Central Texas Technology Solutions
Your Business Partner

Technology Monthly Newsletter
April 2019

Now is the Time For Microsoft 365

You know that your business's growth depends on everyone delivering their best work, and that means enabling your staff with the collaboration tools they need.

At the same time, you must protect your business's vital information, while ensuring your team can access the files and data they need as they work. Now, for the first time, Microsoft is offering an integrated solution that brings together the productivity of Office 365 with the security of Windows 10.

This cost-effective, subscription-based cloud service is built especially for small and midsize businesses like yours. It empowers your team to be productive every day with Office 365, no matter their locations. Your technology needs are taken care of so you can focus on your core business, with the peace of mind that your data is protected, and employees can collaborate, communicate and grow your business. Call us today to schedule a time to learn how Microsoft 365 can benefit your business.

This monthly publication provided courtesy of CTTS, Inc.

What Is Managed IT Services… And Why Should You Demand It From Your IT Services Company?

In today's constantly shifting technological landscape, where fresh viruses and the new security patches designed to protect against them arrive by the week, it takes a proactive approach to stay abreast of all the changes. This is why, in 2019, more small to midsize businesses (SMBs) are ditching their outdated break-fix strategies and making the switch to a managed services provider (MSP) for their IT needs.

But for those of us still coming to terms with the new rapid-fire reality of business in the digital age, it can be difficult to determine which approach is right for your organization, or even what a managed services provider actually does.

Here's a breakdown of the managed services strategy versus the traditional break-fix approach and how it applies to your business.

Managed Services Are Designed For Up-To-The-Minute It Upkeep.

Maintaining the integrity, efficiency and security of your business network is a little like taking care of your car. You don't buy the equipment with the expectation that it'll be good to go forever; you know that it'll take regular upkeep to stay in tip-top shape. For a car, of course, that means regular oil changes, rotating the tires, checking the alignment, checking and replacing the fluids, ensuring adequate tire pressure, changing your spark plugs, flushing the transmission – the list goes on and on. If you don't bother with basic preventative maintenance of your vehicle, it'll fail you sooner rather than later. We're guessing most of our readers wouldn't drive 20,000 miles without checking the oil, for instance. Many of these tasks can be taken care of with some savvy and time investment, but others require the expertise of a seasoned

professional, especially when serious problems arise.

It's the same with your network. Business technology is notoriously finicky. It'll work perfectly for months and, in rare cases, for years – until suddenly it doesn't, at which point it's likely too late. Suddenly all your data is locked down behind some nasty new ransomware, or your server decided to give up the ghost without warning, leaving key customer information swinging in the wind. We constantly hear about Fortune 500 companies shelling out millions for high-profile data breaches, but when these attacks come to SMBs, they often fold the company completely. What was once a thriving small business is now an empty storefront, buried under the never-ending progress of modern technology.

The old break-fix approach to IT management attempts to address the digital risks facing SMBs only after problems arise. Is your server down? Is malware giving you a headache? Is your e-mail not working for some reason?

> **"You don't buy the equipment with the expectation that it'll be good to go forever; you know that it'll take regular upkeep..."**

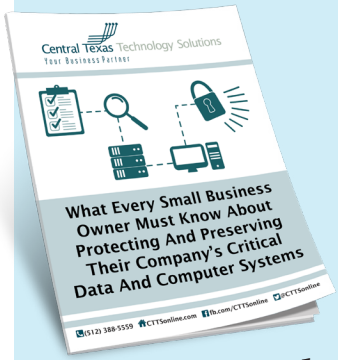
If so, they're on the scene. Otherwise, they're hands-off. The idea behind this strategy is the classic adage "If it ain't broke, don't fix it." Business owners look to cut costs on IT by only addressing the most serious technological crises after they've already happened, rather than shelling out funds for regular preventative maintenance.

Unfortunately, just like how this approach doesn't make sense in the context of your car, it certainly doesn't make sense for your network. A break-fix strategy can save money in the short term, sure, but it results in more network downtime, a much higher frequency of issues and a ton of dollars spent on damage control down the line.

Instead, you should demand that the IT professionals responsible for the backbone of your business provide managed services. This means they're in the guts of your network every day, mastering and locking down every aspect of your technology long before anything goes wrong. They'll detect issues before they cost you money and fix them without hesitation. You might balk at the initial subscription fee, but if you run the numbers, you'll quickly see how much money it will save you in the long run.

An investment in an MSP is an investment in the future of your business. You wouldn't drive your car mindlessly until it breaks down; it's arguably even more dangerous to do the same with your network. Take a proactive approach, demand managed services and breathe a sigh of relief knowing your network is in the hands of professionals well-versed in the ins and outs of your business's specific needs.

Free Report: 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 the common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills, and will provide an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Download your FREE copy today at www.CTTSonline.com/Protect or call our office at (512) 388-5559.

Credential Stuffing Attack: What is it and How to Stay Protected?

A credential stuffing attack is a type of cyberattack where cybercriminals take username-password combinations leaked on other sites to gain illegal access to user accounts.

Attackers attempt to use the stolen set of credentials against multiple websites in order to compromise and take full control of user accounts. The stolen credentials are then leaked at other sites or sold at underground forums and hackers try to brute-force those credentials into various other sites in an attempt to gain unauthorized access to the user account.

Attackers also attempt to use the breached credentials against multiple websites in order to compromise and take full control of user accounts.

In order to stay protected from credential stuffing attacks, it is best to never reuse the same passwords across multiple sites. It always recommended to use unique passwords for each account and periodically rotate passwords. It is further recommended to use strong, complex, and unique passwords that are difficult to crack.

90% of the businesses we search have stolen credentials on the Dark Web! Call us right away to see if your organization is at risk!

