THE CYBERSIDE BRIEF

Insider Wisdom from 20 Years of IT Defense for Your Business Prosperity and Security

INSIDE THIS ISSUE

3 Cyber Security Myths That Will Hurt Your Business This Year P. 1

FREE REPORT: What Every Small-Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems P. 2

COMPLIANCY NAVIGATOR: 5 Ways to Combine Compliance and Cybersecurity Best Practices to Improve Outcomes P. 3

Retired Navy SEAL Shares The Key To Building And Leading A High-Performance Team P. 4

WEB CONCIERGE: 5 Essentials of Using Social Media to Propel Your Business Growth P. 5

Congratulations to our Registered Practitioners P. 5

Preventing Check Fraud P. 6

This monthly publication is provided courtesy of Patrick Birt, President of AdRem Systems Corporation.

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currents of technology and cyber security, businesses often find themselves entangled in a web of misinformation and outdated ideas.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 aving more tech freedom for added convenience while frontline staff deal with less visible cyber security details.

continued on page 2...

...continued from cover

"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 tunderstanding 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.

Compliancy Navigator

5 WAYS

TO COMBINE COMPLIANCE AND CYBERSECURITY BEST PRACTICES TO IMPROVE OUTCOMES

Compliance and security are equally crucial for the seamless operation of your business. Although security is a prime component of compliance, compliance is not the same as security. Both are interconnected but still different.

While compliance helps your business meet industry or government regulations, security protects the integrity of your business and its sensitive data.

Let's take a look at how your business can benefit from combining compliance and security.

PROACTIVELY FIX SECURITY AND COMPLIANCE ISSUES

Failing to take adequate security measures can lead to compliance issues. Similarly, ignoring compliance could also expose your business to security risks and attract fines for non-compliance.

There are multiple security loopholes that you must proactively fix to stay out of danger. Here are a few common issues that businesses like yours face and how you can tackle them:

1. **Advanced Persistent Threats (APTs):** APTs target endpoints, networks and the cloud to paralyze hybrid, remote and on-site work environments. The best way to tackle APTs is by deploying a solution that can:
   a. Offer 24/7 monitoring and threat hunting
   b. Efficiently block malicious actors that evade firewalls and antivirus systems.
2. **Insider Threats:** Insider threats are worrisome since they are tough to detect. That's why we advise having an advanced internal threat detection solution that combines machine learning and intelligent tagging to identify anomalous activity, suspicious changes and threats caused by misconfiguration.
3. **Lack of Clarity About the Network:** Keeping track of all the computers, mobile phones, printers and servers on your business's network is challenging, especially in today's increasingly hybrid approach to work. However, without knowing the devices on your network, it is not possible to know the state of your IT network's health. To combat this problem, you need an automated assessment and documentation solution capable of identifying risks to all assets, including those that are not physically connected to the network.
4. **Untrained Employees:** When your employees are untrained and unaware of risky actions, it could lead to severe security setbacks. For example, an employee carelessly clicking on a phishing link could lead to a full-blown ransomware attack on your business. That's why prioritizing regular employee security awareness training is imperative.
5. **Sale of Credentials on the Dark Web:** Another major security issue that you might encounter is when your credentials get sold on the dark web. This could negatively affect your organization's security, reputation and financial stature. The best way to combat this threat is by deploying industry-best solutions for dark web monitoring as well as identity and access management.

ALIGN SECURITY AND COMPLIANCE

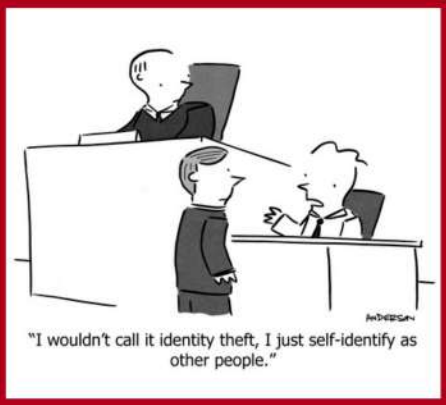
Most workplaces have at least minimum protection in place, such as an antivirus or active firewalls. However, you must ensure that your business's security posture can withstand the growing cyberthreat landscape. With some effort, you can incorporate your security solutions into your compliance strategy as well.

