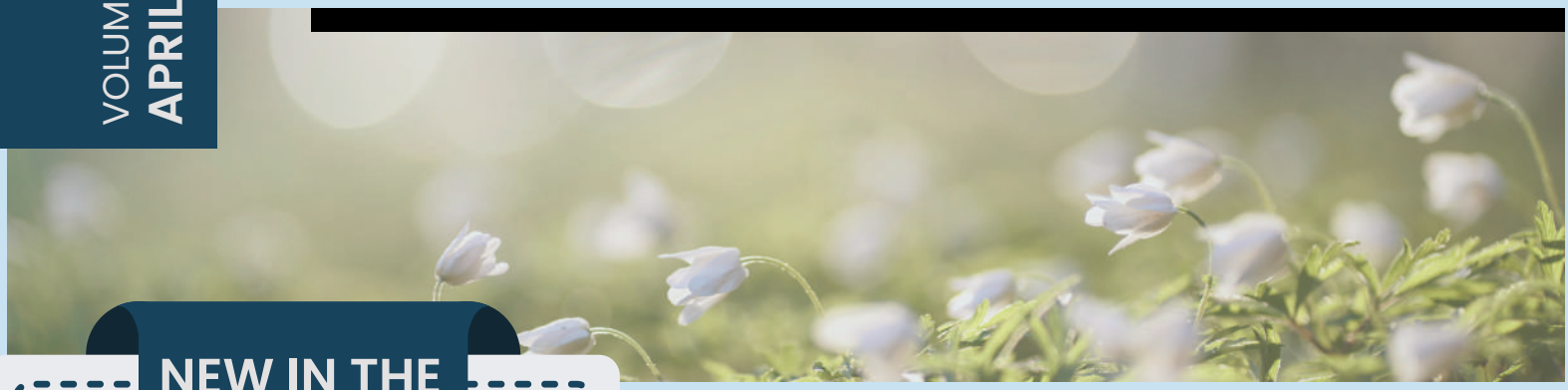
VOLUME 9
APRIL 2024

Loyality it's our word.

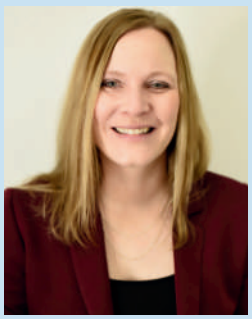
TECH TALK

NEWSLETTER



NEW IN THE NEWSLETTER

WELCOME HOLLY!



This monthly publication is provided courtesy of Kari Renn, President of LoyallTy.

Our Mission: To make IT work at work so our clients can focus on their company goals without interruption.

In This Edition:

In this newsletter, we delve into critical insights spanning cybersecurity and leadership, aiming to empower businesses with knowledge and strategies for success. The first article debunks prevalent cybersecurity myths, urging organizations to prioritize continuous improvement and collective responsibility. The second article, featuring retired Navy SEAL Jocko Willink, explores the concept of extreme ownership as a transformative force for building high performance teams. Our micro-article sheds light on the resurgence of traditional check fraud, providing practical tips to safeguard against this evolving threat.

3 Cybersecurity Myths that Will Hurt Your Business This Year

Working amid the ever-changing currents of technology and cybersecurity, businesses often find themselves entangled in a web of misinformation and outdated ideas.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, including CompTIA's 2024 global State of Cybersecurity report, we will debunk 3 common myths that threaten to derail your success in 2024.

Myth 1: My Cybersecurity is Good Enough

Fact: Modern cybersecurity is about continuous improvement.

Respondents to CompTIA's survey indicated that one of the most significant challenges to cybersecurity 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 cybersecurity. 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.

Continued on pg. 2

Continued from pg. 1

CompTIA's report reveals that over 40% of executives report feeling fully satisfied with their organization's cybersecurity measures. However, the satisfaction among IT staff and business personnel are notably lower, with only 25% and 21% respectively expressing contentment. This discrepancy may stem from executives typically enjoying greater technological autonomy for enhanced convenience, whereas frontline staff are tasked with managing the intricacies of cybersecurity that are less apparent to the organization at large.

