Creative Resources Technology Group

"Insider Tech Tips and Strategies at Your Fingertips"

This Issue's Must-Reads:

What is Managed IT Services? | page 1

Free Report: The Business Guide To Ransomware | page 2

Perfect In Every Way! | page 3

5 Ways To Answer Questions Like A CEO | page 3

Tech Tip of the Month | page 3

#1 Way Hackers Access Your Network | page 4

There Is One Thing That Separates Successful People From Everyone Else | page 4

3 Costly Myths | page 4

April 2019

This monthly publication provided courtesy of Russell Poucher, President of Creative Resources Technology Group.

Our Mission: To make technology work seamlessly with your business and to work for you, not against you. As the leading Apple Consultant in Orange, Riverside, and San Diego County, we pledge to always provide innovative solutions that meets your specific business needs, superior customer service, and expert strategies on how to leverage IT to build your business. Don't worry, we got IT.

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 This is why, in 2019, more small to midsize businesses (SMBs) are ditching their outdated break-fix strategies and making the switch to a managed services provider (MSP) for their IT needs.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

Continued on pg.2

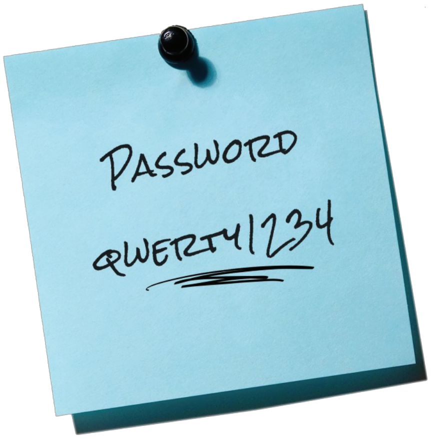
Continued from pg.1

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? 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.

> **"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 … "**



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 beforeanything 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: The Business Guide to Ransomware: Be Prepared

The Business Guide to Ransomware: Everything to Know to Keep Your Company Afloat

Organizations of all types and sizes have been impacted by ransomware, but small businesses can be particularly vulnerable to attacks. Today's ransom seekers play dirty and ransomware is constantly evolving. This report will explain everything you need to know about ransomware and how to protect you and your businesses.

Provided by: Creative Resources Technology Group
3555 Harbor Gateway S Suite B
Costa Mesa, CA 92626
(714) 881-8000

More and more, ransomware has emerge as a major threat to individuals and businesses alike. Ransomware, a type of malware that encrypts data on infected systems, has become a lucrative option for cyber extortionists. When the malware is run, it locks victims' files and allows criminals to demand payment to release them.

In this e-book, you'll learn how the malware is spread, the different types of ransomware proliferating today, and what you can do to avoid or recover from an attack. Hiding your head in the sand won't work, because today's ransom seekers play dirty. Make sure your organization is prepared.

Download your free copy at: http://bit.ly/2V4GoPO

What Our Clients Have to Say:

"Perfect in every way!"

Creative Resources designed and installed every aspect of our multi-location integrated system to manage our diverse business activities. We have high value investment assets and were handicapped by inadequate IT. Creative Resources did everything we could have wanted in a highly professional manner.
We now have a thoroughly integrated system where every aspect fits exactly the need we explained at the outset. They now maintain the system and are immediately responsive and 100% effective. I have no affiliation with them except as a client, but I say hire them!

Barry Meguiar
Founder
Revival Outside the Walls

We don't like to brag but check out what our clients have to say about us here:

www.creativeresources.net/our-clients

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."

Tech Tip of the Month

We're all guilty of it: connecting to free public WiFi. Whether it's at the coffee shop, hotel, or airport - the temptation to check e-mail and surf the web is just too strong to resist. So BEFORE you connect to any free, public WiFi, make sure the connection is legitimate.

PRO TIP: NEVER access financial, medical, or sensitive data while on public WiFi. Also, don't shop online and enter your credit card information unless you're absolutely certain the connection point you're on is secure. It's not uncommon for hackers to set up fake clones of public WiFi access points to try and get you to connect to THEIR WiFi.

Want to stay on top of the latest IT updates? Sign up for our Security Tip of the Week here: *www.creativeresources.net/tech-tip-sign-up*

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, over eight characters in length and comprised of letters, numbers and symbols. Keep the numbers and symbols away from each other, and definitely avoid the common, obvious passwords like "123456789" or "password." 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.
SmallBizTrends.com, 1/3/2019

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 not talking about faith in some divine purpose; he's talking about faith in your own ability to make things work. Instead of developing some "perfect" master plan where every detail is accounted for, we always have to work with imperfect information and step into uncharted territory. Being comfortable with this, according to Jobs, is one of the biggest secrets to success.
Inc.com, 1/2/2019

If your server suddenly crashed and all of your data was erased, how long would it take before your business was back up and running as usual? Just because you've been lucky enough to avoid an accident like this doesn't mean you're not as risk. Here are 3 costly myths most businesses have about data backup.

1. Believing that tape backups are a reliable way to secure your data. Tape backups have an average failure rate of 100%. What makes this even worse is that tape backups will appear to be working, giving you a false sense of security.
2. Relying on an inexpensive, automated online backup provider to backup your company data. Tread carefully here and make sure you've really done your homework on your chosen solution. Make sure you have the option to have your initial backup performed through a hard copy, your database files can be stored and recovered easily, and demand daily status updates because any reputable backup service will send you a daily report to verify everything is backed up.
3. Trusting your backup is automatically working without doing periodic test restores. We see this happening a lot - more times than we can count where businesses believe their backups are working because they don't see any error messages or apparent problems. Then, when they need to restore a file (or entire server), they discover the backups stopped working months ago and all that data is gone.

Not sure if you have your backups configured properly? Contact us for a **FREE Network Assessment** at *www.creativeresources.net/freenetworkassessment*