SECURITY & AWARENESS TRAINING QUARTERLY NEWSLETTER

2026 Q1

HAVE YOU SIGNED UP FOR YOUR TECH TIPS YET?

Designed for busy professionals, these concise and practical insights take less than a minute to read, making them the perfect addition to your routine.

From safeguarding sensitive data to enhancing system security, these tips provide valuable strategies to protect yourself from ever-evolving cyber risks. Signing up is easy and completely free, empowering you to stay informed and proactive without any hassle.

Sign Up for your FREE Tech Tips Today!

CLICK HERE *or go to https://links.sysoft.ca/tip-of-the-week/*

This quarter's publication is provided courtesy of:

Alex Sochka
Director, Operations

Carl Dankwah
Technical Dispatch

What's New

Welcome to this quarter's Security & Awareness Training Newsletter, curated for Canada's discerning professionals committed to safeguarding their organizations.

In this edition, we delve into "Just Start: A Conversation on Cybersecurity, Compliance, and Canadian Innovation," drawing on expert perspectives from Scott Weingust, President of Sysoft, and Steve Gregory, President of 123 Cyber.

Participate in our 2026 Q1 security poll, which explores best practices in Device Hygiene and Habits. For those interested in trend analysis, we also present the findings from the 2025 Q4 poll.

Ask The Analyst returns for your security questions, and we spotlight Bitwarden as a recommended safety tool.

Continue to stay vigilant and exercise sound judgement: cybersecurity is a shared responsibility among Canada's leaders.

WHAT'S INSIDE THIS ISSUE?

Just Start: A Conversation on Cybersecurity, Compliance, and Canadian Innovation

Q1 Security Poll

Ask The Analyst

Safety Tool

Q4 Security Poll Results

Team Message

CyberSecurity Double Puzzle

JUST START: A CONVERSATION ON CYBERSECURITY, COMPLIANCE, AND CANADIAN INNOVATION

Sysoft and 123Cyber Leaders Discuss the Realities and Roadmap of Modern Risk Management

Featuring: Scott Weingust and Steve Gregory

In an era where cyber threats are evolving faster than ever, two Canadian technology leaders—Scott Weingust, President of Sysoft, and Steve Gregory, founder of 123 Cyber—sat down for a candid conversation on the challenges and strategies facing small and medium-sized businesses. Their message?

"Just start."

This deceptively simple advice is a powerful counter to the inertia that plagues so many organizations. As Weingust puts it, “Those are the two words that we really push on all of the people that we meet. Just start.” The fear of not knowing the perfect standard, the right technology, or the ideal partner can be overwhelming. But as anyone who has wrestled with compliance knows, waiting for absolute certainty is a luxury no Canadian SMB can afford.

The path to compliance and effective risk management is, by nature, messy and often frustrating. Consider the experience of organizations that have spent years untangling which standards to follow, which vendors to trust, and which tools are actually necessary. The reality is that even experts admit to lengthy periods of research and trial—proof that there’s no overnight solution or one-size-fits-all approach.

What’s most important is a shift in mindset: moving from simply reacting to problems after they occur to actively seeking them out before they manifest. As Weingust notes, “With a proper set of tools... if something comes up, the problem with those is they're just reactive all the time. There's no proactive... there's no looking for problems before they happen.” True cybersecurity maturity means developing systems and habits that anticipate threats, not just respond to them.

(At its core, cybersecurity isn’t about ticking compliance boxes—it’s about reducing risk in meaningful ways. Gregory explains, “You and I are really in the risk reduction business—your cybersecurity, all it does is reduce the risk. They still have risk, but it reduces their risk.” No organization can eliminate risk entirely, but through deliberate, ongoing effort, risk can be managed and minimized. The journey demands a willingness to embrace imperfection and to view each step as progress, not as a final destination.

The Canadian regulatory environment is evolving to encourage precisely this approach.

With frameworks like Bill C8 and the Canadian Program for Cybersecurity Certification Level 1 bringing “basic hygiene” controls into focus, Gregory points out, “It's basic hygiene. It's only 17 controls. It's completely doable.” The message from policymakers is clear: foundational security is both achievable and expected. Seventeen controls might sound daunting, but they are designed to be accessible—a practical starting line for SMBs across the country.

The biggest obstacle for most organizations isn’t technical complexity; it’s the hesitation to begin. The call to action isn’t to wait for the stars to align, but to step forward—imperfectly, but decisively. As Weingust says, “The only way to do it is with both feet and just jump in and get started.” Dive in, learn as you go, and embrace the discomfort of not having all the answers on day one.

