The IT Insider

1

April 2019

4 DEADLY MISTAKES YOU'RE MAKING WITH IT SECURITY

Today, more and more businesses are switching over to a managed services model for their IT needs.

Find someone invested in your success.

Operate at peak efficiency!

For something so instrumental to the success of your business, technology can be an incredibly unstable, confusing and ever-changing tool. Just when you think you've got a handle on the latest cyber security trend, hackers find a way to circumvent the process completely. A new patch arrives for an essential piece of software, and the next day, another patch is required to repair the vulnerabilities the previous patch created. It can seem impossible to stay on top of the constant technological arms race,
much less stay relevant amid the exponentially increasing pace.

Today, more and more businesses are switching over to a managed services model for their IT needs. A managed services provider is a company that partners with businesses to proactively manage their networks inside and out. With MSPs, you get a full team of professionals who become intimately acquainted with the entirety of your IT structure, not only ensuring that problems are fixed long before they hit your bottom line but offering recommendations and tweaks to optimize processes and save time, money and headaches down the line.

By leaving your network up to an organization that takes the old break-fix approach, you're leaving the health of your entire business up to chance. Here are four ways the adage "If it ain't broke, don't fix it" is putting the security of your company in jeopardy.

1. YOU'RE BASICALLY PRAYING NOTHING EVER GOES WRONG.

The break-fix approach is pretty self-explanatory. The thinking goes that instead of shelling out a monthly fee for daily management of your network, you only pay your IT partners when a problem needs to be addressed. Typically, they're almost entirely hands-off until something goes wrong.

Certainly, this strategy saves money in the short term, but it will invariably come back to bite you

Better to stay one step ahead with an MSP by your side.

in the long term. Hiring a break-fix IT company is a bit like opting for the lowest level of insurance coverage. You may not fret about it now, but you definitely will when an accident happens and you're forced to pour thousands of dollars into repairs. And sadly, the threat of your business being hacked is actually greater than the chances you'll be in a serious car accident!

2. YOU'RE LEAVING HOLES IN YOUR DEFENSES.

Today's tech world is a constant game of whack-a-mole, with security experts frantically hammering down on every digital threat that rears its ugly head. For the entirety of your security structure to be equipped with the latest and greatest, it takes a team of genuine experts keeping an eye on your systems and ensuring everything is up to snuff.

With a break-fix approach, it's likely you don't detect flaws in your system until long after they've already been exploited, costing you dearly. And it's important to remember that every data breach has the potential to be utterly catastrophic, doing so much damage that it can close down your business for good. Better to stay one step ahead with an MSP by your side.

3. YOU'RE OPENING YOURSELF UP TO COSTLY SERVER DOWNTIME.

When the very survival of your business depends upon staying online and serving your customers, every minute your network is down – your assets are locked down behind ransomware or your tech is fried to the point that you're at a standstill – is a minute that you cannot afford. According to Gartner, the average cost of IT downtime is a whopping $5,600 per minute, and that doesn't even factor in disgruntled clients or missed communications.

The top priority of your IT infrastructure should be to prevent downtime from ever occurring, not to minimize the amount of downtime you suffer when something goes wrong.

4. YOU AREN'T OPERATING AT PEAK EFFICIENCY.

One of the most insidious costs of the break-fix approach doesn't have anything to do with your network breaking down. It chips away at your bottom line gradually and silently, without causing much of a fuss.

Without a proactive eye on your systems, chances are you aren't implementing the processes and software that keep everything working at its highest potential. You'll be using clunky workarounds to simple problems without even realizing you're doing it. The seconds you waste on Internet bottlenecks will add up over time, especially when multiplied by your entire company.

The fact is, the break-fix model of doing business is, ironically, broken. Consider partnering with an MSP and invest in the long-term future of your company.

Top Tips To Prevent Cybercriminals From Hacking Your Network

1. PLAN FOR THE WORST. Though it's vital to invest in prevention, you shouldn't focus all your efforts on preventing an attack, because one might occur despite your preparations. Be braced to respond to an incident with a detailed plan.

2. EDUCATE YOUR TEAM. According to the Ponemon Institute, only half of companies surveyed felt that current employee training adequately reduced noncompliant security behaviors. Most cyberbreaches originate from a simple mistake, so training your team is an essential early step.

