TECHNOLOGY BYTES

Insider Tips to Make Your Business Run Faster, Easier & Be More Profitable

"As a business owner, you don't have time to waste on technical and operational issues. That's where we shine! A true professional IT support team you can count on, available 24/7."

- Doug Johnson, CyberTrust IT Solutions
Contact us on:- (949) 396 1100

This Thanksgiving

Want To Feel Thankful Instead Of Frustrated With Your Computers?

● Know More on Page.2

What's Inside

4 Questions Your IT Service Provider Should Be Able To Say "Yes" To

Out with the old and in with the new! For far too long, small businesses have taken an old-school approach to IT services and security. In other words, they wait until something goes wrong before they call an IT services Provider and request help.

Back in the day (think 1990s and 2000s), this approach worked, more or less. External threats, such as hackers and viruses, were still few and far between. A data breach wasn't on anyone's mind. So, it made sense to wait until something went wrong before taking action.

In IT circles, this is known as the "break-fix" approach. Something breaks, so someone has to come in to fix it. And they charge for their services accordingly. If something small breaks and it takes a short time to fix, you could expect a smaller bill. If something big breaks, well, you can expect a pretty hefty bill.

The break-fix approach is 100% reactive. As many businesses have learned, especially in more recent years, as the number of threats have skyrocketed, it can get very expensive. IT services are in demand field. With just about every business relying on the Internet and Internet-connected devices in order to operate, there's a lot of opportunity for something to go wrong.

This is exactly why you can't rely on the reactive break-fix model anymore. If you do, you could be putting your business at serious risk. In some cases, the mounting costs and damages done could put you out of business.

If you're hit by a data breach or if a hacker infiltrates your network (which is a common occurrence), what's next? You call your IT service provider.

If you have a partner and tell them you need help, they might be able to restore lost or stolen data. That is, if you routinely backed up that data. You don't want to find yourself in this position. And you don't have to.

Instead, take a proactive approach to your IT support and security. This is the new way of doing things! It's also known as managed services and it's a far cry from the break-fix approach.

If you work with an IT services provider that only comes out when something breaks, it's time to get them on the phone to ask them four big questions. These are questions they absolutely need to say "yes" to.

1. Can you monitor our network and devices for threats 24/7?
2. Can you access my network remotely to provide on-the-spot IT support to my team?
3. Can you make sure all our data is backed up AND secure?
4. Can you keep our network protected with up-to-date malware solutions, firewalls and web filtering?

If your IT services partner says "no" to any or all of these questions, it might be time to look for a new IT services partner.

"When things go wrong, and these days, things will go wrong, you'll be left with the bill – and be left wishing you had been more proactive!."

If they say "yes" (or, even better, give you an emphatic "yes"), it's time to reevaluate your relationship with this company. You want to tell them you're ready to take a proactive approach to your IT support, and you'll be happy to have them onboard.

Far too many small businesses don't bother with proactive support because they don't like the ongoing cost (think of it as a subscription for ongoing support and security).

They would rather pay for things as they break. But these break-fix services are more expensive than ever before. When things go wrong, and these days, things will go wrong, you'll be left with the bill and be left wishing you had been more proactive!

Don't be that person. Make the call and tell your IT services provider you want proactive protection for your business. Ask them how they can help and how you can work together to avoid disaster!

Want To Feel Thankful Instead Of Frustrated With Your Computers?

3"Techie" Reasons You Can Be Thankful This Season

1. Cyber Thieves Keep A-Knockin' But They Can't Come In. Having the proper firewall and office network security tools can prevent even the most determined cyber hacker from getting his hands on your network. Are your systems covered?

2. Downtime Should Be A Thing Of The Past. Thanks to monitoring and maintenance tools that are openly available, any reputable computer company can now actually notice when things go awry and prevent your computers from having issues.

3. If Disaster Strikes, You Can Be Back Up & Running In Minutes Instead Of Days. Many businesses' operations would be completely down for days or weeks if a major disaster like fire, flood or theft ever occurred. Here's where Backup & Disaster Recovery solutions (BDR) can help you feel very thankful indeed.

Call us before November 30 for a FREE Problem Prevention Network Audit (a $497 value) that will help eliminate problems on your network and give you peace of mind.

Give us a call today at
(949) 396 1100 or request your audit online at:
www.CyberTrust-IT.com

Shiny New Gadget Of The Month:

Arlo Pro 3 Floodlight Camera

In the era of porch pirates, more people are investing in outdoor security cameras. The Arlo Pro 3 Floodlight Camera delivers security and practicality. It features an ultrahigh-definition camera delivering 2K HDR video and color night vision combined with a 2000 lumens light. Nothing goes undetected!

