JOIN THE FIGHT: BLADDER CANCER CANADA WALK COMES TO PRINCE EDWARD COUNTY

On September 20th, Prince Edward County will host a powerful gathering of hope, resilience, and community spirit as part of the 15th annual Canada Walks for Bladder Cancer. Organized by Bladder Cancer Canada, this national initiative unites patients, families, and supporters to raise awareness and critical funds for bladder cancer research and support services.
Bladder Cancer in Ontario: A Closer Look
Bladder cancer is the 5th most commonly diagnosed cancer in Canada, and Ontario sees a significant share of these cases. Each year:

- 13,400 Canadians are diagnosed with bladder cancer—37 people per day
- Over 80,000 Canadians are currently living with the disease
- Men are twice as likely to be diagnosed as women
- The disease has a 60–70% recurrence rate, making ongoing support and research essential

Despite its prevalence, bladder cancer remains one of the most expensive cancers to treat per patient, and awareness is still relatively low.

JOIN OUR TEAM

Celebrating 15 Years of Impact
Founded in 2009 by two bladder cancer survivors, Bladder Cancer Canada has grown into a national force for change. Over the past 15 years, the organization has:

- Provided peer support, educational resources, and online forums for patients and caregivers
- Funded innovative research into diagnosis and treatment
- Hosted annual walks across Canada, raising over 60% of its funding through these events
- Partnered with medical professionals to improve outcomes and raise awareness

This year's walk is not just a fundraiser—it's a celebration of how far the community has come and a recommitment to the work still ahead.
Call to Action: Walk With Us
Whether you're a survivor, caregiver, supporter, or simply someone who wants to make a difference, your steps matter. Join us in Prince Edward County on September 20th to walk in solidarity and support. Register today by calling 1-800-674-8889 Or email walk@bladdercancercanada.org
Together, we can turn awareness into action—and hope into healing.

Join our team https://fundraise.bladdercancercanada.org/ui/CWFBC25/t/b6f61d6f80094e9b903cfcf4f80ada79 or start our own at https://fundraise.bladdercancercanada.org/ui/CWFBC25/g/PEC

ATTITUDE CHRONICLE
Insider Tips To Make Your Business Run Faster, Easier And More Profitably

WHATS ON

August marks a powerful checkpoint for businesses, making it the perfect time to spotlight the value of running a cybersecurity Audit. A well-timed audit uncovers hidden risks, strengthens internal processes, and sharpens long-term strategy. It's not just about compliance — it's about clarity and control. If your business is taking advantage of some downtime, now is a great time to run an audit using your insurance check list or run a more in-depth pen test.

Our Day at the Races with Huntress was a thrilling, read all the details on page 2. Operation Backpack is in full swing, supporting students as they prepare for the school year. Huge thanks to Kalon Services Inc. for partnering with us to support Ignite Durham. Don't forget — Drop-Off Day is August 15th at noon If you would like to join us or have items to donate let our team know at 416-900-6047.

Our next Cyber Brews Series announcement is just around the corner, keep your eyes peeled on our Linked-In and Webpage for the next announcement.

Coming up in September join our team to walk in support of Canada Walks for Bladder Cancer. Search for our team: The Shores Team, we will be walking in Prince Edward County on September 20th. Hope to see you there, after party to follow!

Brandon Jones
CEO Attitude IT

HOW TO TELL IF YOUR BUSINESS HAS SUFFERED A DATA BREACH — AND WHAT TO DO ABOUT IT

While some breaches are glaringly obvious, others slip in unnoticed until serious damage is done. Knowing how to spot early signs — and how to respond effectively — can make all the difference.

Not all data breaches are obvious—some quietly erode trust and cause damage before being discovered. Recognizing early indicators is critical to minimizing impact.
Common Red Flags:

- Unusual Account Activity: Suspicious logins, password resets, or unauthorized changes
- Network Spikes or Slowdowns: Unexpected outbound traffic or sluggish systems
- Missing or Tampered Data: Unexplained deletions or edits to files
- Security Alerts: Warnings from antivirus or intrusion detection tools
- Ransom or Extortion Attempts: Direct messages from attackers demanding payment

Quick action in response to these signs can help contain the breach and protect your business.

What to Do If You Suspect a Breach
Acting quickly and decisively is key. Here are some practical steps:

- Isolate Affected Systems
- Disconnect compromised devices or servers from your network to contain further damage.
- Engage Your Incident Response Team
- Whether internal or external, security experts should assess the scope and nature of the breach immediately.
- Preserve Evidence
- Secure logs, emails, and any relevant data for forensic investigation — don't delete anything until reviewed.
- Notify Stakeholders
- Transparency is crucial. Inform affected customers, partners, and regulators as required.
- Reset Credentials
- Change passwords and revoke access to impacted systems. Ensure multi-factor authentication is enabled.
- Review & Strengthen Defenses
- Conduct a post-incident analysis and patch vulnerabilities. Update security policies and employee training.

