BLUE BAY TECHNOLOGY

TECH BYTES

What's New

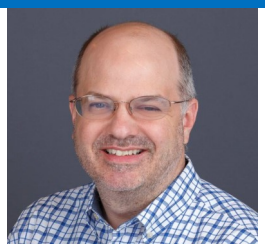
IN HONOR OF VETERAN'S DAY WE SALUTE ONE OF OUR OWN

TONY LOPEZ-PEREZ
Retired Master Sergeant
US Air Force 1989-2013

Tony says he still does his best to live by the Air Force Core values which were instilled in him even before he chose to dedicate his life to service to his country by enlisting in the military. The values that Tony live by are: Integrity First, Service before Self and Excellence in all we do. We here at Blue Bay are truly blessed and honored to be able to work with Tony on a daily basis and be able to have him in our lives.

See Tony's story on Page 3.

November 2020



This monthly publication provided courtesy of Will Sperow, General Manager of Blue Bay Technology.

OUR MISSION

To provide our clients with the same expert-level of support that we would expect ourselves; provide it in an understanding and compassionate environment; and, work to exceed your expectations.

Making This One Mistake With Your Computer Network Could Put You Out Of Business

How do you handle network issues? If you're like most small businesses, you wait until something breaks or goes wrong before getting an IT services company on the phone. At a glance, it makes sense. Why pay to fix something if it isn't broken?

Sadly, this way of thinking can do more harm than good, and it has taken many businesses out of commission.

When you get right down to it, there are two primary ways to handle network security:

- **By being reactive**
- **By being proactive**

One of these costs *significantly* more than the other and can destroy a business. You can probably guess which one we're talking about.

When you're reactive with your IT services, which includes data security, it means something bad has already happened. There are many different things that can harm your data and your business, like an employee accidentally downloading malware onto their computer, you getting hit by a data breach or a power surge occurring late in the night after a thunderstorm hits.

However, being reactive basically opens the door to these threats. It's the one mistake that can put you out of business *for good*.

Hackers, for example, are a HUGE threat to small businesses. These cybercriminals will stop at nothing to break into your network to steal whatever they can get their hands on or do whatever damage they can.

Continued on pg.2

Continued from pg.1

These people don't care if their actions put you out of business.

This is why you cannot rely on a reactive approach to your IT services. When you do, you're a step behind hackers, malware and even natural disasters and equipment failures.

In the past, IT services were very reactive. They were built on the break-fix model, which is exactly as it sounds. A business would wait for something to break or go wrong before calling an IT services company for help to fix it.

In the 1990s and even into the 2000s, the break-fix model had its place and it worked. But as technology improved and it became easier for even the smallest businesses to stay ahead of the curve, the break-fix model stopped making sense.

The number of external threats has increased *dramatically* over the last 10 years. There are countless malware programs floating around on the Internet, and hackers are working 24/7 to wreak havoc.

It's time to get proactive.

Today, IT services companies can predict threats. They can stop attacks in their tracks and protect your business and your data. This is called **managed services** — and it could save your business.

When you work with a managed services provider, you can state exactly how you want to be proactive. Do you want your network monitored for threats 24/7? Do you want them to have remote access to your networked devices so they can provide instant support to you and your team? They can do all of that!

A good IT services company can help you make sure all your data is backed up and secure. They can make sure external threats are spotted before they become a problem. They can make sure phishing e-mails don't expose you to harm. The list goes on!

If you're already working with an IT services company and they're only providing outdated break-fix support, it's time to say, "Enough!" Demand that they get proactive to manage your network. Don't wait until something breaks to make that phone call. Because, as many businesses have learned, waiting to make that call can be devastating!

Continued from pg. 1

THANK YOU FOR YOUR SERVICE

TONY LOPEZ-PEREZ

We are proud to have Tony as a member of the Blue Bay family for over three-and-a-half years. You have most likely interacted with Tony at some point during his time with Blue Bay and you probably know a little bit about him. But what you don't know about him is his impressive and exemplary service to us all. Here's a little bit about our Tony:

Tony entered active duty in September 1989 and was initially stationed at Grandforks Air Force Base (AFB), North Dakota until 1993. In late 1990 to early 1991 he was deployed, and served in, Desert Shield/Storm at a compound just outside of King Khalid International Airport.

In 1993, his application was accepted to the B-2 Stealth Bomber Program and was stationed at Whiteman AFB in Missouri from 1993 to 2004. Where in 2004 he crossed over field specialty and was trained in the Communications field and was subsequently reassigned to Langely AFB.

At Langley he served as non-commissioned officer in charge (NCOIC) of Circuit Actions responsible for long haul/short haul communications to the base. He maintained circuit records and the fiber optic networks using a Cisco Multi Service Provisioning Platform for secure and non-secure networks. He was also deployed to the Middle East three times during his time at Langley, serving in a Network Operations center which supported high level personnel directly involved with the war effort, including General Abizaid during his first tour. Other tours were served as Help Desk and Network Management Supervisor. Most notably he was directly responsible for over 500 tactical encryption devices.

