THE CYBERSIDE BRIEF

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

INSIDE THIS ISSUE

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

MAKE TAX SEASON LESS MISERABLE

Ah, February – love is in the air and Cupid may just have his arrow pointed toward you and a special someone. But Cupid has competition. It's also tax season and scammers are out looking for their special someone(s), too. As if taxes weren't horrible enough on their own, criminals are devising new ways to trick us into tax scams, with horrific consequences.

According to IRS data, tax scams spike in January and February and intensify through April. Last year, scammers targeted numerous business owners by misrepresenting the Employee Retention Credit (ERC), charging hefty fees for assistance with applications – even for a credit many victims didn't qualify for. So many business owners were attacked that the IRS set up an ERC withdrawal program to help those who realized they had unknowingly submitted fraudulent claims.

Popular Tax-Time Scams

Tax scams are particularly tricky because no well-meaning taxpayer wants to make a mistake and get in trouble with the government. Scammers and cybercriminals prey on our fear of compliance issues by posing as IRS agents, tax software providers or even colleagues in financial departments, with urgent messages demanding payment or Social Security numbers.

continued on page 2...

...continued from cover

It may be only February, but these scammers are likely already in your inbox. Take a few minutes to read about these common tax-time scams and what you can do to prevent them.

Phishing And Smishing Scams

Scammers love pretending to be the IRS to get your personal information. They'll send fake e-mails or texts promising refunds or threatening legal action, hoping you'll click on their links or share sensitive details. These scams don't just target individuals – they often go after tax pros and businesses because those can give access to loads of valuable data.

How to prevent it: Never click on links or reply to unexpected messages claiming to be from the IRS. If something feels off, report suspicious e-mails to phishing@irs.gov, and aways verify messages directly with the IRS through official channels.

Online Account "Help"

Scammers are targeting taxpayers by offering help setting up an IRS online account. Their goal is to steal your personal tax and financial information, which they can use for identity theft. These criminals may pretend to be "helpful" third parties, tricking you into handing over sensitive details like Social Security numbers or IDs, which they can use to file fake tax returns and steal refunds.

How to prevent it: Only create your online account directly through IRS.gov and avoid any unsolicited offers for third-party help. If someone reaches out offering to assist, it's probably a scam.

Fuel Tax Credit Scams

The IRS is warning taxpayers about popular scams pushing Fuel Tax Credit claims, which are only available for off-highway business or farming use. Scammers will mislead you by fabricating documents or receipts for fuel to make false claims, often charging hefty fees in the process. While these scammers profit, you are left with the risk of facing IRS scrutiny and potential penalties.

How to prevent it: If you're considering claiming a Fuel Tax Credit, make sure you're eligible, as incorrectly claiming it could lead to serious consequences like fines or criminal charges. Always consult a qualified tax professional to ensure your claims are legitimate.

You Know The Saying: If It Sounds Too Good To Be True, It Probably Is

Many of these scams are plastered all over the Internet, often with promises of tax savings that sound too good to be true. But the old saying still rings true: If something seems too good, it probably is. These schemes might look tempting, but they can land you in hot water with the IRS and lead to serious legal trouble. This year, make tax season a little less miserable by sticking to legitimate, proven methods. You can also check out the IRS Dirty Dozen list with details on all the common tax scams and tips on how to stay safe this tax season.

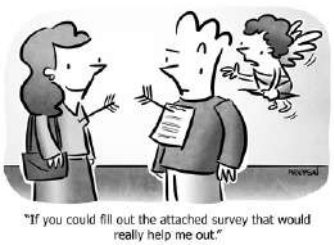
FREE REPORT:

What Every Small-Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems

This report will outline in plain, nontechnical English the common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills, and will provide an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Download your FREE copy today at www.AdRem.com/protect or Call Our Office at (703) 860-2233.

CARTOON OF THE MONTH



Compliancy Navigator

Compliance Pitfalls

5 COMMON MISTAKES THAT PUT YOUR BUSINESS AT RISK

Compliance and cybersecurity go hand in hand, but meeting compliance requirements involves more than just having strong security measures in place. Many businesses unknowingly make critical mistakes that put them at risk of fines, data breaches, and reputational damage. To help your business stay on track, we're breaking down five common compliance pitfalls - and how to avoid them.

MISTAKE #1: ASSUMING CYBERSECURITY EQUALS COMPLIANCE

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.

Having robust cybersecurity protections in place is essential, but compliance requires more than just firewalls and encryption. Each regulatory framework has specific documentation, reporting, and procedural requirements.

Why This Matters:

- **HIPAA:** Requires documented risk assessments and employee training to ensure patient data security.
- **PCI DSS:** Mandates encryption, access controls, and secure transaction procedures to protect payment data.
- **CMMC/NIST:** Demands adherence to strict security baselines, with ongoing audits and system security plans (SSPs) to ensure compliance.

