Connectability Corner
PUTTING THE PIECES TOGETHER.
Powered by: Connectability
Insider Tips To Make Your Business Run Faster, Easier And More Profitably

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 and industry standards are placing increased emphasis on data protection, privacy, and cybersecurity. Laws like the Personal Information Protection and Electronic Documents Act (PIPEDA), Ontario's PHIPA, and Canada's Anti-Spam Legislation (CASL) are evolving to hold businesses accountable for how they collect, store, and use personal information.

Noncompliance isn't just a legal issue – it's a financial and reputational risk that cripples businesses.

Key Regulations Affecting Small Businesses

1. PHIPA (Personal Health Information Protection Act)

If your organization handles personal health information (PHI) in Ontario, you must comply with PHIPA. This applies to healthcare providers, community organizations, and any business acting as a health information custodian or service provider.

Key requirements include:

- Encrypting electronic PHI
- Conducting regular risk assessments
- Training staff on privacy and security
- Establishing breach response procedures

Non-compliance can lead to investigations, fines, and reputational damage. The Information and Privacy Commissioner of Ontario (IPC) has increased enforcement in recent years — even small clinics have faced penalties for inadequate safeguards.

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.

continued on page 2...

...continued from cover

- **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. Protecting Financial Information

Canadian businesses that handle consumer financial or personal information must comply with privacy laws such as PIPEDA (federal) and Law 25 (Quebec), which set clear expectations for data protection. Key requirements include:

- Maintaining a written privacy and security policy
- Appointing a privacy officer to oversee compliance
- Conducting regular risk assessments
- Implementing safeguards like encryption and multifactor authentication (MFA)

Under Law 25, serious violations can result in fines of up to $25 million or 4% of global revenue.

Real-World Consequences Of Noncompliance

This is 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 heavy fine, 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.

Earn $1,000 by Referring a Business to Us!

We know that great businesses are built on strong connections, and we'd love your help connecting with organizations that need reliable IT support. To show our appreciation, we're offering $1,000 for every qualified referral - even if they don't become a client!

How It Works:
1. Refer a business with 10+ computer users in the GTA.
2. Make an introduction via phone or email.
3. If they book and attend a Free IT Cybersecurity Risk Assessment, you earn $1,000 - no strings attached.

Who Makes a Great Referral?
We're looking to connect with CEOs, Executive Directors, or IT Managers in any industry that relies on technology. Some great examples include financial services, real estate, professional services, property management, wholesale distribution, and manufacturing - but any growing business with IT needs is a great fit!

Know Someone? Let's Make It Easy!
Whether it's a client, vendor, or colleague, simply introduce us, and we'll take it from there.
We're even happy to co-host a webinar, seminar, or special offer for any business groups you belong to.

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 businesses 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.

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 [the rest 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.

CYBERSECURITY TOOL OF THE MONTH

MANAGED DETECTION & RESPONSE

MDR is a fully managed cybersecurity service that continuously monitors your environment, detects suspicious behavior in real time, and responds to threats before they impact your business.

You get expert-level protection – without needing to build an internal security team.

Why It Matters

1. Most cyberattacks happen after business hours – MDR never sleeps
2. Traditional antivirus and firewalls miss modern threats
3. Early detection can prevent costly downtime and data loss
4. Cyber insurance providers increasingly expect or require MDR-level protection

Monthly Charity Donation

Save Fur Pets

This month, we're proud to support Save Fur Pets Rescue, a volunteer-run charity based in Ontario dedicated to rescuing, rehabilitating, and rehoming abandoned and neglected animals.

As shelters across the province face overwhelming intake numbers, every act of care matters. By supporting grassroots rescues like Save Fur Pets, we help give vulnerable animals a second chance at life in loving, permanent homes. Let's continue to raise awareness, promote adoption, and stand behind the people doing this compassionate work every day.

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 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.