5 Ways To Answer Questions Like A CEO

In my work as a consultant, I've had the privilege of posing questions to over 1,000 business leaders. As a result, I've been on the receiving end of many great answers from some of the most respected CEOs on the planet.

Unfortunately, I've also heard answers from less-skilled managers. There are key differences between both. Here are five ways to answer questions like a CEO:

1 Answer a yes-or-no question with a "yes" or "no" before you provide details.

Does John Thomas work at Google?

Bad Answer: "John Thomas? I knew him back at the University of Michigan. He and I were in the same engineering lab. This one time …"

Great Answer: "Yes. He works at Google now. We went to college together, and we're Facebook friends."

2 Answer a number question with a number answer before you provide details.

How much did your sales decline during the last recession in '08?

Bad Answer: "The Great Recession was a really hard time for us. It felt like we were running a marathon in quicksand. No matter what we did …"

Great Answer: "Twenty percent. Fortunately, the compensation of our team was largely variable, so we all made a bit less income during that period and avoided layoffs."

3 Say what your goal was, what you did and what the results were.

What happened in that job?

Bad Answer: "Well, it was in the South. I was not used to the South. Wow, were the summers humid. And the mosquitoes? Big as birds …"

Great Answer: "My mission was to set up a new food bank in Atlanta. The goal was to recruit 20 restaurant partners, hire the first five employees and serve 100 meals a day within three months. Things moved a little more slowly than I was used to, so I had to get creative. We hired a video crew, interviewed restaurant managers and customers and gave free social media advertising to the restaurants if they signed up with us. This allowed us to achieve our goals a month earlier than planned, and my bosses were thrilled!"

4 Answer from the other person's point of view.

Why do you want me to invest in your ice cream stores?

Bad Answer: "Because we need the capital to grow."

Great Answer: "Because 10% return on invested capital is what you say you want, and that is what we have delivered reliably on a per-store basis for over 50 years."

5 Share just enough information to prove your point, but not more.

Why should we buy from your company?

Bad Answer: "For starters, here's our 150-page brochure, a 25-page PowerPoint slide deck and a dozen customer cases about some companies that are nothing like you, as well as a bunch of random anecdotes – whatever comes to mind!"

Great Answer: "Three reasons: 1) Gartner group did a survey of our industry and rated us #1 in the three areas that are most important to you. 2) We know this space better than anybody. Our team published the #1 book on this topic, both in sales and review ratings on Amazon. 3) We offer a 100% money-back guarantee."

Geoff Smart is chairman and founder of ghSMART. Geoff is co-author, with his colleague Randy Street, of the New York Times best-selling book, Who: A Method For Hiring, and the author of the #1 Wall Street Journal best seller, Leadocracy: Hiring More Great Leaders (Like You) Into Government. Geoff co-created the Topgrading brand of talent management. He is the founder of two 501(c)(3) nonprofit organizations. SMARTKids Leadership Program™ provides 10 years of leadership tutoring and the Leaders Initiative™ seeks to deploy society's greatest leaders into government. Geoff earned a BA in economics with honors from Northwestern University, and an MA and Ph. D in psychology from Claremont Graduate University.

The #1 Way Hackers Access Your Network

(And How To Prevent It From Happening)

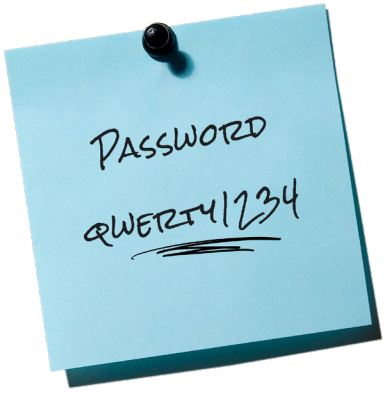
It's easy to imagine the hackers attacking your network as a team of computer masterminds. But in reality, the vast majority of data breaches don't occur from some genius hacking into the mainframe.

According to Trace Security, a full 81% of breaches happen as a result of poorly constructed passwords.

Luckily, avoiding this is pretty simple: Ensure every member of your team uses strong passwords!

Here's How:

1. Passwords should be over eight characters in length, comprised of letters, numbers and symbols.
2. Avoid using obvious personal information like addresses and family names.
3. Start using a password manager.



4. Avoid the common, obvious passwords like "123456789" or "password."
5. Change your password every 60-90 days.

You also might consider implementing two-factor authentication in your system, which is several degrees of magnitude more secure than ordinary passwords, but it can be a headache to set up without an expert on your team.

You can always call CTTS for any password security questions you may have. We are your local IT Support Team! (512) 388-5559.

There Is One Thing That Separates Successful People From Everyone Else

Steve Jobs was a notoriously exacting boss. He constantly held himself to the highest standards of business and creativity and drove himself, and those around him, to greatness. But in his own words, one of his greatest strengths wasn't the quality of his mind, but his strength of belief. As he put it, "You can't connect the dots looking forward; you can only connect them looking backward. So, you have to trust that the dots will somehow connect in your future. You have to trust in something – your gut, destiny, life, karma, whatever. This approach has never let me down, and it has made all the difference in my life."

Of course, he's talking about faith in your own ability to make things work. Being confident in your own abilities, according to Jobs, is one of the biggest secrets to success.

Did you miss it?

Check Out This Month's Top Tech Tip:

Tech Tip #114: Protect Your Laptop On The Go

You'll want to read this tech tip if you work remotely or bring your laptop along while traveling. Protecting your laptop with a password is not enough to prevent an attacker from accessing your files. In Tech Tip #114, we go over 3 actionable steps you can take to increase your laptop security.

By Josh Wilmoth

Read it Here: http://bit.ly/Tech-Tip-114