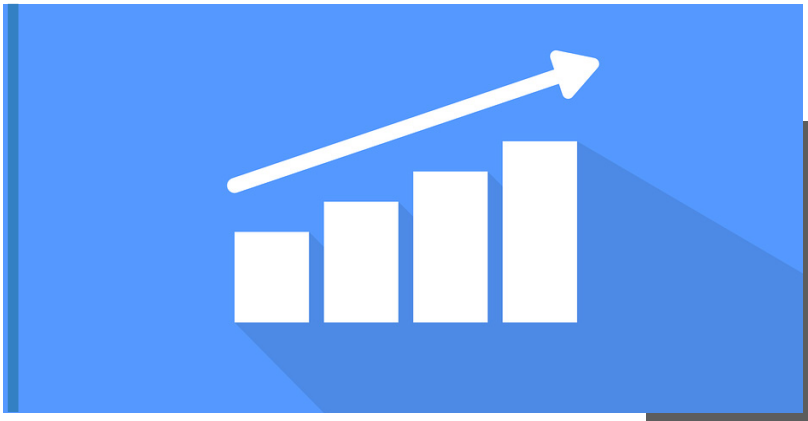
The IT Insider

1

March 2019

3 IT INVESTMENTS YOU SHOULD NEVER SKIMP ON

Small and medium sized businesses are skimping on technology costs where they shouldn't, cutting corners wherever possible and, as a result, leaving themselves open to a huge variety of potential disasters.



Don't assume you're the "little guy" and there's no reason for hackers to target you. SMBs are the single biggest target.

Avoid the pitfalls of our technology-dependent world.

There's a disturbing trend underlying the business world's increased reliance on technology. No, we're not about to decry technology itself. Nor will we downplay the endless list of ways in which tech has enhanced business owners' ability to reach more prospects, build meaningful relationships with clients and make the previously labyrinthine tasks of yesterday seem positively mundane today. There's no denying that the Internet age has empowered companies of all sizes to do incredible things and that technology is forever transforming the way we do business. Today's savvy businesses are intertwined to an unprecedented extent with the technology they use.

But there's a problem that goes along with this increased dependence. Despite the inextricable relationship today's companies have with IT, the vast majority of them – SMBs in particular – are neglecting key aspects of their tech. They're skimping where they shouldn't, cutting corners wherever possible and, as a result, leaving themselves open to a huge variety of potential disasters.

To avoid the pitfalls of our technology-dependent world, it's important to ensure you have a firm IT foundation. Here are three IT investments where you should avoid underspending or risk shuttering your business forever.

1. CYBER SECURITY

Across the tech industry, it has practically become trendy to point out how woefully underprepared SMBs are for modern crime. But it's true: according to the 2016 State of Cyber Security in Small and Medium-Sized Businesses report, a full 50% of all U.S. small businesses succumbed to cyber-attacks in 2015, a statistic that is rising and shows no sign of slowing down. Most small business owners assume that since they're the "little guy," there's no reason why a well-equipped and highly trained team of hackers would ever target their meager stores of data. But, in fact, it's these hapless businesses that end up being the low-hanging fruit for these operations. Millions upon millions of dollars are stolen from SMBs each year, and most of it is gleaned via vicious ransomware.

2. PROACTIVE TECH SUPPORT

It's probably easy to imagine how a vicious cyber-attack could leave your business reeling, but there are equal-

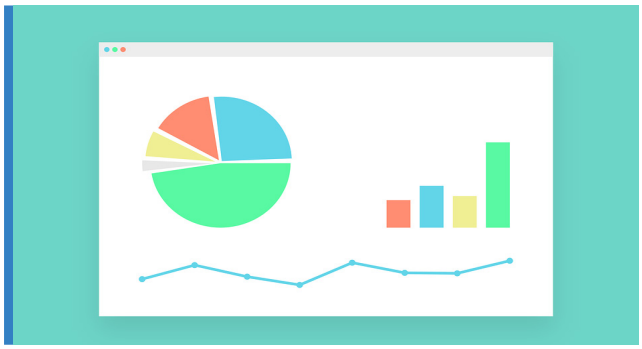
> 73% of businesses have had some type of operations interruption in the past five years, causing a staggering $70 million loss. The vast majority of these interruptions are avoidable.

equally insidious risks that could cost your business big-time. Consider server failure, for example. No matter the caliber of equipment you're dealing with, failure is an inevitable risk of technology. But instead of being proactive, most business owners just assume that downtime is a fact of the modern world. As a result, 73% of businesses have had some type of operations interruption in the past five years, causing a staggering $70 million loss, according to an infographic published in VentureBeat. The worst part? The vast majority of these outages are avoidable.

