THE INTEGRATED AXIS TECH CHRONICLE

What's New

Events Around Town

- 6 - Science at Sunset @ Flandrau Planetarium
- 11 - UA Dance: Springs Eternal
- 14 - Blenman Elm History Home & Garden Tour
- 18 - Pima Country Fair
- 20 - Agave Heritage Fiesta

CARE^2

Customer Focus
Accountability
Respect
Excellence & Empathy

April 2024

This monthly publication provided courtesy of Sean Oseran, CEO of Integrated Axis Technology Group

3 CYBER SECURITY MYTHS THAT MAY HURT YOUR BUSINESS

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currents of technology and cyber security, businesses often find themselves entangled in a web of misinformation and outdated ideas.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

Continued on pg. 2

"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 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 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.

CYBERSECURITY CORNER: AT&T DATA BREACH

AT&T confirms a data breach affecting 73 million customers, highlighting the critical need for robust cybersecurity measures in businesses. Personal information like SSNs were leaked on the dark web, emphasizing the importance of safeguarding sensitive data. AT&T is launching a thorough investigation with cybersecurity experts and resetting passcodes for impacted customers. While financial information and call history remain unaffected, the breach underscores vulnerabilities in data protection. This incident reinforces the urgency for businesses to prioritize cybersecurity to mitigate risks and protect customer trust.

If you have questions about how to safeguard your business against breaches and want to implement robust network security measures, call the IA team today. We can help protect your data within your budget, to best support your organization from potential attacks. 🔒👨‍💻

AGAVE HERITAGE FESTIVAL HOSTED BY HOTEL CONGRESS

IA is a proud sponsor of the 16th annual Agave Heritage Festival, set to take place from April 18-21, promising an unparalleled experience celebrating the agave plant's versatility and sustainability. This year marks the largest event yet, with over 55 activities packed into four days.

Attendees will indulge in curated dinners, educational sessions, and tastings of premium agave spirits, culminating in the inaugural Howard Scott Gentry Lifetime Achievement Award Gala Dinner and Fundraiser. This special event honors the legacy of botanist Howard Scott Gentry, celebrating his contributions as a leading authority on the agave plant.

The festival's diverse program showcases the rich cultural heritage of the Southwest and the Sonoran Desert borderlands. From heritage dinner series featuring regional Mexican cuisine paired with curated agave spirits, to guided tastings led by industry experts, there's something for everyone to explore.

New highlights this year include literary and film events such as a poetry reading and a documentary screening on traditional mezcal production. Additionally, Mujer Agave, a collective empowering women in the agave industry, will offer conferences and experiences geared toward female stakeholders.

Cultural events like the Spirit of Sonora Cultural Expo & Celebration and the Agave Fiesta on the Plaza provide opportunities for attendees to engage with topics like water conservation, agriculture, and community resilience.

Live music, spirit samples, farm tours, and discussions highlight the importance of agave in shaping regional identity and fostering community connections.

Overall, the Agave Heritage Festival promises an immersive and enriching experience, offering guests a unique perspective on the flavors, traditions, and sustainability of agave in the Southwest.

agaveheritagefestival.com

A NAVY SEAL SHARES THE KEY TO BUILDING A HIGH-PERFORMING 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."