SECURITY & AWARENESS TRAINING QUARTERLY NEWSLETTER

2026 Q2

WHAT'S INSIDE THIS ISSUE?

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

https://links.sysoft.ca/tip-of-the-week/

This quarter's publication is provided courtesy of:

Scott Weingust
Founder, President

WHEN HACKERS DON'T TARGET YOU, THEY TARGET SOMEONE YOU TRUST

Why Supply Chain Attacks Are a Growing Risk for Professional Firms

By: Scott Weingust

At Sysoft, we talk a lot about CARE, delivering a Consistent and Reliable Experience with technology. One of the biggest threats to that consistency today isn't an obvious cyberattack.

It's trust being quietly abused.

Over the past year, attackers have increasingly stopped trying to "break in" directly. Instead, they've shifted to a more efficient strategy. They compromise trusted vendors — including IT providers — and inherit access.

This is why supply chain and MSP-targeted attacks are now one of the fastest-growing cybersecurity risks for professional services firms.

What Is a Supply Chain Cyberattack?

A supply chain cyberattack happens when attackers compromise a trusted third party — such as a software vendor, cloud platform, or managed IT provider — to gain indirect access to client environments. Rather than attacking dozens of organizations individually, attackers compromise one trusted relationship and scale from there.

Threat intelligence reports show a sharp increase in attacks exploiting:

- Vendor credentials and integrations
- Remote management tools
- Trusted software updates
- Identity relationships between organizations

Major industry reports confirm that supply chain and third-party compromises have increased dramatically over the past five years, largely because they provide speed, scale, and stealth. [ibm.com]

Why MSPs Are High-Value Targets

Managed Service Providers aren't targeted because they're careless. They're targeted because they're trusted.

A modern MSP legitimately manages:

...continued on page 2

2026 Q2 SECURITY POLL: CYBER RISK READINESS

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

...continued from page 1

- Administrative access
- Endpoint and device management
- Backup and recovery systems
- Cloud tenant configurations
- Identity and security controls

Recent MSP-focused threat reports show that attackers are increasingly abusing valid credentials and trusted access, rather than relying on new malware or zero-day exploits. [markets.bu...nsider.com]

In practice, this means:

- Attacks often look like normal activity
- Traditional security tools may not trigger alerts
- Damage can occur before anyone realizes access was misused

From an attacker's perspective, it's efficient. From a business perspective, it's disruptive — and often invisible until it's serious.

Why This Matters to Your Firm

Many organizations assume that outsourcing IT also outsources risk.

It doesn't.

Regulators, insurers, and courts increasingly expect organizations to:

- Understand third-party risk
- Perform reasonable vendor due diligence
- Maintain oversight of privileged access
- Respond quickly and decisively to incidents

Global cybersecurity outlooks now classify supply chain exposure as a board-level business risk, not an IT detail. [www3.weforum.org]

Why Traditional Security Often Misses These Attacks

Supply chain attacks succeed because they don't behave like "classic" cyberattacks, rather they use:

- Use valid credentials
- Operate through approved tools
- Blend into normal workflows
- Exploit assumptions of trust

As one major threat report put it: attackers no longer need to "break down the front door" if they can walk in using trusted access. [ibm.com]

This is why organizations sometimes only discover an issue after:

- Data has already been accessed or exfiltrated
- Backups have been interfered with
- Extortion or ransomware demands appear

What CARE-Driven IT Looks Like Today

A Consistent and Reliable Experience doesn't come from piling on tools. It comes from intentional control of trust.

At Sysoft, modern MSP security focuses on:

- Identity-first security design
- Continuous monitoring of privileged activity
- Strong separation between client environments
- Clear, documented incident response coordination

In other words: Trust is no longer assumed, it's continuously verified.

The Bottom Line

Supply chain attacks work because they exploit something human: Trust.

Organizations that handle this best aren't the most paranoid, they're the most prepared. They ask better questions, demand visibility, and insist on consistency in how access is managed.

That's what CARE looks like in practice.

