NOVEMBER 2020

InTech Intelligencer

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

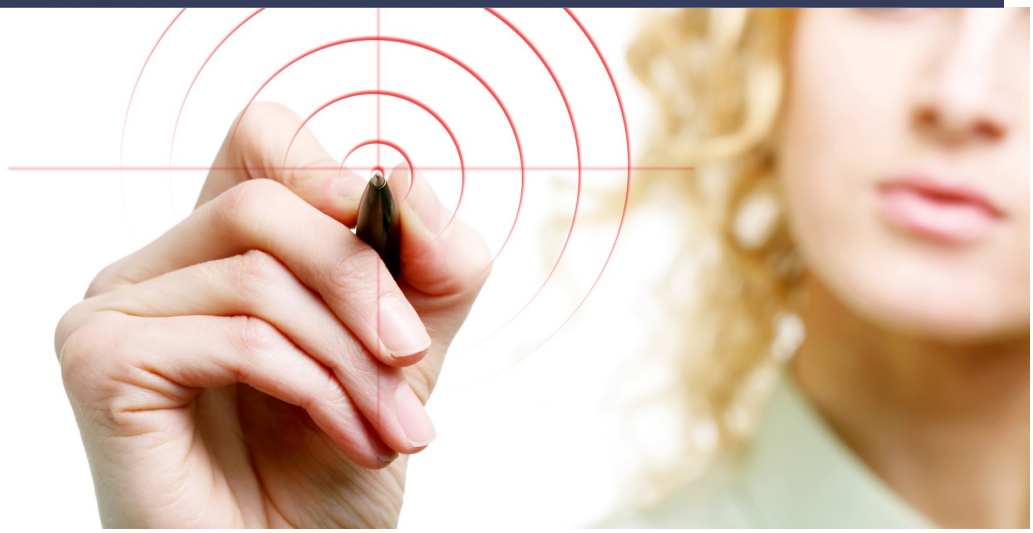
"As a business owner, you don't have time to waste on technical and issues. That's where we *shine*! Call us and put an end to your IT problems finally and forever!"

- Leia Shilobod,
President & I.T. Princess of Power

Inside This Issue…

InTech SOLUTIONS

One Northgate Sq., Ste. 202
Greensburg, PA 15601
724.235.8750



4 Questions Your IT Services Company 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 company 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 specialists are an 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 services partner – 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.

Continued on pg.2

Continued from pg.1

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 company 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!

Call today to schedule a Cyber Security Risk Assessment for your business. 724.235.8750 or email Leia@intechit.net.

Free Report Download:
Questions You Should Ask Any IT "Expert" Before Letting Them Touch Your Network

How can you tell if you are going to receive poor or substandard service? How do you know if your computer guy or network consultant is doing everything possible to secure your network from downtime, viruses, data loss or other frustrating and expensive disasters? Could your current provider actually be jeopardizing your network?

This valuable Free Report helps you avoid common pitfalls of choosing an IT Provider. Download yours today!

Claim Your FREE Copy Today at www.intechit.net/whattoask

Shiny New Gadget Of

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!)

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.

Andy Bailey is the founder, CEO and lead business coach at Petra, an organization dedicated to helping business owners across the world achieve levels of success they never thought possible. With personal experience founding an Inc. 500 multimillion-dollar company that he then sold and exited, Bailey founded Petra to pass on the principles and practices he learned along the way. As his clients can attest, he can cut through organizational BS faster than a hot knife through butter.

Need NIST 800-171/DFARS Compliance?

For businesses in the DoD Supply Chain who need to comply with DFARS/ NIST 800-171 Security Protocols, InTech provides Risk Assessments, Security Audits, Compliance Audits, Plans of Action, and Remediation to bring YOU into compliance and assure you keep your contracts. Start the process today with a free, no obligation survey to get an idea of what you need to do to come into compliance. Go to **www.intechit.net/NISTassessment** and take just 5 minutes to jump start compliance.

Who Else Wants To Win A $25 Gift Card?

You can be the Grand Prize Winner of this month's Trivia Challenge Quiz! Just be the first person to correctly answer this month's trivia question and receive a $25 Visa gift card Ready?

What do we call a collection of two or more computers that are located within a limited distance of each other and that are connected to each other directly or indirectly?

A) Internet
B) Interanet
C) Local Area Network
D) Wide Area Network

Email us right now with your answer!
info@intechit.net

InTech SOLUTIONS
One Northgate Sq., Ste. 202
Greensburg, PA 15601

US POSTAGE
PAID
GREENSBURG, PA
PERMIT NO. 1117

- RETURN SERVICE REQUESTED—

"Why Do They Do It? The People You Call Hackers Are Criminals, Pure And Simple "

Too often a client or prospect complains when I tell them we are going to need to invest more in a security tool, or change a business process to keep them secure. "Why do we have to do this stuff? Why do I have to spend this money. I don't think I need it."

Well, yes. You do. If you want to keep your business safe, your livelihood intact, and your employees in their jobs.

"This is just ridiculous. I don't understand why people do these things. It's a burden on my company." If I had a dollar for every time I held a conversation like this I could close up shop and live a pretty comfortable life.

So let me spare you the pleading with me or another IT person that the world should be different: the reason you have to take cyber security seriously is because cyber crime is run by CRIMINALS who are in the BUSINESS of taking your hard earned money.

Before you ask me WHY again, please remember that in the whole course of human history there have ALWAYS been criminals, the "bad guys." They used to creep up behind you in dark alleys or hijack trains or airplanes, but you get your hands dirty that way. Its much easier to buy a piece of software or hire a malicious actor for rent and have money pour in from behind the comfort of your computer screen.

Every time you move, they find ways to counter-move. That's why you need to take the total security of your company seriously: physical security, cyber security, and personnel security (anyone reading this do drug tests or background checks?).

Now I'm certainly not suggesting you spastically buy up all the newest cyber security tools and services you can. Its important to approach your investment with a solid plan, based on **the assessed risk your business has against attacks, your risk tolerance, and of course, your budget.**

I recently spoke at IUP's Cyber Security Symposium on "How To Choose A Security Vendor or Product Without Getting Fleeced" and put together a handy checklist to use in your assessment. Grab a copy for yourself here: **http://www.intechit.net/cyber-threat-assessment**. Stay secure out there!

To Your Success,

Leia

Leia Shilobod, CEO of InTech Solutions, Author and Cyber Security Advisor.