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

Bring your IT and business teams together to assess current risks and necessary adjustments. With cybersecurity, stagnation is not an option. 'Good enough' falls short in protecting your business; perpetual vigilance is imperative.

Myth 2: Cybersecurity Keeps Threats Out

Fact: Cybersecurity 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 $150,000 in fines.

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

Because security threats are diverse and wide-ranging, 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 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, when that chain involves outside parties, finding the weakest link requires detailed planning."
>
> -CompTIA

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 Cybersecurity

Fact: Cybersecurity 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 cybersecurity efforts, as they are all potential gatekeepers against evolving threats.

Continued on pg. 3

FREE CYBERSECURITY REPORT:

It's coming...

- That day a hacker steals critical data, rendering your office useless...
- That day when your bank account or credit card is compromised...
- Or that day when your customers' private lives are uprooted...

Download your free copy today and ensure you are prepared for any digital dilema!

CARTOON OF THE MONTH

"I wouldn't call it identity theft, I just self-identify as other people."

Continued from pg. 2

Don't Listen to Myths

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

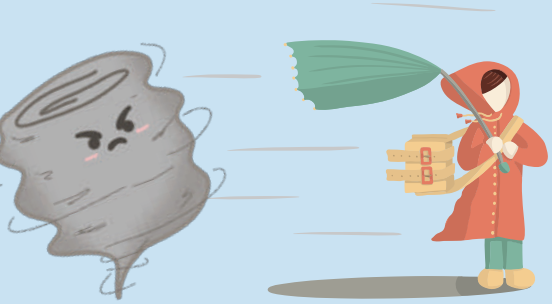
Retired Navy SEAL Shares the Key to Building and Leading a High-Performance Team

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. 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."

-Jocko Willink

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."

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 email compromises 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.

Reported by AARP, a 60-year-old man had a $235 check stolen and fraudulently cashed for $9,001.20, all in a span of 24 hours. Such incidents are not isolated to the US. In Ontario, a business owner mailed a $10,800 check to the Canada Revenue Agency for tax payments on his maple syrup company, only to discover days later that it had been intercepted and deposited into an unauthorized 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 WiFi 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 nonerasable gel ink in blue or black for writing checks; these are harder to erase than a 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.

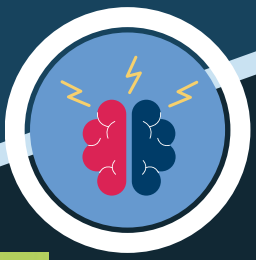
ARE YOU PREPARED FOR NATURAL DISASTERS?

Ensuring network resilience during natural disasters is crucial, so here are some tips to keep you company running continuously year!

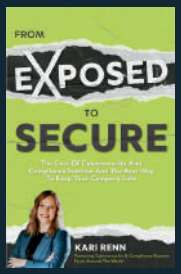
Risk Assessment and Prioritization
- Identify potential risks and their impact on business operations.
- Conduct a business impact analysis to prioritize critical functions.

Communication and Coordination
- Establish clear communication protocols for stakeholders.
- Define roles and responsibilities, designate a spokesperson, and update contact information.

Regular Testing and Training
- Conduct regular simulations and drills to test the plan.
- Provide ongoing training to ensure team readiness and awareness.



READING CORNER



From Exposed To Secure

The Cost Of Cybersecurity And Compliance Inaction And The Best Way To Keep Your Company Safe

Cybercrime has developed into a billion-dollar industry. And as long as it's profitable to be a hacker or a scammer, these criminals aren't going away.
Featuring top cybersecurity and compliance professionals from around the world, From Exposed To Secure reveals the everyday threats that are putting your company in danger and where to focus your resources to eliminate exposure and minimize risk.
These experts share their decades of experience in utilizing data protection regulations and complete security measures to protect your company from fines, lawsuits, loss of revenue, operation disruption or destruction, intellectual property theft, and reputational damage.
From Exposed To Secure delivers the crucial, smart steps every business must take to protect itself against the increasingly prevalent and sophisticated cyberthreats that can destroy your company – including phishing, the Internet of Things, insider threats, ransomware, supply chain, and zero-day.
Consider this book the secret weapon that hackers never saw coming!