two river™
TECHNOLOGY TIMES

What's New

The 'Not Me!' Problem …

Remembering 24 different passwords, memorizing four PIN numbers and installing updates all the time is frustrating enough. Many of us also have to remember the code for the door, the alarm code for the alarm panel next to the door, the secret password to tell the alarm company, the passcode to your phone, the garage code … You get the idea.

This logic is based on a time when threats were more "real," like the idea of someone robbing our house. In 2020, these types of threats are statistically less likely to happen than virtual threats like fraudulent credit card charges, data loss and identity theft. In fact, cyberattacks occur three times as often as home burglaries in the United States, according to a 2016 study by the University of Kentucky.

It's important to avoid the "Not me!" approach to this shift. Businesses say this all the time: "I'm too small for anyone to want to steal my data. I have a good firewall, hourly backups and a great IT support partner – no one will steal my files."

But the truth is that businesses with under 100 employees are low-hanging fruit for cybercriminals – yes, that's a lot of you! It can happen to you, so you must approach all aspects of physical and electronic security with the attention they deserve in today's business world.

August 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!"

The #1 Mistake Companies Make With Their IT

If you're like many businesses today, there's a good chance you've made this one mistake with your IT security: you don't budget for it.

Or if you do budget for it, it's not enough to *really* protect your business.

Time and time again, business owners decide NOT to invest in IT services. Instead, they go it alone or skip it completely.

Or they might approach an IT services company and ask, "What do you charge for your services?" They don't ask, "What will I get for my money?" or "How can you meet the needs of my company?"

This is a backward approach to IT – and it's a big mistake.

The fact is that a lot of business owners don't take IT seriously. They think that because they haven't been hit by a data breach or a malware attack that it will never happen to them. That's another big mistake. Just because a business hasn't fallen victim to a cyber-attack DOES NOT mean they're safe.

It's the opposite.

When you hire an IT services company, what *do* you get for your money?

The honest answer is that it depends on your specific needs. Many IT services companies offer everything from basic to advanced network security. You can expect services like:

- Cloud backup
- Data protection
- Data monitoring
- Threat detection
- Technology maintenance
- And more!

Continued on pg.2

Continued from pg.1

Everything is designed to protect you, your network, your technology, your employees and your business as a whole. It's all about giving you the information and resources you need so you can worry less about outside threats and focus on your customers and the success of your business.

When you're invested in good IT security, you shouldn't even know it's there. It runs in the background like a quiet but powerful electric motor. It's there when you need it, and it's there when you're not even thinking about it.

For some business owners, this is a tough pill to swallow. They don't have something tangible in front of them that they can see 24/7. A lot of business owners like to be more hands-on. They like to see what their money is buying.

> **"We can't wait to react until something happens. Because when something does happen, it's often too late."**

The great thing is that a good IT services company will provide you with something tangible. If you want to see what is going on behind the scenes of your IT security, they will give you a complete report. Every day (or week or month), you can have an e-mail delivered to your in-box that breaks down exactly what your IT services firm is doing for you.

You can see things like the threats they blocked from getting through. You can see when they performed system maintenance or when your data was backed up. You can customize these reports to your needs.

Basically, you can see what you're paying for and how it's working. This is the very definition of "peace of mind."

Today, none of us can afford to skip out on good IT security. We can't wait to react until something happens. Because when something does happen, it's often too late. The cybercriminals have done their damage and moved on. Meanwhile, your business comes to a screeching halt, and you have to pay the big bucks to get everything back on track – if you *can* get back on track.

Some businesses don't get back on track. They are forced to close after a cyber-attack because they don't have the money or resources to recover. The damage is simply too much and the cost too high. If they had invested in IT security upfront, it might be a different story.

Don't get caught off guard by a data breach, malware infection, hacker attack or data loss due to technology failure or natural causes like flood or fire. It's time to take your IT to the next level. Protect your business the right way and avoid the mistake so many others make when they avoid the investment in good IT.

Work with an IT services firm that takes your business as seriously as you do.

Free Report: What Every Small-Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems

PROTECT YOUR NETWORK

"What Every Business Owner Must Know About Protecting and Preserving Their Network"

Don't Trust Your Company's Critical Data And Operations To Just Anyone!

This report will outline in plain, nontechnical English the common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills, and will provide an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Get Your FREE Copy Today by emailing your request to kmarquez@tworivertech.com

Shiny New Gadget Of The Month:

The Manta5 Hydrofoiler XE-1

If you could ride your bike on the water, would you? Thanks to the Manta5 Hydrofoiler XE-1, *you can*. The Manta5 Hydrofoiler XE-1 is a high-performance watercraft for people of all ages. The minds behind Manta5 wanted to bring cycling to the water – and they succeeded.

The hydrofoil design helps keep you balanced while you pedal across the water, similar to how you pedal on a bike. You can use it on the ocean, in rivers and in lakes. Learning to ride takes practice, but once you get the hang of it, it's a breeze! It won't be long until you're jetting across the water – on your own power! There's even a small electric motor that brings you up to speed if you need it. Take your summer to the next level and learn more at Manta5.com.

