VOLUME 25
AUGUST 2025

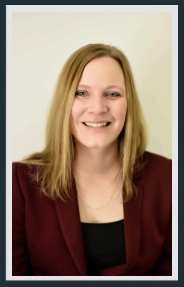
Loyality it's our word.

TECH TALK

NEWSLETTER

In This Edition

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



OUR MISSION:

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

The Compliance Blind Spot: What You're Missing Could Cost You Thousands!

Many small business owners operate under the misconception that regulatory compliance is a concern solely for large corporations. However, in 2025, this belief couldn't be further from the truth. With tightening regulations across various sectors, small businesses are increasingly in the crosshairs of compliance enforcement agencies.

Why Compliance Matters More Than Ever!

Regulatory bodies like the Department of Health and Human Services (HHS), Payment Card Industry Security Standards Council (PCI SSC) and the Federal Trade Commission (FTC) have intensified their focus on data protection and consumer privacy. Noncompliance isn't just a legal issue – it's a financial and reputational risk that can cripple small businesses.

Key Regulations Affecting Small Businesses:

1. HIPAA (Health Insurance Portability and Accountability Act)

If your business handles protected health information (PHI), you're subject to HIPAA regulations. Recent updates emphasize:

- Mandatory encryption of electronic PHI.
- Regular risk assessments to identify vulnerabilities.
- Employee training on data privacy and security protocols.
- Incident response plans for potential data breaches.

Failure to comply can result in hefty fines. For instance, in 2024, the HHS imposed a $1.5 million penalty on a small health care provider for inadequate data protection measures.

Continued on pg. 2

Continued from pg. 1

2. PCI DSS (Payment Card Industry Data Security Standard)

Any business that processes credit card payments must adhere to PCI DSS requirements. Key mandates include:

- Secure storage of cardholder data.
- Regular network monitoring and testing.
- Implementation of firewalls and encryption protocols.
- Access control measures to restrict data access.

Sources say noncompliance can lead to fines ranging from $5,000 to $100,000 per month, depending on the severity and duration of the violation.

3. FTC Safeguards Rule

Businesses that collect consumer financial information are required to:

- Develop a written information security plan.
- Designate a qualified individual to oversee security measures.
- Conduct regular risk assessments.
- Implement multifactor authentication (MFA).

Violations can result in penalties up to $100,000 per incident for businesses and $10,000 for responsible individuals. Scary, huh!

Real-World Consequences Of Noncompliance:

Consider the case of a small medical practice that suffered a ransomware attack due to outdated security protocols. Not only did they face a $250,000 fine from the HHS, but they also lost patient trust, leading to a significant drop in clientele. You have to take responsibility for and control of your data!

Steps To Ensure Compliance:

1. Conduct Comprehensive Risk Assessments: Regularly evaluate your systems to identify and address vulnerabilities.

2. Implement Robust Security Measures: Use encryption, firewalls and MFA to protect sensitive data.

3. Train Employees: Ensure your staff understands compliance requirements and best practices.

4. Develop An Incident Response Plan: Prepare for potential breaches with a clear action plan.

5. Partner With Compliance Experts: Engage professionals who can guide you through the complexities of regulatory requirements.

Don't Wait Until It's Too Late!

Compliance isn't just a legal obligation – it's a critical component of your business's integrity and longevity. Ignoring these requirements can lead to devastating financial penalties and irreparable damage to your reputation. Don't let a compliance blind spot jeopardize your success.

Jess Cole On How To Create Raving Fans!

Jesse Cole built the iconic Savannah Bananas brand from nothing by doing things differently. The key to his success was his "fans first" mindset, which centers on creating an incredible experience for each individual fan.

"Fans aren't buying because of the product," Cole explained. "They're buying it because of how we make them feel. That's the differentiator."

Here are his takeaways for Businessess who want to create raving fans too.

Eliminate Friction:

Put yourself in the customer's shoes and eliminate the friction they experience. Just like Walt Disney used to walk around Disneyland every day to find things to improve, businesses should go through the sales and onboarding process to look for friction points—and reduce them whenever possible.

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 dilemma!

CARTOON OF THE MONTH

"Oh, that. We beefed up security."

Continued from pg. 2

Entertain Always:

The heart of entertainment is to provide enjoyment, according to Cole. "How do you map the journey for your customers, every step of the way, to provide enjoyment and make their lives better?" he said. Think about the little details; there are many stages of the experience of working with you, from first impressions to onboarding. Try to make every stage remarkable. Those interactions set the tone when someone starts working with you.

