The AvTek Chronicle

Wayne's World Where in the world is WAYNE?

April 1-5
Bootcamp in Nashville, TN

April 12
AvTek Solutions will be celebrating our 20th Anniversary!

April 16-18
NYC

April 30th
Episode 4 of Wayne's Deep Dives
Link

April 2024

Wayne Hunter is the President and CEO of AvTek Solutions, Inc. where he concentrates his efforts on providing the best solution to customers.

Wayne has over 30 years of experience in Information Technology, focusing on implementing storage and data systems, IT management, and systems integration.

3 Cyber Security Myths That Will Hurt Your Business This Year

Working amid the ever-changing currents of technology and cyber security, businesses often find themselves entangled in a web of misinformation and outdated ideas. But failing to distinguish between myth and fact can put your business's security at serious risk.

Based on expert research in the field, including CompTIA's 2024 global State Of Cybersecurity report, we will debunk three common misconceptions that threaten to derail your success in 2024.

Myth 1: My cyber security is good enough!

Fact: Modern cyber security is about continuous improvement.

Respondents to CompTIA's survey indicated that one of the most significant challenges to cyber security initiatives today is the belief that "current security is good enough" (39%).

One of the reasons businesses may be misled by the state of their security is the inherent complexity of cyber security. In particular, it's incredibly challenging to track and measure security effectiveness and stay current on trends. Thus, an incomplete understanding of security leads executives to think all is well.

Over 40% of executives express complete satisfaction with their organization's cyber security, according to CompTIA's report. In contrast, only 25% of IT staff and 21% of business staff are satisfied. This could also be accounted for by executives often having more tech freedom for added convenience while frontline staff deal with less visible cyber security details.

"Either way, the gap in satisfaction points to a need for improved communication on the topic," CompTIA writes.

Get your IT and business teams together and figure out what risks you face right now and what needs to change. Because cyber security is constantly changing, your security should never be stagnant. "Good enough" is never good enough for your business; vigilance and a continuous improvement mindset are the only ways to approach cyber security.

Myth 2: Cyber security = keeping threats out

Fact: Cyber security protects against threats both inside and outside your organization.

One of the most publicized breaches of the last decade was when BBC reported that a Heathrow Airport employee lost a USB stick with sensitive data on it. Although the stick was recovered with no harm done, it still cost Heathrow £120,000 (US$150,000) in fines.

Yes, cyber security is about protection. However, protection extends to both external and internal threats such as employee error.

Because security threats are diverse and wideranging, there are risks that have little to do with your IT team. For example, how do your employees use social media? "In an era of social engineering, there must be precise guidelines around the content being shared since it could eventually lead to a breach," CompTIA states. Attacks are increasingly focused on human social

Continued on pg. 2

engineering, like phishing, and criminals bank on your staff making mistakes.

Additionally, managing relationships with third-party vendors and partners often involves some form of data sharing. "The chain of operations is only as strong as its weakest link," CompTIA points out. "When that chain involves outside parties, finding the weakest link requires detailed planning."

Everyone in your organization is responsible for being vigilant and aware of security best practices and safety as it relates to their jobs. Make sure your cyber security strategy puts equal emphasis on internal threats as much as external ones.

Myth 3: IT handles my cyber security

Fact: Cyber security is not solely the responsibility of the IT department.

While IT professionals are crucial in implementing security measures, comprehensive cyber security involves a multidisciplinary approach. It encompasses not only technical aspects but also policy development, employee training, risk management and a deep understanding of the organization's unique security landscape.

Because each department within your organization involves unique risks, people from various roles must be included in security conversations. But many companies are not doing this. CompTIA's report shows that while 40% of respondents say that technical staff is leading those conversations, only 36% indicate that the CEO is participating, and just 25% say that business staff is involved.

"More companies should consider including a wide range of business professionals, from executives to mid-level management to staff positions, in risk management discussions," CompTIA writes. "These individuals are becoming more involved in technology decisions for their departments, and without a proper view into the associated risks, their decisions may have harmful consequences."

Business leaders and employees at all levels must actively engage in cyber security efforts, as they are all potential gatekeepers against evolving threats.

Don't Listen To Myths

By embracing a mindset of continuous improvement, recognizing the wide range of threats and understanding the collective responsibility of cyber security, your business will remain safe, resilient and thriving, no matter what the future holds.

Why Your Business Needs

REGULAR NETWORK PEN TESTS

Regular assessment of your network is essential to gauge your cybersecurity effectiveness. A network penetration test (pen test) is a security test in which experts attempt to hack into your network to identify potential vulnerabilities that malicious actors could exploit.

