The DIGITAL MINDSET

INSIDER TIPS TO MAKE YOUR BUSINESS RUN FASTER, EASIER AND MORE PROFITABLE

Our Mission:

Honor God, Serve People, Protect Businesses

This monthly publication is provided courtesy of Sean Priddy, President of Alexaur Technology.

What's New:

BOOST YOUR BUSINESS WITH VOIP

Businesses across West Houston are upgrading to VoIP phone systems for seamless, flexible communication.

Unlike traditional phone lines, VoIP uses the internet to deliver crystal-clear calls, lowers monthly costs, and has built-in features like voicemail-to-email, call forwarding & auto-attendants, video conferencing, and CRM integrations.

It's a game-changer for teams working in-office, remote, or hybrid.

VoIP is quickly becoming the go-to choice for SMBs thanks to Houston's expanding fiber network and the need for reliable, boots-on-the-ground support that we provide.

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 cripples businesses.

Key Regulations Affecting Small Businesses

1. **HIPAA (Health Insurance Portability & 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.

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.

Real-World Consequences Of Noncompliance

This isn't just talk. 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!

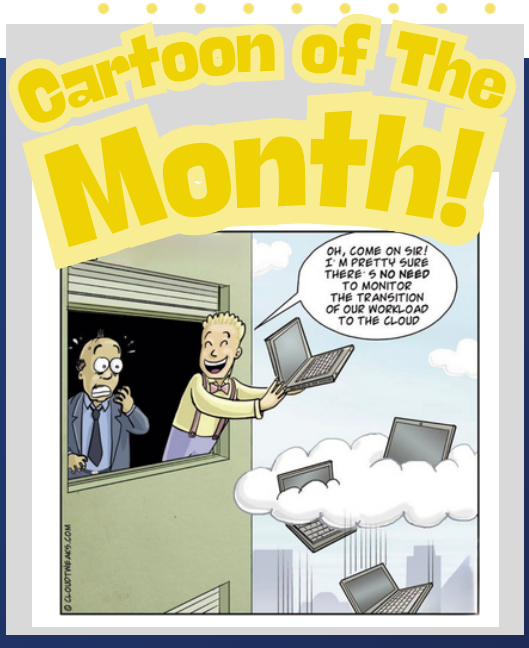
Steps To Ensure Compliance

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.



Know Someone Struggling With IT? GET MONEY By Sending Them Our Way!

At **Alexaur Technology Services,** we believe referrals are the greatest compliment - and they come with **real rewards.**

When you refer a business that becomes a client, we'll thank you with a **CASH REWARD.** It's our way of saying thank you for spreading the word.

You already know the peace of mind that comes with reliable, worry-free IT support. Why not help someone else experience the same- and enjoy a little something in return?

Share the peace of mind. **Get rewarded!**

alexaur.com/referral-program/

Helping others has never been more worthwhile!

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 sad 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

There are several ways someone might track your phone:

Spyware Apps: These can be 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 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."

Why This Is 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 any time.

Signs Someone Might Be Tracking Your Phone

Most spyware tools are designed to operate quietly, but there are still signs to watch for:

- Battery drain that doesn't match usage
- Increased data usage or strange spikes
- The phone feels hot when idle
- Unexplained apps or icons
- Background noise during calls
- Frequent crashes/unresponsive screens

These symptoms don't guarantee your phone is compromised, but when paired alongside other unusual behavior, they're worth investigating.

How To Stop Phone Tracking

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, complete the reset and then change all important passwords.
5. Set Up Security Controls: Use biometric logins (like Face ID or fingerprint) and enable multi-factor authentication on business apps.

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 a priority.

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