two river™
TECHNOLOGY TIMES
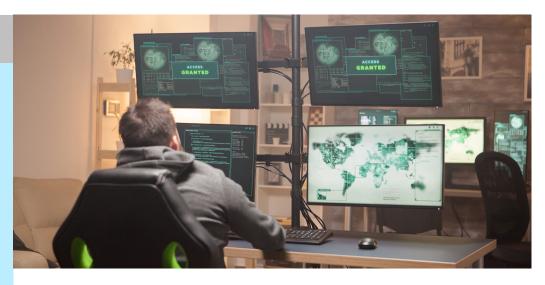
June 2020

This monthly publication provided courtesy of Frank M. DeBenedetto, President of TRTG.

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

Making This One Mistake With Your Network Can DESTROY Your Business

A lot of businesses wait until something breaks before they fix it. And even then, they may take a "patchwork" approach to fixing the problem. They are reactive rather than proactive. Sometimes taking a reactive approach is fine, but other times, and depending on the circumstances, it can lead to even bigger problems.

When it comes to network security, for example, being reactive to problems can be downright dangerous. It's not just hackers you have to worry about. There are power outages, data loss, equipment failure and more. In IT, a lot can go wrong. But if you're proactive about cyber security, you can avoid many of those pitfalls.

Reactive IT support used to be the norm. Most network security specialists went to work after something went wrong. Unfortunately, some businesses still have this reactive mindset when it comes to their IT and network security. They have an "it won't happen to me" attitude. The truth is that these are the people most at risk. It's not a matter of if, but when. Hackers and cybercriminals are more active than ever.

Thankfully, proactive support is now the norm. More and more IT services and security firms have the tools and resources to protect you BEFORE the worst happens. So, why partner with an IT services company?

There are many reasons why it's a good idea. One great reason that doesn't often get talked about is that working with an IT services company is an added value for your customers. When they know you're

taking IT security seriously – and when they know their data is safe – their trust in you is boosted.

When you build trust, you build loyalty, and customer loyalty is getting harder to come by these days. Plus, happy, loyal customers are much more likely to refer you to others who may be in need of your services. That alone makes investing in proactive IT security worth it.

Here's another reason why working with a proactive IT services firm makes sense: it's MUCH easier than trying to do it yourself. Many small businesses simply don't have the resources to hire an internal IT specialist or a team. Not only can 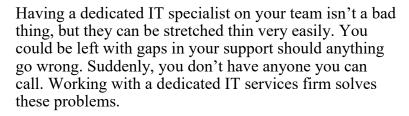that be very costly, but it's also rarely practical. Think of it this way: if you hire an IT specialist to handle your network security, manage cloud backups and provide general IT support, then what happens when they take a day off or take a vacation?

> **"Unfortunately, some businesses still have this reactive mindset when it comes to their IT and network security."**

Having a dedicated IT specialist on your team isn't a bad thing, but they can be stretched thin very easily. You could be left with gaps in your support should anything go wrong. Suddenly, you don't have anyone you can call. Working with a dedicated IT services firm solves these problems.

To take that a step further, good IT services companies are also great at catching problems before they become problems. They can catch things that might not have even been on your radar. For example, if your cloud backup service isn't backing up your data correctly or is backing up the wrong data, they'll catch that. Maybe you're saving data that's not properly encrypted. They'll catch that. Maybe you have an employee using software that's months out-of-date. Again, they'll catch that.

When you call up an IT services company and say you want to take a proactive approach to your network security, they should be willing and able to provide just that. An experienced firm will have a team with the training, certification and experience required to tackle today's cyberthreats while managing your network's day-to-day needs.

They know IT because they live IT. They help with data recovery should anything go wrong; they are your help desk when you have questions or concerns and they keep your on-site malware protection up-to-date. They are tailored to your business's specific needs. And as you grow, they adapt to your changing needs.

Put an end to the outdated way of thinking about IT security. It's time to be proactive and to recognize your company's vulnerabilities before they become vulnerabilities. You just have to make the call.

Shiny New Gadget Of The Month:

The Many Faces Of Corporate Leaders

Employees' happiness at work is more important in the workforce than ever before, and that feeling of fulfillment and engagement often comes from the top. If you are aware of what type of leader you are and how your leadership affects employees and clients, you can mitigate your weaknesses and discover your strengths to ultimately lead more effectively. Let's take a look at a few leadership personas I've witnessed while coaching and what works best for each.

In-The-Weeds Leaders
Leaders who are "in the weeds" tend to spend too much time in the day-to-day. They get bogged down with what's in front of them and don't think outside the box. Without innovation, the company runs the risk of coming to a grinding halt.

These leaders need to delegate current tasks to their team members. They can then focus on finding new ways to drive the business forward. In-the-weeds leaders may even need an outside party to hold them accountable for setting and reaching these new goals.

Frustrated Leaders
These leaders know their companies can be better, but they're upset because they can't scale at the rate they want. They bottle up their grievances and aren't sure where the disconnect is with their teams.

These leaders could seek guidance from a third party, whether that's a friend or colleague. An outside perspective can help identify problem areas. They also need to hear out their team members and get firsthand accounts on what's not working. Both perspectives can help turn frustration into focus.

