyber attacks in the news, but more than 80% of cybercrimes are committed against small businesses. Small businesses are easier targets because they are usually left unprotected (or have limited security). Plus, the cybercriminals are able to attack thousands of small businesses all at once with ease.

Want To Know For Sure If Your Data Is Safe?

Thanks to our Done-For-You Disaster Recovery you can rest assured that your data is being backed up in a format that is not only secure, but also easily recovered when you need it.

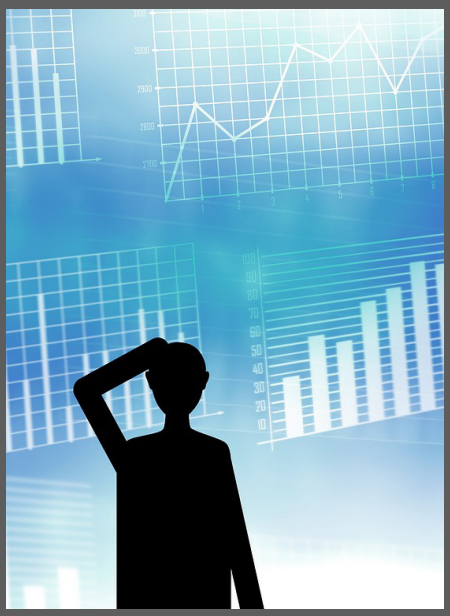
Your files are automatically backed up every hour locally and over the Internet.

Your data is safe from fire, floods, storms, viruses, hackers, hardware malfunctions, and human error! With image-based and file level backups, your data is immediately accessible even during a disaster.

Should a disaster occur, you can be back up and running the very same day…we **GUARANTEE** it.

Preferred IT Group will provide the hardware required, **absolutely free**.

Learn more at www.preferreditgroup.com/dfydr



OUR COMMUNITY

Help out a neighbor, and get put in our giveaway contest!

If you know of a business owner who have 10 or more employees in northeast Indiana in need of IT services, let us know!

Anyone you refer will receive a free Network Health Check (a $1,675 value), plus you'll get an Amazon gift card.

We'll also enter you to win our quarterly referral contest - this quarter the prize is an Rtic Cooler (filled with your favorite beverage)!

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.