In 2008, he was selected and accepted for a position with the Air Force Office of Special Investigations (OSI) which is the Air Force version of NCIS and was stationed at Andrews AFB, Maryland. He served as NCOIC of network management and was responsible for supporting 3,000 personnel at over 200 locations worldwide. In 2011 he earned the rank of Master Sergeant (MSgt), attained certifications in Security + and ITILv3. He assisted with the transition from Andrews AFB to a newly built "green" facility at Marine Corps Base, Quantico. The 700,000 square foot facility christened, The Russell-Knox building became home to Navy Criminal Investigative Service NCIS, Air Force Office of Special Investigations AFOSI, Defense Intelligence Agency (DIA), Defense Security Service (DSS) and the U.S. Army Criminal Investigation Command (CID). During the transition he helped maintain dual operations at both locations and oversaw technical refreshes of Cisco routers and switches across three networks. His experience was broad as he helped to maintain the server room, assist with account creation in Active directory, troubleshot network issues, maintained tactical network devices, maintained voice over IP phones, and remote access telework solution.

4 Ways Leaders Can Identify And Overcome Blind Spots

One of the biggest challenges leaders face in their personal and professional development is identifying blind spots, the unseen obstacles that hold them back from achieving their full potential.

Unfortunately, many leaders don't take the time to find out if they have blind spots. Research by Zenger Folkman found that 30% of leaders had at least one major flaw that they did not know about.

Finding and fixing blind spots isn't for the faint of heart. It takes a lot of effort, courage and discipline to identify them and course-correct. But going through the process will help you and your business to keep moving forward. Here are four tips to guide you.

1. **LOOK IN THE MIRROR.**
   Conduct a self-assessment and categorize your known strengths and weaknesses. Block out time on your calendar and don't allow interruptions. Force yourself to answer tough questions about your abilities and limitations. Then, write down the answers so you have a better understanding of where you are succeeding, where you are falling short and what steps you need to take to improve. The inventory you create during the self-assessment will be incredibly helpful when you compare it to information collected from other sources.

2. GAIN INSIGHT FROM PERSONALITY TESTS.
Standardized personality tests are another tool to help uncover blind spots. Wiley's DiSC and the Myers-Briggs Type Indicator are two popular tests that provide insight into your leadership style. Most of these assessments are based on the "Big 5" personality traits: agreeableness, conscientiousness, extroversion, neuroticism and openness. When compared to your own self-assessment, the tests can shed more light on your tendencies and preferences in communication, decision-making and problem-solving.

3. SEEK INPUT FROM OTHERS ABOUT YOUR BLIND SPOTS.

This is where the process gets tough, but it's also the most important step to take. Ask several members of your team and peers to list your strengths, weaknesses and blind spots. Ask them to recommend ways that you can improve. If you are unsure that team members and peers will share their true feelings for fear of looking critical, then use online tools like Google Sheets or Survey Monkey to obtain anonymous feedback.

4. CREATE A PLAN AND ACT ON IT.
The most effective personal and professional development initiatives have a written plan that includes the information collected in the previous steps and identifies tasks to be completed and milestones to be achieved. It's your blueprint for success and will keep you on track to achieve your goals. Make sure every goal is SMART (specific, measurable, attainable, relevant and time-bound) and that tasks and milestones are reviewed on a weekly, monthly and quarterly basis so you can quantify your progress.

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.

Become A Pro At Videoconferencing From Home

At the start of the year, most of us weren't prepared to take video calls at home. We just didn't have the right setup.Now we're practically at the end of the year, and we're out of excuses! Here are four quick tips to transform into a videoconferencing pro:

1. Boost your sound. A dedicated microphone is going to sound much better than the mic in your phone or laptop. Creating an optimal sound environment can make a difference, so turn off external speakers and hold the call in a quiet zone.

2. Adjust the video. Keep your camera at eye level with a simple background. This not only looks more natural, but it also minimizes visual distractions and instantly looks more professional.

3. Light it up. This can get complicated fast. You want a light source in front of you, but your computer monitors are not enough. However, you don't want harsh, direct lighting. Diffused lighting is best, but ring lights are popular among YouTubers and work great for video calls.

4. Look good! Keep simple button-down shirts, ties, blouses and other items near the computer so you can dress and look professional for a call. Keep it business casual and avoid complicated patterns and harsh colors that can look awkward on camera. *Small Business Trends, May 28, 2020*

Are Your Employees Leaving This Backdoor Wide Open?

Most of your employees have wireless networks set up in their homes.

Unlike your business WiFi, many home wireless networks lack proper security, leaving a backdoor open to hackers. WiFi signals often broadcast far beyond your employees' homes and out into the streets. Drive-by hacking is popular among cybercriminals today.

Here are a few tips for securing your employees' WiFi access points:

- Use stronger encryption and a more complex password.
- Hide your wireless network name.
- Use a firewall.

These security measures are not difficult to set up. If you have any questions or need assistance, we will be happy to help get your employees set up remotely.

How Do I Know If My Security Camera Has Been Hacked?

Yes, hackers can access security cameras; are yours at risk? Here are three signs to look for to identify a compromised security system.

You hear voices or other odd sounds. Some hackers love to scare people and will speak through your camera's speaker system. Sometimes, the hacker might not realize the sound is on. Either way, strange sounds can mean your camera needs to be shut off immediately.

The camera moves. Generally speaking, the average security camera doesn't move, but there are many models that can be adjusted remotely. If you see a camera move or you find it in a new position, check on it!

There's unusual data traffic. Accessing your camera remotely uses data. Many wireless routers let you track data usage. So, if someone is accessing your camera remotely, that data usage should be logged. *Digital Trends, Sept. 1, 2020*