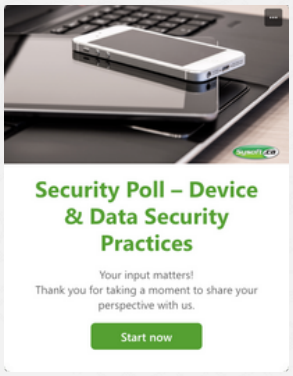
In a world where hesitation is itself a risk, the most innovative thing a Canadian SMB can do today is to take that crucial first step. The journey to robust cybersecurity and compliance starts not with mastery, but with momentum.

Want to learn more?

Watch the full video for the complete conversation and additional takeaways.

Discover their practical advice, hear the real-world stories, and get actionable insights that can help your organization future-proof its operations.

Go to https://youtu.be/R6sqr1cN9Xg
or scan the QR code



2026 Q1 SECURITY POLL: DEVICE HYGIENE & HABITS

Calling all guardians of cyber space, take our security poll and help us defend you against digital threats!
Your participation in this poll is essential for strengthening how you and your colleagues protect devices and sensitive data. By reflecting on your own security habits and identifying where support is needed, you help create a safer workplace and reduce the risk of cyber threats for everyone.

https://links.sysoft.ca/securitypoll

ASK THE ANALYST

Cybersecurity can feel like a maze of unfamiliar terms, constant updates, and ever-changing threats. That's why we've created Ask the Analyst. A place where we break down common questions into clear, practical answers you can actually use.

What is the most common cybersecurity risk organizations underestimate today?

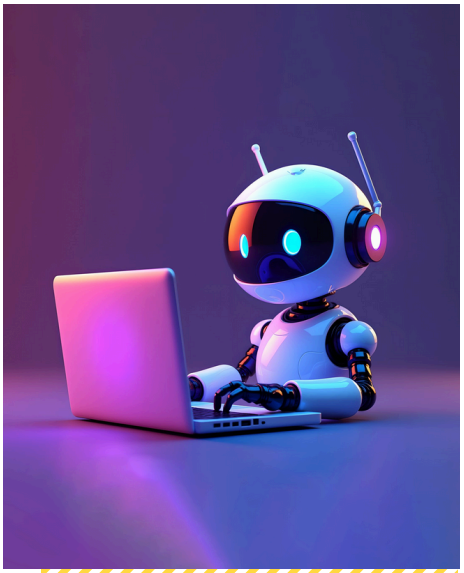
One of the most underestimated risks is identity-based attacks, such as credential theft via phishing or MFA fatigue. Rather than exploiting software vulnerabilities, attackers increasingly target users directly —using social engineering to gain legitimate access. Once inside, they can move laterally without triggering traditional security alerts, making identity protection just as critical as network security.

What role does employee training really play in preventing cyberattacks?

Employee training is a critical first line of defence because many attacks begin with human interaction, most commonly phishing. Well-trained employees are more likely to recognize suspicious emails, report incidents quickly, and avoid risky behaviours. While training alone won't stop every attack, it dramatically reduces the success rate of social engineering campaigns when combined with technical controls.

What's one quick cybersecurity habit everyone should build into their daily routine?

Regularly reviewing account activity and



security alerts is a small habit that pays off quickly. Unexpected login notifications, password reset emails, or unfamiliar transactions are often early warning signs of compromise. Catching these early makes recovery far easier and helps limit potential damage.

Is using public Wi-Fi still risky, or is that outdated advice?

Public Wi-Fi still carries risks, especially if the network is unsecured or fake (set up by an attacker to look legitimate). While modern encryption helps, sensitive activities like online banking or work logins should be avoided on public networks. Using a trusted VPN and ensuring websites use HTTPS can significantly reduce exposure when public Wi-Fi is unavoidable.

Do you have a question for the Analyst?
Submit your question to the asktheanalyst@sysoft.ca and if your question is answered on an upcoming newsletter you'll receive a $25 gift card!

SAFETY TOOL OF THE QUARTER

Bitwarden

Bitwarden is an open-source password manager that keeps your passwords and sensitive information secure using end-to-end, zero-knowledge encryption—meaning only you can access your data.