MISTAKE #2: NEGLECTING REGULAR COMPLIANCE AUDITS & ASSESSMENTS

Compliance isn't a one-time event. Regular audits and assessments help businesses identify gaps before they become serious problems.

Why This Matters:

- **HIPAA:** Requires annual risk assessments to identify and mitigate security vulnerabilities.
- **PCI DSS:** Requires quarterly vulnerability scans and annual penetration tests.
- **CMMC/NIST:** Demands continuous monitoring, system security reviews, and documentation updates.

Critical Note: If penetration testing is conducted as part of an audit for CMMC Compliance, it must be FedRAMP-equivalent if it has the potential to access Controlled Unclassified Information (CUI). This ensures that the testing adheres to the same rigorous security standards required for protecting sensitive government-related data and maintains full compliance with CMMC regulations.

MISTAKE #3: POOR EMPLOYEE TRAINING & AWARENESS

Employees are often the weakest link in compliance. Without proper training, they can unintentionally expose an organization to data breaches or regulatory violations.

Why This Matters:

- **HIPAA:** Employees must be trained to recognize and prevent unauthorized disclosures of patient data.
- **PCI DSS:** Staff handling payments must follow secure transaction procedures.
- **CMMC/NIST:** Employees handling CUI must understand security protocols to prevent unauthorized access or leaks.

MISTAKE #4: LACK OF PROPER DOCUMENTATION & POLICY UPDATES

Failing to maintain up-to-date compliance documentation can be as dangerous as not having security measures in place.

Why This Matters:

- **HIPAA:** Requires detailed security policies, documented risk management plans, and breach response strategies.
- **PCI DSS:** Mandates written policies on cardholder data protection and employee security procedures.
- **CMMC/NIST:** Requires ongoing documentation of security controls, incident response plans, and access management procedures.

MISTAKE #5: FAILING TO MONITOR & SECURE THIRD-PARTY VENDORS & SUBCONTRACTORS

Businesses often assume their vendors and subcontractors are compliant, but if they fail to meet regulatory standards, it can put your company at risk.

Why This Matters:

- **HIPAA:** Vendors handling Protected Health Information (PHI) must sign Business Associate Agreements (BAAs) to confirm compliance. Also note, medical service providers do not inherit HIPAA compliance from their vendors—such as using compliant Electronic Medical Record (EMR) systems—and are fully responsible for their own compliance.
- **PCI DSS:** Third-party payment processors must be PCI-DSS compliant to ensure secure transactions.
- **CMMC/NIST:** Subcontractors must be CMMC compliant or capable of working within your company's CMMC security restrictions. If they are not, they could introduce security vulnerabilities and compliance risks.

CONCLUSION

Avoiding these common compliance pitfalls helps businesses maintain regulatory compliance while enhancing their overall cybersecurity posture. By taking proactive steps —such as conducting regular audits, training employees, and ensuring vendors meet compliance standards—businesses can mitigate risks and stay ahead of evolving regulations.

PRESENTED TO YOU BY SHERPA, AN ADREM SYSTEMS COMPANY:

SHERPA An AdRem Company SYSTEMS

THE INFLUENTIAL PERSONAL BRAND:

HOW TO TURN YOUR REPUTATION INTO REVENUE

Many business owners dismiss building personal branding as unnecessary or time-consuming. Yet Rory Vaden, co-founder of Brand Builders Group and author of *Take The Stairs and Procrastinate On Purpose*, argues that a personal brand is essential for earning trust and growing your business. His practical approach makes creating a personal brand much simpler than you think.

Credibility + Recognition = Your Personal Brand

At its core, a personal brand is what people think of when they think of you. Vaden defines it as "the digitization of your reputation." According to recent studies, 74% of Americans are more likely to trust individuals with a personal brand. This trust impacts consumer action, with 63% more likely to buy from companies whose leaders have personal brands.

So why do so many business owners avoid it? Vaden explains that branding is often linked to posting on social media or YouTube – activities that seem annoying or irrelevant. However, he emphasizes that personal branding builds "celebrity authority," a blend of authentic credibility and recognition that is necessary to convince consumers to work with you.

Why Most Personal Brands Fail

"Just because it's simple doesn't mean it's easy," says Vaden. A common mistake is to imitate others' success, leading to diluted focus. "When you have diluted focus, you get diluted results," he says. Instead, the key is to hone in on what makes you unique.

How To Stand Out

"Find your uniqueness and exploit it in the service of others," Vaden advises. Start by answering one crucial question in one word: **What problem do you solve?**

For example, after 10 years dedicated to research on shame, Brené Brown now "owns" the problem of shame and is recognized as the leading authority on the topic. Similarly, Dave Ramsey built an empire by focusing entirely on solving personal debt. "Become an ambassador of the problem," Vaden says. "That's how this works."