Mindful Leaders
These leaders recognize that rapid growth is positive as long as they scale appropriately with formal organization and efficient processes. They are careful to avoid pushing forward blindly and losing essential parts of their culture and

values along the way. However, they may take too long to think things through and miss new opportunities that come along because they couldn't act quickly enough.

These leaders should make sure they are sticking to the systems they have in place while remaining open to new opportunities and evaluating them in a timely manner. It's important to constantly reevaluate and adapt as the company grows and changes shape.

Control Freaks
These leaders can't seem to let go of the wheel. They micromanage and don't trust their team to get the job done, which fosters an atmosphere of frustration and mistrust. In this atmosphere, they can no longer lead effectively.

They should work with their teams to identify why the company exists, what motivates team members and why their work is important. That will not only help the leader and the team establish a better dynamic, but it will also help them both understand where the company is now and where it's going.

When evaluating your leadership style, be honest with yourself. If you can pinpoint where you are on the leadership spectrum, then you'll better account for your challenges and capitalize on your assets. And that's how you become more self-aware and, in turn, a much stronger leader.

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.

How to foil ransomware

Not too long ago, the CryptoLocker ransomware virus was all over the news, infecting over 250,000 computers in its first 100 days of release (at least that's the number reported – the real numbers are probably MUCH higher). The threat was fairly straightforward: Pay us or we'll delete all your data.

Ransomware, like the CryptoLocker attack, works by encrypting your files to prevent you from using or accessing them. After your files are compromised, the hackers behind the attack then pop up a demand screen asking for payment ($400 to $2,000) within a set time frame (e.g., 72 hours or three days) in order to get the key to decrypt your files. The last CryptoLocker virus forced many business owners to lose data or pay up since there was no other way to decrypt the files.

Obviously the best way to foil a ransomware attack is to be incredibly diligent about IT security; but with hundreds of thousands of new attacks being created daily, there are no guarantees that you won't get infected. Therefore, it's critical to maintain a full, daily backup of your data OFF-SITE so that IF you do get whacked with ransomware, you can recover all your files without having to pay a thin dime; and don't forget to back up off-site PCs, laptops, remote offices and third-party software data stored in cloud apps as well!

Don't send your private information to anyone!

We're seeing a new variant of an old scam. Here's what happens: a secretary gets an e-mail from her boss – who is traveling – to please send him, as soon as possible, scanned copies of all the W2s the company issued at the end of January. The message appears to come from her manager, including having what looks like his actual e-mail address when she looks at in

Outlook. She gets suspicious – she has just talked to her boss on the phone that morning, and he never mentioned needing that information. Before she collects the W2 PDFs that are on the HR drive, she decides to text her boss and check on it. Great catch! The boss never requested that information. Had she not been proactive and instead just completed the task assigned to her, she would have given a scammer all of the confidential information that is on a federal W2 form for every employee in her firm! The scammer likely would have used the information to commit identity theft and/or file false returns next year to claim the refund.

Always be vigilant and proactive – it's better to be suspicious and double-check everything when dealing with confidential information. Try to provide that detail in an encrypted e-mail, or at minimum with a password on the files (and don't include the password in the body of the e-mail!). The few extra minutes it takes could save months of heartache for all of your employees

How to spot a phishing e-mail

A phishing e-mail is a bogus e-mail that is carefully designed to look like a legitimate request (or attached file) from a site you trust in an effort to get you to willingly give up your login information to a particular website or to click and download a virus.

Often these e-mails look 100% legitimate and show up in the form of a PDF (scanned document) or a UPS or FedEx tracking number, bank letter, Facebook alert, bank notification, etc. That's what makes these so dangerous – they LOOK exactly like a legitimate e-mail. So how can you tell a phishing e-mail from a legitimate one? Here are a few telltale signs…

First, hover over the URL in the e-mail (but DON'T CLICK!) to see the ACTUAL website you'll be directed

to. If there's a mismatched or suspicious URL, delete the e-mail immediately. In fact, it's a good practice to just go to the site direct (typing it into your browser) rather than clicking on the link to get to a particular site. Another telltale sign is poor grammar and spelling errors. Another warning sign is that the e-mail is asking you to "verify" or "validate" your login or asking for personal information. Why would your bank need you to verify your account number? They should already have that information. And finally, if the offer seems too good to be true, it probably is.

Don't just throw out that old computer

Getting rid of old computers or servers? Did you know that the components used in technology equipment are not landfill-safe? On top of the environmental hazards, unprotected e-waste typically contains a lot of confidential and private information in the form of saved passwords, Internet history and files left on the retired computer or server.

As a first prevention step, find a local recycling facility where e-waste can be safely disposed of. And make sure to take the following #1 security precaution before you haul it off: remove and destroy the hard drives. A drill and hammer usually do the trick just fine. Alternatively, many companies that shred paper documents will also destroy your hard drives.

We offer free e-waste recycling services to our clients – just let us know and we'll pick up your old hardware and make sure it's properly recycled.

Don't forget other e-waste such as mobile phones, copy machines and any other device that ever touched your company data. Give serious thought to what data is on any device before you recycle it.