PALMTECH
I.T. Solutions For Business

THE LEGAL TECH TIMES

PalmTech Computer Solutions April 2019

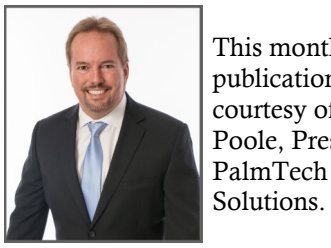
PalmTech's Cybersecurity Breakfast Seminar

"9 Critical IT Security Protections Every Business Must Have In Place NOW To Avoid Cyber Attacks, Data Breach Lawsuits, Bank Fraud and Compliance Penalties"

Meet me for breakfast at one of our two upcoming cyber security seminars!

Visit here for details!

www.palmtech.net/events/



This monthly publication provided courtesy of Chuck Poole, President of PalmTech Computer Solutions.

Our Mission

To equip small and midsized businesses in the West Palm Beach area with a smooth running and seamless IT platform that enhances productivity, improves efficiency, and creates a competitive advantage.

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 This is why, in 2019, more small to midsize businesses (SMBs) are ditching their outdated break-fix strategies and making the switch to a managed services provider (MSP) for their IT needs.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

continued on page 2

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? 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.

> **"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 ... "**

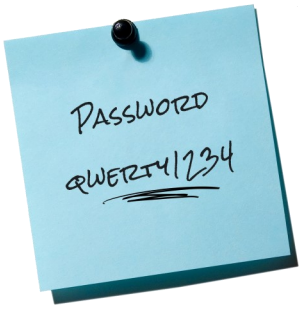
Unfortunately, just like how this approach doesn't make sense in the context of your car, it certainly doesn't make sense for your network. A break-fix strategy can save money in the short term, sure, but it results in more network downtime, a much higher frequency of issues and a ton of dollars spent 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. Contact us for more information on our managed services at (561)969-1616.

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

Work Smarter In Outlook With These Tips

People are constantly searching for an easier way to keep their email inboxes in order, customize their email signatures, and improve group communications. The good news is that Microsoft Outlook has these features built in, you just need to know where to look.

Clean Up your inbox

No matter how meticulously organized your Outlook inbox is, there's always room for improvement. For a little computer-assisted help, try the 'Clean Up' feature.

From your Inbox, click the Home tab and choose from Outlook's three Clean Up options:

- Clean Up Conversation – Reviews an email thread or a conversation and deletes redundant text.
- Clean Up Folder – Reviews conversations in a selected folder and deletes redundant messages.
- Clean Up Folder & Subfolders – Reviews all messages in a selected folder and any subfolders, and deletes redundant messages in all of them.

Ignore (unnecessary) conversations

An overstuffed inbox is often caused by group conversations that aren't relevant to you. The Ignore button helps you organize your inbox and focus on relevant emails.

- Select a message, then click Home > Ignore > Ignore Conversation. You can also do this by opening a message in a new window and clicking Ignore under the Delete function. To recover an ignored message, go to the Deleted Items folder, and click Ignore > Stop Ignoring Conversation.

Send links instead of a file copy

Help your colleagues save storage space by sending a link to a cloud version of a file instead of the file itself. This is particularly useful when sending massive files. You can also set permissions to allow recipients to edit and collaborate on linked files in real time.

- Upload the file you wish to send on OneDrive and send it to your recipients. From the message box, click Attach File > Browse web locations > OneDrive.

Improve meetings with Skype and OneNote

Outlook allows you to combine Skype's HD video and screen-sharing features with OneNote's organizational and project planning functions. It's easy:

- Go to the Meeting tab in Outlook, then click Skype meeting and send the link to the participants. After the meeting has started, select Meeting Notes (under the Meeting tab) and choose whether you want to Take notes on your own or Share notes with the meeting.

Tag contacts

To get the attention of a specific person in a group email message, use the @Mention function. This works particularly well for emails sent to multiple recipients or if you simply want to convey the urgency of your message.

- In the email body or meeting request, type the '@' symbol followed by the first and last name of the person you wish to tag (e.g., @firstnamelastname).
- To search for emails you're tagged in, select Filter Email from the Home tab and choose Mentioned, then choose Mentioned.

These are just a few strategies for getting more out of Microsoft's email platform. To unlock Outlook's true potential, you need the support of certified IT professionals. Give us a call today at (561)969-1616.

Published with permission from TechAdvisory.org. Source.

Every Business Needs An MSP For Cybersecurity

Businesses can no longer afford to relegate cybersecurity to the bottom of the budget, not with cyberattacks targeting any business regardless of size, strict security, and privacy regulations surrounding data. Businesses with a small or limited budget have the advantage of partnering with a managed IT services provider (MSP) for their cybersecurity needs. Why is this need more urgent than ever, and why is an MSP the intelligent business choice?

The Numbers

According to the Ponemon Institute's 2018 State of Cybersecurity in Small & Medium Size Businesses (SMBs) survey, cyber attacks on SMBs have increased from 61 percent in 2017 to 67 percent in 2018. Only 28 percent of these SMBs evaluated their ability to mitigate threats, vulnerabilities, and attacks as highly effective. 58 percent of SMBs in the study experienced a data breach in the last year.

Most SMBs in Ponemon's research said attacks against their companies had severe financial consequences. For instance, the report cited that many of them spent an average of $1.43 million because of the damage or breach of IT resources, a 33 percent increase from 2017. Disruption to operations also cost an average of $1.56 million, a 25 percent increase from 2017.

The Attacks

So what types of cyberattacks on SMBs were prevalent last 2018? According to the study, the order from most to least common are as follows: phishing/social engineering, web-based attacks, general malware, compromised/stolen devices, denial of services, advanced malware/zero day attacks, SQL injection, malicious insider, cross-site scripting, and uncategorized attacks.

Why Managed Services?

Partnering with MSPs is the most effective way to prevent attacks and protect your business from these malicious threats. They include a full range of proactive IT support that focuses on advanced security, such as around the clock monitoring, data encryption and backup, real-time threat prevention and elimination, network and firewall protection, security awareness training, and more.
Not only that, but because managed services are designed to identify and fix weak spots in your IT infrastructure, you'll optimize the digital backbone of your business processes. You'll have faster network performance, a business continuity and disaster recovery strategy, as well as minimal downtime. One of the best things about managed services is that you get a dedicated team of IT professionals ready to assist you for any technology problems you may encounter. This is much more effective and budget-friendly than having in-house personnel handling all your IT issues.

Being proactive when it comes to cybersecurity is the only way to protect what you've worked hard to build. If you'd like to know more about how managed services can benefit your business, just give us a call, we're sure to help.

Published with permission from TechAdvisory.org. Source.

Are Your Credentials For Sale On The Dark Web?

Visit
www.palmtech.net/darkweb/
For A Free Scan!