The Rest Is My Job

How would you like to be in the position to create the largest army that the world has ever seen *(over 13 million soldiers)* and do it mainly with people who have NEVER commanded troops in their life?

That was exactly the position General George C. Marshall found himself in during World War II. Not only did he have to assemble this incredible army, but he also had to do it in the shortest amount of time possible. He appointed over 600 people to positions of general officer or division commander, with few "slackers."

So, what was his secret to being so successful in putting the right people in the right positions? Smart leaders hire people based on their strengths – what the person *can* do, not what they *can't* do.

For example, General Marshall's aides were worried about him putting a certain colonel, who was known for **not** getting along with his superiors and being terribly rude, in charge of training. They told Marshall, "If things go wrong and he has to testify in front of Congress, he will be a disaster for you and your reputation."

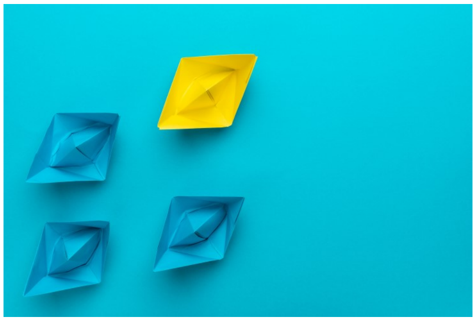
General Marshall asked his aides, "What is his assignment … what do we need him for?"

They responded, "To train troops – an entire division."

Marshall then asked, "Is he a first-rate trainer?"

His aides responded, "Yes sir, General. He is the best we have."

He said, "Well, give him the assignment. The rest is my job."

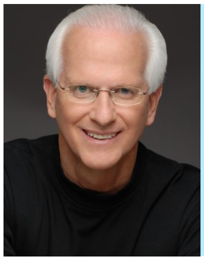


THE REST IS MY JOB. What a great statement. Sometimes a good leader will have to protect, and even defend, some of their subordinates who may have some rough edges when it comes to diplomatically communicating with other bosses or departments. These leaders know they have a high achiever, a real winner, when it comes to getting the job done, and they will do everything they can to protect their asset.

Who would you rather have in a position: **1)** the most polite communicator who ruffles no feathers; challenges no person, policy or procedure and has an average performance rating, or **2)** a highly focused, determined, loyal, "tells it like it is – good or bad" leader who occasionally upsets those who hindered their progress and is known for always getting the job done? Give me #2 any day – the **rest is my job to keep the peace.**

Leadership is not about authority. If you are taking the position because it gives you power, supremacy or authority over people, please do not apply. It is a servant position. You are there to help others succeed. **It isn't about you; it's about them**. Hire others for their strengths and let them at it. Learn about the man who created the largest army in the history of the world and who understood we are graded on results …

The rest was his job.



Robert Stevenson is one of the most widely recognized professional speakers in the world. Author of the books How To Soar Like An Eagle In A World Full Of Turkeys *and* 52 Essential Habits For Success, *he's shared the podium with esteemed figures from across the country, including former President George H.W. Bush, former Secretary of State Colin Powell, Tony Robbins, Tom Peters and Stephen Covey. Today, he travels the world, sharing powerful ideas for achieving excellence, both personally and professionally.*

Services We Offer

Cloud Services ~Managed Networking Services
Cybersecurity ~ Hosted Voice over IP

TRTG Happenings

New Client Alert:
Zimmet Healthcare

ZIMMET HEALTHCARE
SERVICES GROUP, LLC

TRTG is proud to announce we have recently onboarded our newest clients at Zimmet Healthcare to our managed services and cloud platform!

Zimmet Healthcare Services Group, LLC is a full-service consulting firm committed to developing innovative solutions to the challenges of operating in the post-acute care industry.

Founded in 1993, ZHSG has grown from a small cost-reporting concern to a nationally recognized leader in reimbursement/compliance, outsourced management solutions, performance analytics and post-acute strategy.

Their firm is comprised of more than 50 full-time professionals and currently supports more than 3,000 providers and related organizations nationwide. Their clients range from independent, not-for-profit and government sponsored facilities to national chains. In addition to providers, they advise state associations, countless ancillary concerns, insurers, attorneys, private equity/lenders and other stakeholders that demand the highest level of service.

As their firm continues to grow, they expressed their concern about making sure they keep up with HIPPA laws and financial compliance requirements. They also want to ensure they are fully protecting their data along with their client's data. We are happy to have put their minds at ease by switching them on to our fully secure cloud solution.

We are happy they decided to put their trust in our firm and we look forward to a long and successful partnership!

TRTG Security Tips:

REMOVE that unwanted freeware

Like it or not, PC manufacturers LOVE to stuff your brand-new PC full of "free" applications (they get paid to do it, so you've got a slim chance of getting one without a side of spamware). But clutter is the enemy of a speedy PC, and if you're not using a particular software on a regular basis, it's best to REMOVE it completely. That way you don't have it sucking up processing speed AND leaving the door open to hackers and malware.

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

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.

How to foil ransomware

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!