By systematically bringing both security and compliance together, you can significantly reduce risks. To ramp up your organization's security posture, you can implement strong authentication, data protection, access monitoring, network-to-edge defenses and more. Routinely validate the effectiveness of these solutions once they are in place to ensure your organization is taking the necessary measures to avoid non-compliance and security breaches.

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!

CARTOON OF THE MONTH



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

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."

5 ESSENTIALS OF USING SOCIAL MEDIA TO PROPEL YOUR BUSINESS GROWTH

In today's digital age, social media has become a powerful tool for businesses to connect with their audience. Here's how you can leverage social media to propel your business growth:

Identify Your Platform: Understanding where your target audience is most active is key to maximizing your social media efforts. Once you've identified your platform, LinkedIn, Facebook, or perhaps Pinterest, you can start generating content that maximizes engagement with content that capitalizes on each platform's unique features and audience preferences. We recommend focusing your efforts on mastering only one or two platforms that align closely with your target audience's preference and behaviors before expanding to manage additional platforms.

Create Compelling Content: Create unique content that resonates with your audience. Share valuable insights, behind-the-scenes glimpses of your business, testimonials, and promotions or discounts. Remember to keep your content authentic and consistent with your brand identity.

Actively Engage: Engagement is key, so make sure you interact with your audience regularly. Respond to comments, answer questions, and participate in relevant conversations within your industry. Building relationships with your followers helps to foster trust and loyalty over time.

Consider Running Ad Campaigns: Ad campaigns can help your business reach a broader audience and drive additional traffic to your website or landing pages. Most platforms offer easy-to-use ad creation tools that allow you to set specific targeting criteria based on demographics, interests, and behaviors.

Track Your Progress: Keep track of your performance regularly by analyzing your post data. Pay attention to metrics such as reach, engagement, and conversions, so you understand what's working well and where there's room for improvement. Use this data to refine your strategy and optimize your efforts over time.

By following these tips and staying consistent with your social media efforts, you can effectively leverage social media to propel your business growth and achieve your marketing goals.

OUR SERVICES

IT BUSINESS SOLUTIONS

Managed and Co-Managed Service (MSP)
Managed Security Service (MSSP)
Cloud Computing
VoIP Solutions
Data Backup and Recovery
Cybersecurity
Vendor Management
Hardware as a Service (HaaS)
Secure Access Service Edge (SASE)
Virtualization
Remote Work Environments

COMPLIANCE SOLUTIONS

CMMC, NIST, HIPAA, ISO, FTC, etc.
Email Enclaves
Employee Security Training
Data Backup and Recovery
Data Privacy and Encryption
Disaster Recovery Planning
Penetration Testing
Vulnerability Scanning
Policy Consulting
Cybersecurity Consulting

HARDWARE PROCUREMENT

Shop.AdRem.com

HOSTING & ONLINE SERVICES

OnlineServices.AdRem.com

Domain Registration and Transfer
Website Hosting: Website Builder & WordPress
Website Security Solutions
Custom Website Design
WordPress Website Support Solutions
Logo Design
Virtual Private Servers (VPS)
Dedicated Servers
Email Marketing

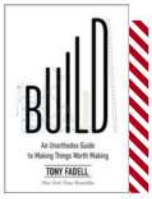
AdRem SYSTEMS

OUR MISSION

To apply our 20 Year Legacy of knowledge and innovation, to defend Critical IT Networks, and encourage a more secure nation of Tomorrow by delivering Today's technologies with respected, trusted, and proven individuals.

BUILD: AN UNORTHODOX GUIDE TO MAKING THINGS WORTH MAKING

By Tony Fadell



Build is an indispensable read for any business owner looking for motivation and practical advice. The book spans Tony Fadell's journey from early-career product designer to accomplished leader, and offers a treasure trove of insights for anyone trying to run a successful business.

Tony's real-world narrative, enriched by his experiences with icons like Steve Jobs, is compelling, easy to read and relatable. Each short chapter, ranging from five to 20 pages, tackles real-world challenges – from start-up funding to critical career-life choices and workplace dynamics. What sets this book apart is its blend of personal stories with the wisdom of Silicon Valley, all while advocating for a refreshingly "old-school" approach to leadership and management. *Build* is a must-read for those who want to find real solutions to modern business problems.

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.