Experiment Constantly:

And don't just experiment—try the exact opposite of what's normal. Not every experiment will work, but the ones that do have the opportunity to become groundbreaking successes. And people only remember the successes, not all the failures along the way.

Engage Deeply:

"Do for one, what you wish you could do for many," Cole said. The Magic Castle Hotel in Hollywood is a master of this tactic as well; their CEO says the key is to "listen carefully, respond creatively." By creating tailored experiences for individuals, you show your entire fan base that you care deeply for the people who support you.

Empower Action:

"Stop standing still, start standing up," said Cole. "None of it matters if we don't empower first ourselves, and then our team." To this end, he advised businesses to not underestimate the power of a thank you—to your team, your mentors and your clients—when it comes to building raving fans.

Your Phone Can Be Tracked – And It's Easier Than You Think!

Most of us carry our phones everywhere, trusting them with everything from passwords to private business conversations. But here's the unsettling truth: phone tracking is far more common – and easier – than most people realize.

Whether it's a jealous partner, a disgruntled employee or a cybercriminal targeting your business, anyone with the right tools can monitor your location, read your messages or even access sensitive business data without you ever knowing. And for business owners, that puts more than just your privacy at risk. It puts your operations, clients and bottom line in danger.

How Phone Tracking Works:

Spyware Apps: These can be secretly installed to monitor calls, texts and app usage. Some can even activate your microphone or camera without your knowledge.

Phishing Links: Clicking a malicious link in an e-mail or SMS can silently download tracking software onto your phone.

Location Sharing: Apps with excessive permissions or with social platforms you forgot were still logged in might be sharing your location in the background.

Stalkerware: This specific type of spyware is designed to hide in plain sight, often disguised as harmless apps or settings tools.

These methods don't require advanced hacking skills – many are sold commercially under the guise of "monitoring software."

Continued on pg. 4

Continued from pg. 3

Why This A Big Deal For Business Owners...

If you run a company, your phone likely contains more than just personal messages. Think: e-mails with confidential client data, saved passwords, banking access and employee records. A compromised phone can be an open door to your entire business.

The scarier part is the likelihood that you won't realize you're being tracked until it's too late, after an account is drained, a deal is leaked or customer trust is broken.

Consider this: a single data breach costs US small businesses an average of $120,000 (Verizon Data Breach Investigations Report). If your device is the weak link, that breach could start in your pocket at any moment.

Signs Someone Might Be Tracking Your Phone!

If you suspect someone is tracking your phone, here's what to do:

1. Run A Security Scan:

Use a reputable mobile security app to detect and remove spyware or malware. These tools can also monitor your device in real time and alert you to new threats.

2. Check App Permissions:

Go through your app list and review permissions. Disable unnecessary access to location, microphone and camera – especially for apps you rarely use.

3. Update Your Phone:

Security updates often include patches for vulnerabilities that spyware might exploit. Make sure your phone is running the latest OS.

4. Perform A Factory Reset:

If spyware is confirmed and can't be removed easily, a factory reset is the most thorough option. Just make sure to back up critical data and change all important passwords after the reset.

5. Set Up Security Controls:

Use biometric logins (like Face ID or fingerprint) and enable multifactor authentication on critical business apps and accounts.

Don't Leave Your Phone – And Business – Exposed!

Because you're a business owner, your phone is more than a personal device. It's a mobile command center, customer file cabinet and sometimes a virtual vault. That's why keeping it secure should be nonnegotiable.

Cybercriminals are opportunists, and a compromised mobile device gives them an easy way in – no firewall needed.

Stop Phishing Emails Before They Hook You!

Phishing emails are getting trickier, often disguised as urgent requests, invoices, or messages from people you trust. One careless click can expose sensitive data or install malicious software on your device.

How to Stay Safe:

Pause Before You Click: Hover over links to check the real URL before opening.

Verify the Sender: If something feels off, contact the sender through a trusted method—not by replying to the suspicious email.

Use Multi-Factor Authentication (MFA): Even if credentials are stolen, MFA can block attackers from getting in.

Report It: Don't just delete—report phishing attempts to your IT or security team so they can protect others.

Remember, cybercriminals count on you being in a rush. A few extra seconds of caution could save your business from hours—or even days—of costly recovery.

Ready to take your IT to the Next Level?

Scan the QR code and book a 30 Minute Discovery Call with us to learn about what we can do for your IT!