TECHNOLOGY TIMES

INSIDER TIPS TO MAKE YOUR BUSINESS RUN FASTER, EASIER AND MORE PROFITABLY SINCE 2003

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currents of technology and cybersecurity, businesses often find themselves entangled in a web of misinformation and outdated ideas.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 risk.

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

Over 40% of executives express complete satisfaction with their organization's cybersecurity, 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 cybersecurity 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 cybersecurity 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

Continued on pg.2

April 2024

Slash Your Phone Bill Up To 80%

Next-Gen Office Phone System

3CX will serve your business now and into the future. Suitable for any business size, 3CX can accommodate your every need; from mobility and status to advanced contact center features and more, at a fraction of the cost.

- √ **Affordable, flexible solution**
- √ **Effortless user & system management**
- √ **Appliance or virtualized**
- √ **Your business phone, anywhere**
- √ **One platform for all communication**

This monthly publication provided courtesy of David Luft, CEO of LDD Consulting, Inc.

Our Mission:

We promise to provide knowledgeable, courteous and prompt service. We care as much about your business as you do. If you are not completely satisfied, be sure to let us know. If we cannot resolve the issue, we will refund your money.

... continued from cover

the only ways to approach cybersecurity.

Myth 2: Cybersecurity = Keeping 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 £120,000 (US$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," 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 cybersecurity 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 cybersecurity 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.

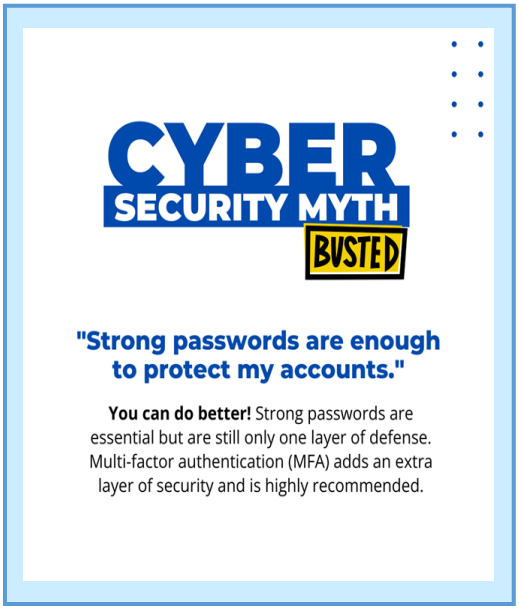
"More companies should consider including a wide range of business professionals, from executives to mid-level management to staff positions, in risk management discussions," CompTIA writes. "These individuals are becoming more involved in technology decisions for their departments, and without a proper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

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.

> **"...But failing to distinguish between myth and fact can put your business's security at serious risk.."**



Retired Navy Seal Shares the Key to Building & Leading a High-Performance Team

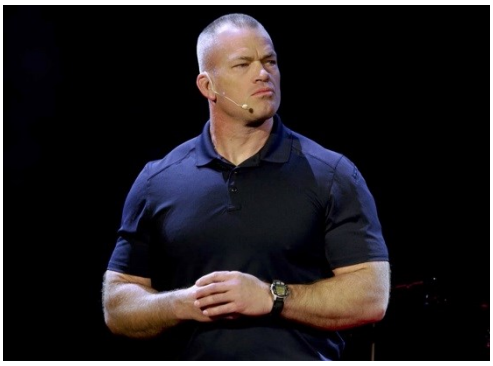
Most business leaders strive for one thing: to be a strong and competent leader of a high-performing team. To do this, they'll try just about anything, from free lunches to daylong team-building retreats. Although these are helpful, high-performing teams don't begin with external motivators. They begin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

Client Spotlight

On-Site Within an Hour To Resolve Issues

LDD Consulting and LDD Web Design are crucial to our school's success. Their exceptional customer service ensures swift resolution of technical issues. During PARCC testing, they provided flawless network setup and on-site support, resulting in zero technical glitches. They seamlessly integrate new technology into our network, demonstrating unparalleled dedication. Highly recommended!

Dr. Sandy Roth
Director of Curriculum & Assessment
Albuquerque Charter School

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 Industry 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 a runner-up, causing 23% of tech-related boo-boos. Eyes up, friends!

Making Technology Work for You
2420 Midtown PL NE, Suite K
Albuquerque, NM 87107

«Name»
«Company Name»
«Street Address 1» «Street Address 2»
«City», «State» «Postal Code»

Inside This Issue

Check Fraud Crimes Are "Washing" Away Bank Accounts

Headlines are typically dominated by the latest digital breaches targeting businesses. Weak passwords, sophisticated social engineering tactics, and business email compromise often take center stage in discussions about cybersecurity threats. However, amidst the focus on digital vulnerabilities, traditional paper-and-pen crimes have quietly made their way into the spotlight, particularly concerning fraudulent checks.

According to the Financial Crimes Enforcement Network, fraudulent-check crimes experienced a staggering increase of 201.2% between 2018 and 2022. This rise in check fraud gained momentum in 2020, coinciding with the onset of the COVID-19 pandemic, when criminals began targeting stimulus checks. As government stimulus programs ended, criminals sought alternative sources of illicit income. By 2023, S&P Global reported that check fraud accounted for one-third of all bank fraud, excluding mortgage-related schemes.

What distinguishes check fraud is its simplicity and affordability, making it an attractive option for criminals. "Check washing" is a prevalent technique, involving the use of bleach or acetone to remove ink from stolen checks, allowing criminals to alter the payee and amount before cashing them. AARP recounts the story of a 60-year-old man whose $235 check was fraudulently altered and cashed for $9,001.20 within a mere 24 hours. Similarly, a business owner in Ontario, Canada, sent a check for $10,800 to the Canada Revenue Agency for tax payments, only to discover days later that it had been stolen and deposited into another account.

The allure of check fraud lies in its ability to yield fast cash with minimal effort. Furthermore, some financial institutions impose deadlines for reporting such crimes and may not reimburse victims if they fail to report promptly.

Fortunately, there are practical steps individuals and businesses can take to mitigate the risk of check fraud:

1. **Pay Online:** Conduct bill payments online using a secure internet connection and reputable portals provided by banks or vendors.
2. **Mail Safely:** Utilize postal services for mailing checks rather than leaving them in personal or outdoor mailboxes susceptible to theft.
3. **Use Gel Ink:** Employ non-erasable gel ink in blue or black when writing checks, as it is more resistant to tampering compared to ballpoint pen ink.
4. **Collect Mail Daily:** Retrieve mail promptly, ideally on a daily basis, and arrange for mail collection when away from home.
5. **Monitor Accounts:** Regularly review bank account activity online, checking for any unauthorized transactions or suspicious activity.
6. **Report Incidents Immediately:** If you suspect fraud, promptly inform your bank and relevant authorities, such as the Postal Inspection Service. Many institutions will reimburse stolen funds if reported within 30 days.

In conclusion, as digital threats dominate cybersecurity discussions, the resurgence of traditional check fraud underscores the need to protect against both digital and analog vulnerabilities. Implementing these measures can significantly reduce exposure to check fraud and safeguard assets.