3. MAKE A BUDGET THAT REFLECTS YOUR PRIORITIES. Best practices are easy to preach at the beginning, but in order to keep strengthening your barriers and staying abreast of cyber security trends, you need to build regular cyber security actions into your yearlong plans. This means that security should be a permanent, substantial item in any budget you develop. SmallBizTrends.com, 11/20/2018

PILOTLESS PLANES ARE ON THEIR WAY — BUT WOULD YOU EVER FLY IN ONE?

Last January, Airbus CTO Grazia Vittadini stated the company is hopeful that, soon, advancements in artificial intelligence will allow for autonomous planes to take to the skies. This would mean lower pilot costs, fewer pilot shortages and, eventually, cheaper flights for consumers. The question is, can airlines persuade passengers to get in a sealed sky-tube six miles in the air piloted by a machine? Maybe after cargo planes start to go autonomous, we'll be convinced, but for now, that prospect seems more than a little iffy. DigitalTrends.com, 1/20/2019

PREFERRED IT SECURITY SPOTLIGHT

Imagine you're walking down the street, out of the corner of your eye you catch a glimpse of a small shadowy figure. As you get closer you recognize its form. It's a duck…. That's right a duck. A harmless little duck. However this little duck has an attitude and he wants your money.

You think over your options and decide… this is just one duck, how tough could it be? The thought of fighting a duck may have never crossed your mind, however now that it has, you may be thinking of all the possibilities of you possibly getting hurt from this one little duck. Chances are, you could probably fight off one duck….but what about 100,000 ducks at the same time?

This scenario is similar to what happened to Dyn. A company responsible for 1000's of businesses' online resources. As a major playing in the online DNS and hosting scene, Dyn has become a popular hot spot for attacks. But it wasn't until October of 2016, that they were humbled by the smaller attackers.

A massive botnet consisting of over 100,000 device began attacking Dyn's network services. Over the course of several hours, major websites that rely on Dyn's network started crashing. Sites like, Etsy, Github, Spotify, and Twitter suffered service interruptions or went offline altogether. Dyn's team of highly skilled IT personnel were able to restore order, but the damage had been done.

It is important to pick providers online that can mitigate these kinds of attacks. Research your options, ask questions, and don't be afraid to put them on the spot. Some important questions to ask could be things like; "What is your data encryption technology?" or "What certifications for data protection do you have?" or "How much control of my data do I have vs. you?" In the end, it may be better to partner with a technology provider that can ask them the tough questions and pick the right cloud hosting provider for you.

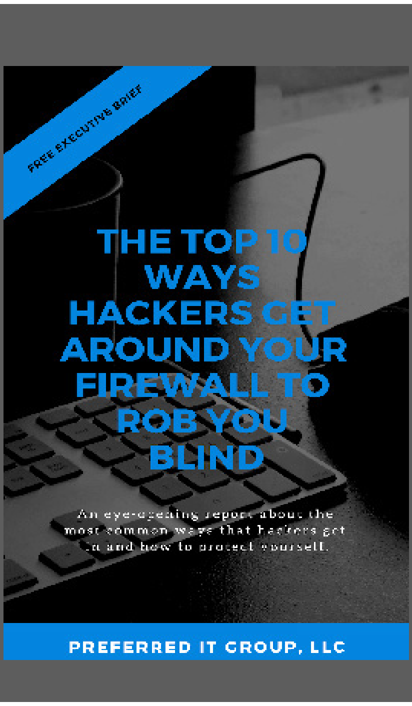
The Top 10 Ways Hackers Get Around Your Firewall to Rob You Blind

Cybercrime is at an all-time high, and hackers are setting their sights on small and medium businesses who are “low hanging fruit.” Don’t be their next victim!

This report reveals the most common ways that hackers get in and how to protect yourself today.

The shocking facts about why small business are the #1 target of cybercriminals - more than half of the reported cyber attacks are focused on small business for this one main reason that is easily fixed.

Get this free report at preferreditgroup.com/10ways



FREE EXECUTIVE BRIEF

THE TOP 10 WAYS HACKERS GET AROUND YOUR FIREWALL TO ROB YOU BLIND

An eye-opening report about the most common ways that hackers get in and how to protect yourself.

PREFERRED IT GROUP, LLC

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	Warsaw
260.440.7377	574.306.4288
Columbia City	Indianapolis
260.213.4266	317.426.8180

www.preferreditgroup.com

6333 Constitution Drive
Fort Wayne, IN 46804

Subscribe to our blog and follow us on social media.