The fact is that a cheap "break-fix" technology technician is only there to put out fires, not to proactively prepare your business for success. By the time your break-fix IT guy shows up on the scene, the damage will already be done. This results in dramatically lowered efficiency and potentially thousands of dollars in lost sales – not to mention the cost of all those customers you lost while you were off dealing with a tech crisis. And that's only one example. Finicky software, stuttering computers and lost backups may seem like small issues until you're in the midst of disaster and the costs are adding up. It's better to avoid these catastrophes in the first place.

3 TECH STRATEGIES TO BEAT THE COMPETITION

Technology isn't just a crutch we use to make navigating the marketplace easier; it can equip us with a set of tools that allow us to actively surpass customer expectations and streamline our efficiency, lowering expenses and empowering our employees. You can bet on the fact that your competition is doing everything it possibly can to stay abreast of the latest technological trends. Don't let them pull ahead. Instead, invest in strategies and software that will trim away precious seconds from inefficient processes and enable you to focus on what really matters: making your business succeed.



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**.

3 Ways Your Employees Will Invite Hackers Into Your Network

No matter how professional they are, members of your team, yourself included, are going to make mistakes. They may unknowingly bumble into the cyber-attack that forces your business to go belly-up for good. In the majority of cases, that will be by design. There's a saying in the cybersecurity industry, coined by renowned cryptographer Bruce Schneier: "Only amateurs attack machines; professionals target people."

This strategy works disturbingly well, but how does it happen? There are three primary causes of employee-related breaches, each of them contributing to a sizable portion of hacks across the country.

1. Social Engineering

Phishing remains one of the most prominent strategies deployed by hackers to lift data from small and midsized businesses. The majority of these attacks stem from an employee clicking on a suspicious link that is embedded in an absolutely convincing email. To lure your team into the trap, cybercriminals often use data gathered from cursory investigations of your organization from the Internet or social media. Maybe they pose as a security expert contracting with your company or a member of a customer support team behind one of your employee's personal devices. Whatever mask they wear, it doesn't take much to convince an uninformed employee to click on these links, resulting in a high success rate for phishing attacks.

2. Circumvented or Incorrectly Implemented Security Measures

Even if you do everything you can to protect your business from digital attack, your team may just dodge those measures anyway. According to a recent report by cybersecurity firm Dtex Systems, around 95% of companies have employees who will attempt to override previously implemented security processes. And that's if te security measures are configured, patched, and installed properly in the first place. The IBM X-Force report lists "misconfigured cloud servers and networked backup incidents" among chief concerns of last year.

3. Insiders With Malicious Intent

Hell hath no fury like an employee scorned. A strikingly large number of breaches come not from error at all, but from insidious tactics by disgruntled employees or undercover criminals looking to make a quick buck. It's not quite a "you can't trust anyone" scenario, but there are definitely folks out there who would sell your business right out from under your noise.

With each of these in mind, it's vital that you incorporate extensive employee training and vetting protocols to maximize their cyber security know-how. In addition, you need to implement safe practices that reduce the room for human error, alert employees when something is amiss, and protect them from the worst.

PREFERRED IT SECURITY SPOTLIGHT

Your Data Is Safer In The Cloud

The reverberating impact that natural disasters have on the community is not as clear as the immediate physical damage. This is never truer than it is with the small businesses in the areas.

Far too often, this kind of catastrophic loss of data due to physical damage of servers, firewalls, and computers will shut a business down for good. A 2010 report by technology research firm Gartner Group stated that 43% of businesses went belly-up almost immediately after a "major loss" of data, while 51% shut down within two years. That leaves a measly 6% survival rate for businesses that suffer company-wide data loss.

Those numbers aren't great, but you can prepare yourself for this kind of disaster. Just like you pay for flood insurance in hurricane-heavy areas, you've got to preemptively protect your business data, too. Any business that migrates their data to the cloud is significantly less likely to lose that data. This isn't just because a cloud service provider typically backs up your data several times a day, and in several different places, but also because the cloud data centers are actually more secure than their onsite counterparts. There are always, always backups.

Even after all this, the cloud isn't a fit for every single business. Some business models need onsite structures for a variety of reasons. Some find it cheaper. But, it is better to do your research and understand the cloud as a potential option for your company. It could save your business.

Read more tips like this on our blog!

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

OUR COMMUNITY

The Fourth Annual Charity Event hosted by Preferred IT Group for the Children's Sanctuary is fast approaching and tickets are available now!

If you'd like to help local foster children have a fantastic year, join us for a round of golf and a poker game May 18-19! As always, our silent auction is held online and in-person at the event.

Tickets are available at preferreditgroup.com/charity.

We can't wait to see you there!

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.