CONTINUED FROM PAGE 1

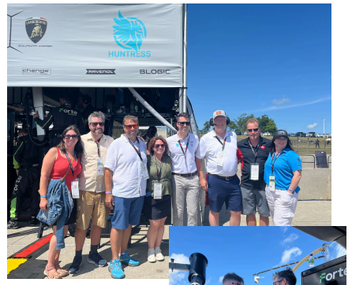
Prevention Is the Best Medicine
While no defense is impenetrable, a proactive cybersecurity strategy acts as your business's immune system — ready to detect, respond, and evolve with emerging threats. Think of it not just as technical hygiene but as a culture of vigilance. Here's how to fortify your defenses:

- Regularly Update Software & Systems
- Apply patches as soon as they're released. Outdated software is one of the most common attack vectors — and one of the easiest to fix.
- Conduct Regular Security Audits & Penetration Testing
- Routine assessments identify vulnerabilities before bad actors exploit them. External audits bring an unbiased view of your security posture.
- Educate Employees Continuously
- Human error is still the leading cause of breaches. Offer ongoing training on phishing, password hygiene, data handling, and mobile device security.
- Implement Multi-Factor Authentication (MFA)
- A single compromised password shouldn't be a gateway to your systems. MFA adds an essential layer of protection.
- Use Endpoint Detection and Response (EDR) Tools
- Go beyond basic antivirus: use tools that monitor behavior, detect anomalies, and respond to threats in real time.
- Segment Your Network
- Limit access between internal systems so a breach in one area doesn't allow full network infiltration.
- Encrypt Sensitive Data
- Whether in transit or at rest, encryption ensures stolen data remains unusable.
- Back Up Critical Data Frequently
- Secure, offsite backups help you recover quickly from ransomware or accidental data loss.
- Establish and Test Your Incident Response Plan
- Don't wait for an emergency to find out what's broken. Run drills to identify gaps in your preparedness.

Even a minor breach can snowball into financial loss, regulatory scrutiny, and damaged relationships. But with layered protection, a strong security culture, and an agile response plan, your business can turn risk into resilience.

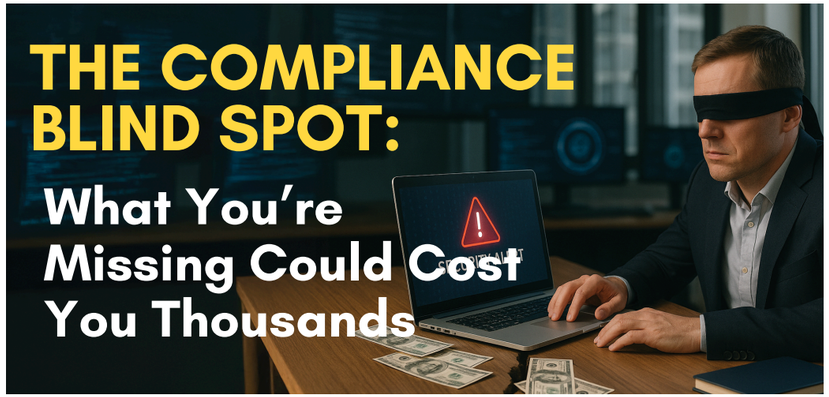
CARTOON OF THE MONTH

A Day at the Races with Huntress



Kyle Hanslovan Huntress CEO invited our team to take part the Chevrolet Grand Prix at Canadian Tire Motorsports Park. The day was thrilling! The day started with meeting the drivers and pit team, watching the tests being completed getting the car ready for the track. Walking the car line up and watching the air show and steel band perform. It was an incredible day. Our team even was super lucky to be at the pit during the driver change. All while chatting with our industry partners, hearing about the latest cyber criminal take downs and best practices

At these events it is a great opportunity to speak with others in our industry and chat about what is working well in security and the areas for improvement. The biggest topic, MFA (Multifactor Authentication) the importance of having this in place across the board for all employees as 94% of breaches start through email. The next line of defence is to make sure to use an authenticator app as your second method of authentication. Text message authentication needs to be upgraded as mobile devices posse a risk of getting intercepted. Join us at our cyber brews event to learn more about industry insights, next event to be announced soon!



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 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.

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 & FTC Safeguards Compliance
- To protect consumer financial data, businesses must enforce strict access controls and adhere to the FTC Safeguards Rule, which requires:
- A written security plan
- A designated security officer
- Regular risk assessments
- Use of multifactor authentication (MFA)
- ⚠️ Noncompliance risks serious penalties:
- Up to $100,000/month for data violations
- $100,000 per incident for businesses
- $10,000 per incident for individuals
- Now's not the time to cut corners on cybersecurity.
- Scary, huh!

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 $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

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

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

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

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

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

Don't Wait Until It's Too Late
Don't let a compliance blind spot jeopardize your success.
.