To deeply understand your uniqueness, Vaden suggests answering each of the following questions in one word:

1. What problem do you solve?
2. Who do you solve that problem for?
3. How do you solve that problem?
4. What one revenue stream matters most?

If you're struggling to answer those questions, Vaden offers this shortcut: **"You are most powerfully positioned to serve the person you once were."** Sharing your journey makes your message authentic and relatable.

Content That Converts

There's no point in creating a personal brand unless it helps you connect with more customers.

Once you're clear on your uniqueness, Vaden says, it's time to create content that builds trust.

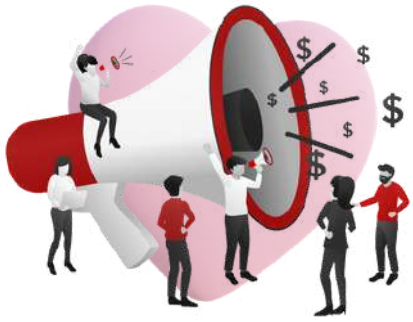
Your content should help customers to:

1. see you (understand what you do);
2. know you (understand who you are);
3. learn from you (solve their problems).

Focus on the "Three E's," Vaden says, creating only content that entertains, encourages and educates. Share relatable stories, inspire your audience and provide practical advice. Standing out isn't simply about what you do but who you are. By focusing on your unique value and creating meaningful content, you can build a personal brand that earns trust and transforms followers into loyal customers.

REFERRAL PROGRAM

Unlock Opportunities This Valentine's Day!



As we celebrate the spirit of love this Valentine's Day, we invite you to be a part of something special!

Your network is your greatest asset, and we believe in the power of connections. While you may not have experienced our services firsthand, your insight and recommendations could spark transformative collaborations.

Refer a business in need of IT or Cybersecurity Assistance to us, and as a token of our appreciation, we'll gift you a $500 gift card for every referral that signs on with us. It's our way of thanking you for trusting us with your connections.

Rest assured; your referred businesses are under no obligation. We prioritize nurturing relationships and providing value above all else.

TO SPREAD THE LOVE:

Scan the QR code, call us directly or visit www.AdRem.com/about-us/referral-program/ to share the love!

TRIVIA

In recent years, reported losses to romance scams have surged. How much money was reported lost to romance scams in 2023?

A. $765.4 million
B. $1.14 billion
C. $33.8 million
D. $67.9 million

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.

CYBERSIDE CHAT

Love isn't the only thing in the air... Apple fixes AirPods' Bluetooth eavesdropping problem.

A flaw was found on Apple AirPods that allowed attackers to connect to your device and even eavesdrop on your conversations. Apple released a new firmware update for AirPods and Beats, so make sure your devices are up-to-date!

Pay for new stuff with your old stuff!

One of the founders of Postmates is back with a new payment service called Tiptop that lets you pay for online purchases by trading in something old. Soon you'll be able to see the service alongside PayPal and Apple Pay when you check out online and you can use it to trade in anything TV-sized or below (sorry, no husbands) to help pay for something new.

Concerned your spouse is ignoring you? Use AirPods to test their hearing.

Millions of people are living with hearing loss and have no idea, so Apple has designed a convenient way to test our hearing. To take the test, you'll need a specific model of AirPods 2 (A2931, A2699, A2698, A3047, A3048, A3049) and an iOS-compatible iPhone or iPad. For full instructions, you can go to www.apple.com/airpods-pro/hearing-health.

Big nostalgia, tiny screen.

TinyTV 2 is a nostalgic novelty – a fully functional mini-TV combining retro charm and modern convenience. This teensy TV has a 1.14-inch screen, working rotary knobs and authentic static effects when changing channels, just like the '80s portable TVs we loved. You can even upload up to 10 hours of your own videos, making it as practical as it is delightful when you're craving a tiny trip down memory lane.

FOR YOUR EYES ONLY:

THE COST OF "FREE" BROWSING

Online interactions fuel companies like Google, allowing them to gather data on your habits and location for targeted ads. While these "free" services seem convenient, they come at the cost of your personal information. This trade-off not only makes ads feel invasive but also exposes you to risks like identity theft and scams.

To protect your online privacy, consider these steps:

1. Use Incognito Mode: Prevent browsers from saving history and cookies.

2. Switch Search Engines: Privacy-focused options like DuckDuckGo avoid tracking.

3. Add Privacy Extensions: Block trackers and secure connections with vetted tools.

4. Use a VPN: Encrypt your connection and hide your IP address on public WiFi.

5. Clear Cookies: Limit tracking by managing or deleting cookies regularly.

With simple measures, you can minimize exposure and reclaim control of your digital footprint.