BENEFITS OF PEN TESTING

REAL-WORLD SIMULATION
Simulates a cyberattack to assess your security measures.

RISK PRIORITIZATION
Prioritizes vulnerabilities by degree of risk, addressing critical issues first.

VULNERABILITY IDENTIFICATION
Exposes security vulnerabilities to reveal potential entry points.

COMPREHENSIVE SECURITY ASSESSMENT
Evaluates current security controls to ensure systems can withstand cyberthreats.

RISK MITIGATION
Enables effective prioritization and mitigation of potential cyber-risks.

COMPLIANCE WITH REGULATIONS
Maintains compliance to avoid legal and financial consequences.

CUSTOMER DATA PROTECTION
Addresses vulnerabilities that lead to breaches, identity theft or unauthorized access.

PROACTIVE OFFENSE
Proactively reduces attack vectors through regular assessments.

THREAT DEFENSE
Identifies vulnerabilities missed by traditional security measures.

PROACTIVE CYBERSECURITY STARTS HERE.

Schedule your network penetration test today.

Retired Navy SEAL Shares The Key To Building And Leading A High-Performance Team

Most business leaders strive for one thing: to be a strong and competent leader of a high-performing team. To do this, they'll try just about anything, from free lunches to daylong team-building retreats. Although these are helpful, high-performing teams don't begin with external motivators. They begin when leaders embrace a culture of extreme ownership.

"Extreme ownership is pretty straightforward," Jocko Willink says. "You're not going to make any excuses. You're not going to blame anybody else. When something goes wrong, you're going to take ownership of those problems and get them solved."

Willink is the author of the New York Times bestseller Extreme Ownership: How U.S. Navy SEALs Lead And Win. He explains that the same leadership concepts that enable SEAL teams to succeed in the most intense circumstances can also help businesses win again and again.

As a young SEAL, Willink noticed that a culture of finger-pointing grew when blame was directed toward a person or a team. When that happens, "no one solves the problem," he says. However, when leaders owned issues and responsibility for finding a solution, the team reflected that ownership. "It actually made the other people inside the platoon have the same attitude. They'd say, 'It was my fault; let me fix it,'" Willink explains.

Eventually, Willink went on to fill leadership roles within the SEALs, learning to embrace personal accountability and team empowerment. Now a retired SEAL officer and co-founder of the leadership consulting firm Echelon, he's worked with hundreds of civilian companies on extreme ownership, finding the same results: when leaders take ownership of problems, the entire team is more likely to be high-performing and successful.

How To Create An Extreme Ownership Culture

"The biggest thing you've got to overcome is your ego," Willink explains. Pointing out that someone didn't do their job right or that the marketing plan wasn't carried out correctly doesn't solve the problem. "You're the boss. You own it," Willink says. When one person takes ownership, it spreads. "That's what develops the culture."

Although extreme ownership starts with the boss, the key to a high-performing team is to empower individuals to take responsibility for projects and tasks too.

"If you want people to take ownership, you have to give them ownership," Willink says. This way, you empower your team to make decisions while you serve as a reliable guide and offer direction when needed. "Put them in positions where they make decisions, make mistakes and learn to be honest with you," he says. If you're not getting the behaviors you need, you can study it and start to correct it by figuring out what support you can provide.

Willink points out that there will always be team members who don't embrace ownership. But when extreme ownership is a culture, they'll naturally get weeded out.

Those who are ready to step up, however, will rise to the top. "There's something more important to many people than how much money they make," he says. "That is control over their destiny, autonomy and freedom."

Shiny New Gadget Of The Month

JSAUX USB Data Blocker

Last year, the FBI warned consumers not to use public charging stations because hackers were installing malware into USB ports and stealing data. If you forget your charger, the JSAUX USB-A Data Blocker is a game-changer for secure charging when you're on the go.

Designed exclusively for charging with no data-sync function, it's perfect for public charging stations in airports, hotel lobbies and coffee shops, eliminating hacking risks. It offers a rapid 2.4A charge and works with a wide range of devices. Compact, portable and cheap, the USB Data Blocker is the no-brainer companion you need in your travel backpack right now!

Check Fraud Crimes Are "Washing" Away Bank Accounts

Headlines are usually flush with the latest digital breaches out to get businesses. Weak passwords, complex social engineering and business e-mail compromise are often the culprits we hear about. But while our eyes and ears were honed in on digital threats, old-fashioned paper-and-pen crimes were sneaking into our bank accounts.