https://bitwarden.com/

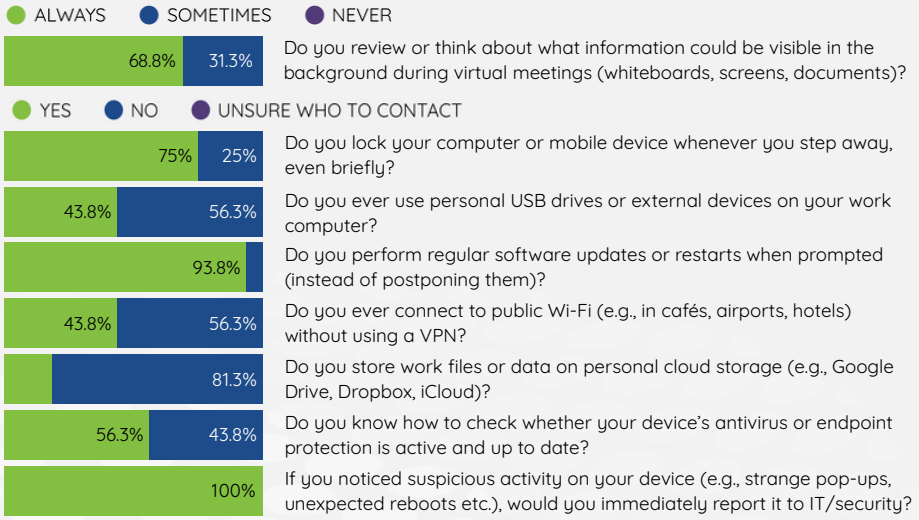
Why It's Useful:

- **Secure by Design:** Protects your data with end-to-end, zero-knowledge encryption—only you can access your vault.
- **Transparent & Trusted:** Fully open-source and independently audited, offering confidence through public scrutiny.
- **Unlimited Syncing:** Even the free plan allows unlimited passwords across unlimited devices.
- **Works Everywhere:** Compatible with all major operating systems, browsers, and mobile devices.
- **Easy to Use:** Features password generation, autofill, secure sharing, and simple import from other password managers.
- **Budget-Friendly:** Offers a generous free tier plus low-cost premium upgrades.

With transparent, independently audited security, Bitwarden provides a reliable and affordable way to strengthen your digital safety.

To view our full library of newsletters go to:
www.sysoft.ca/newsletters
or scan the QR code

Trojan, Malware, Threat, Risk, Access Control, Social Engineering, Sandboxing, Backdoor, Exploit, Security Policy, Incident, Behavioural Analytics
Phishing hooks are everywhere—don't bite



2025 Q4 SECURITY POLL RESULTS

TOPIC: Device & Data Security Practices

An analysis reveals 3 key insights:

1) Most respondents do not store work files or data on personal cloud storage, indicating good adherence to data security policies regarding cloud usage.
2) While most perform regular software updates, a notable minority (over 43%) admit to connecting to public Wi-Fi without a VPN and using personal USB drives or external devices on work computers, highlighting areas where risky behaviours are still present and could be improved.
3) The majority consistently lock their devices when stepping away and report suspicious activity to IT/security, reflecting strong device security awareness and incident reporting habits

A Message From Your Cybersecurity Team

As the calendar turns and 2026 begins, from the desks of the Sysoft Security Team, we offer this New Year's reflection: **cybersecurity is no longer a niche concern reserved for IT departments.**

In today's interconnected environment, each new innovation ushers in opportunities for growth, collaboration, and creativity. But it also opens doors for increasingly sophisticated attacks. Ransomware, social engineering, and data breaches are more than headlines—they are real-world challenges we must face together.

The strength of cybersecurity lies in our collective vigilance: every password you strengthen, every suspicious email you flag, every update you install becomes a brick in the wall of defence against cyber criminals.

As we look ahead, the landscape of cybersecurity demands more than technical solutions; it calls for a culture of awareness and shared responsibility. Whether working from home or in the heart of our offices, every member of the Sysoft community plays a vital role in keeping our systems secure. **Training, open dialogue, and a willingness to learn from both triumphs and mistakes will define our resilience in the year to come**.

Let this be our resolution: to stay alert, informed, and united against cyber threats. Together, we can build a foundation of safety that empowers innovation rather than stifling it. The journey ahead may be unpredictable, but with vigilance and collaboration, we can meet every challenge head-on.

Stay safe, stay smart, and let's make 2026 our most secure and successful year yet.

CYBERSECURITY DOUBLE PUZZLE

JNTORA (9)

SIBDOXNNGA (25 29 3)

RPCCIUOYESYLIT (4 15 14 31 20) (30)

MARLAWE (21 13)

CRDOABKO (11)

OCLSTOARCSENC (23 10)

HRTTEA (5)

LIEOXTP (22 1 26 28)

NEIICESORINELGNGA (32 8 24)

SRKI (6 12)

IDNENTIC (27 16 7)

UHALSANRICETAYIBVLAO (18 2 17 19)

1 2 3 4 5 6 7 8 — 5 9 10 11 12 — 13 14 15 — 16 17 18 19 20 21 2 22 23 24 — 25 26 27 ' 28 — 29 30 31 32