Plus, the Arlo Pro 3 is wireless. It connects to WiFi and doesn't need a power cord (it just needs to be plugged in for charging periodically). Because it's on WiFi, you can check the feed anytime from your smartphone. You can even customize notifications so you're alerted when it detects a car or person. And it has a speaker and microphone so you can hear and talk to anyone near the camera. Learn more at:

Arlo.com/en-us/products/arlo-pro-3-floodlight.aspx

4 Steps To Move Your Business From Defense To Offense During Times Of Disruption

"Everyone has a plan until they get punched in the mouth." –Mike Tyson

As business leaders, we've all been punched in the mouth recently. What's your new game plan? Since COVID-19, the annual or quarterly one you had is now likely irrelevant.

You have two options:

1. Sit and wait for the world to go back to the way it was, a place where your plan may have worked (and let's face it, that's not happening).

2. Create and act upon a new game plan. One that's built to overcome disruption and transform your business into something better and stronger.

Option Two is the correct answer! AND, we at Petra Coach can help.

At Petra Coach, we help companies across the globe create and execute plans to propel their teams and businesses forward. When disruption hit, we created a new system of planning that focuses on identifying your business's short-term strengths, weaknesses, opportunities and threats and then creates an actionable 30-, 60- and 90-day plan around those findings.

It's our DSRO pivot planning process. DSRO stands for Defense, Stabilize, Reset and Offense. It's a four-step process for mitigating loss in your business and planning for intentional action that will ensure your business overcomes the disruption and prepares for the upturn better and stronger than before.

Here's a shallow dive into what it looks like. Defense: A powerful offensive strategy that hinges on a strong defense. Identify actionable safeguards you can put in place. The right safeguards act as the backbone of your company, giving you a foundation you can count on.

Stabilize: The secret to stabilization is relentless communication with everyone. That includes internally with your teams AND externally with your customers.

Streamline communication and eliminate bottlenecks through a visual dashboard.

Reset: By completing the first two steps, you'll gain the freedom to re-prioritize and focus your efforts on the most viable opportunities for growth.

Offense: Don't leave your cards in the hands of fate. Shifting to offense mode gives you the power to define the future of your business. Equip yourself with the tools and knowledge to outlast any storm.

Interested in a deep dive where a certified business coach will take you (and up to three members from your team) through this process? Attend Petra's DSRO pivot planning half-day virtual group workshop. (We've never offered this format to non-members. During this disruptive time, we've opened up our coaching sessions to the public. Don't miss out!)

Quick Tip

BE CAREFUL
What You Post Online
DON'T Be An Easy Target

When you call a time-out and take in this session, you'll leave with:

- An actionable game plan for the next 30, 60 and 90 days with associated and assigned KPIs;
- Effective meeting rhythms that will ensure alignment and accountability;
- Essential and tested communication protocols to ensure your plan is acted upon.

I'll leave you with this statement from top leadership thinker, John C. Maxwell. It's a quote that always rings true, but is crystal clear in today's landscape: "Change is inevitable. Growth is optional."

Let that sink in.

Is Working From An Office More Secure Than Working Remotely?

It may come as a surprise, but working remotely can be just as (or more) secure than working in the office, if done right.

Those are the three operative words: if done right. This takes effort on the part of both the business and the remote employee. Here are a few MUST-HAVES for a secure work-from-home experience:

Secure networks. This is non-negotiable. Every remote employee should be connecting to a secure network (at home, it should be WPA2 encrypted), and they should be doing so with a VPN.

Secure devices. All devices used for work should be equipped with endpoint security antivirus, anti-malware, anti-ransomware and firewall protection. Employees also only use employee provided or approved devices for work-related activity.

Secure passwords. If employees need to log in to employer-issued programs, strong passwords that are routinely updated should be required. Of course, strong passwords should be the norm across the board. Entrepreneur, June 17, 2020

Top Tips On How To Prevent Your Smart Cameras From Being Hacked

Smart cameras have been under attack from hackers for years. In fact, one popular smart camera system (the Amazon Ring) had a security flaw that allowed hackers to get into homeowners' networks. That issue has since been patched, but the risk of being hacked still exists. Here are three ways to keep your camera (and your network) safe from hackers:

1. Regularly update your passwords. Yes, passwords. This includes your smart camera password, your WiFi network password, your Amazon password, you name it. Changing your passwords every three months is an excellent way to stay secure. Every password should be long and complicated.

2. Say no to sharing. Never share your smart camera's login info with anybody. If you need to share access with someone (such as a family member or roommate), many smart camera systems let you add a "shared user." This will let them access the camera, without the ability to access the camera's configuration or network tools.

3. Connect the camera to a SECURE network. Your smart camera should only be connected to a secure WPA2 encrypted, firewalled WiFi network. The more protection you put between the camera and the rest of the digital world, the better. Digital Trends, May 7, 2020.