According to the Financial Crimes Enforcement Network, fraudulent-check crimes rose 201.2% between 2018 and 2022. Experts say that the rise of check fraud began in 2020 when criminals started stealing stimulus checks. Once those ended, they needed a new source of income. In 2023, S&P Global noted that check fraud made up one-third of all bank fraud, excluding mortgage fraud.

It's a cheap and relatively simple crime happening under our noses, and that's why they're getting away with it.

How Criminals "Wash" Checks

AARP says that most check fraud involves check "washing." This is when criminals use bleach or acetone to wash away the ink used to write the payee and check amount after stealing it from your mailbox or fishing it from a drop box. Once washed, the check dries, is filled out with new information and deposited at banks or cash-checking shops.

According to AARP, a 60-year-old man had a check for $235 stolen and cashed for $9,001.20 – all within 24 hours. It's not just the US either. An Ontario business owner sent a check for $10,800 to the Canada Revenue Agency to make tax payments for his maple syrup company. Days later, it had been stolen and deposited into another account.

It's a low-budget, fast-cash reward for criminals. Even worse, some banks have deadlines for reporting this kind of crime and won't reimburse you if you alert them too late.

Prevent Check Fraud With These 6 Tips

Thankfully, there are a few simple steps you can take to significantly reduce your risk of check fraud.

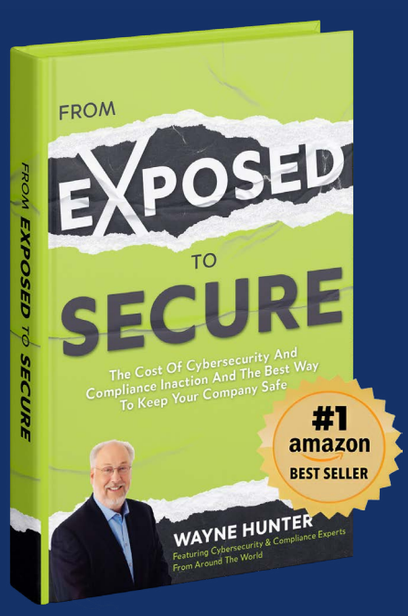
1. ***Pay Online:*** Pay bills online using a private Wi-Fi connection and a secure portal, like through your bank or vendor website.
2. ***Mail Safely:*** Use the post office for mailing checks; avoid leaving them in personal or outdoor mailboxes.
3. ***Use Gel Ink:*** Use non-erasable gel ink in blue or black for writing checks; these are harder to erase than ballpoint pen ink.
4. ***Collect Mail Daily:*** Pick up your mail daily. If away, arrange for collection.
5. ***Monitor Your Accounts:*** Regularly check your bank account online – a few times a week is best.
6. ***Report Incidents Immediately:*** Report fraud quickly to your bank and Postal Inspection Service. Most institutions are required to reimburse stolen funds if the theft is reported within 30 days.

It might be a digital world, but criminals will use every tactic to get hold of your hard-earned cash. Add these simple tips to your routine to significantly reduce your risk of check fraud.

The Generation Most Prone To Phone-Related Accidents Will Surprise You

It's time millennials stop making fun of their elders for butt dials, weird FaceTime angles and other tech snafus. According to data from the National Electronic Injury Surveillance System, millennials are more prone to embarrassing tech-related accidents than any other generation. Since 2020, injuries across the board have shot up 20%, likely due to people being home more during the pandemic. The biggest culprit: people lifting televisions, resulting in strains and sprains (lift with your legs, people!). This accounts for 30% of injuries in the US. Unsurprisingly, walking and using a cellphone is runner-up, causing 23% of tech-related boo-boos. Eyes up, friends!

Protect Your Business and Assets from Hackers!



Here's What You'll Learn From The New Book, From Exposed To Secure:

- The biggest cyberthreats that could take your company down. Page 18.
- How to take the confusion out of compliance. Page 32.
- The incorrect perceptions on compliance that could be putting you in danger. Page 41.
- 8 best practices to minimize risk. Page 63.
- The surprising first line of defense. Page 72.
- How to protect yourself from fines…and jail. Page 141.
- 10 strategies you must have in place to be considered for insurance. Page 174.
- Critical steps to take immediately if you are hacked. Page 182.
- How an IT expert keeps her own kids safe online. Page 205.

And much more.

CHECK IT OUT NOW