CALL TO ACTION

5-Question Supply Chain Risk Checklist

If you're not sure how exposed your organization is, start here. Ask yourself:

1. Who has administrative access to our systems today (including third parties)?
2. Which vendors or providers can log in as us, not just support us?
3. How is that access restricted, monitored, and reviewed?
4. What would happen if one of our vendors was compromised tomorrow?
5. How quickly would we know, and who would be responsible for responding?

If any of these answers are unclear, that's not a failure, it's a signal.
Clarity is the first step toward a more consistent and reliable technology experience.

CYBERSECURITY NEWS THIS QUARTER

www.getcybersafe.gc.ca

CLICK TO READ MORE

Protecting yourself from telemarketing and retail scams over the phone

www.thehackernews.com

CLICK TO READ MORE

Google Adds 24-Hour Wait for Unverified App Sideloading to Reduce Malware and Scams

www.bleepingcomputer.com

CLICK TO READ MORE

Critical Microsoft SharePoint flaw now exploited in attacks

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.

Ransomware is our biggest fear. If the worst happens, how do we make sure we can recover without paying?

Ransomware resilience means you can reliably recover, so your backups must be routinely tested and trustworthy.

For professional services firms, we also focus on restoring what matters most first, email, documents, line-of-business apps, and validating that restores work before you need them. Good backups turn ransomware into a disruption, not a catastrophe.

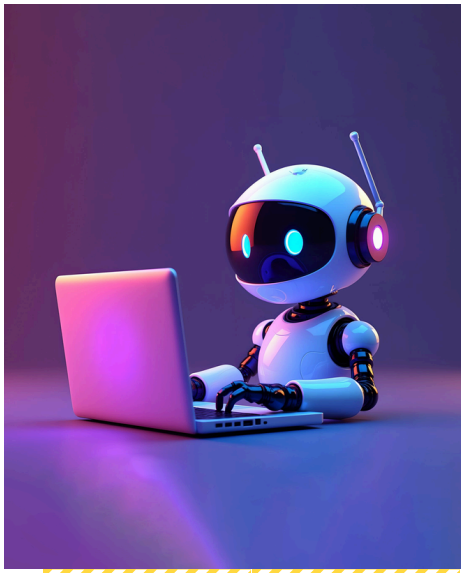
Our team works from home, the office, and on the road. What's a realistic security baseline for laptops and cloud apps?

A practical baseline has four pillars:

- **Strong Identity:** push beyond 'just MFA' toward phishing-resistant MFA methods where possible. Traditional MFA methods like SMS and basic push prompts are increasingly vulnerable to modern tactics, prioritize stronger approaches such as passkeys and platform authenticators.
- **Healthy Devices:** consistent patching, encryption, and modern endpoint protection—plus ensure you have the ability to isolate a device quickly if suspicious behavior appears.
- **Visibility:** a staffed security operations function and monitoring help catch what humans miss.
- **People Training:** ongoing security awareness training matters—because one click can bypass great tooling.

We're a small firm and we live in Microsoft 365. What's the single most effective step we can take to reduce account takeovers?

While we know we talk about the importance of MFA constantly, however implementing MFA really is one of the most effective steps to protect your accounts from unauthorized access. The use of MFA



makes businesses dramatically less likely to be compromised.

Despite this, many organizations still haven't made it standard practice, often due to perceived complexity or change fatigue.

MFA adds a second proof of identity, so a stolen password isn't enough to get in. Our rule is simple: if you didn't just try to log in, deny the prompt and report it immediately. That one habit prevents a surprising number of breaches.

We've seen stories about fake invoices and 'CEO emails' that look real. How do we reduce business email compromise?

Email fraud is a top threat for professional services because it targets trust and payment workflows. There are two layers: technical controls and process controls.

On the technical side, we harden domains using tools like SPF, DKIM, and DMARC so criminals can't easily spoof your firm's 'From' address. We also treat domain spoofing protection as foundational, along with monitoring and user training, as it reduces the volume of convincing impostor emails.

On the process side, we recommend a simple rule: if an email changes bank details, payment timing, or urgency, verify using a known phone number or a separate channel.

Technology blocks a lot, workflow and zero-trust employee habits discipline blocks the rest.

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

INKY®

INKY is an advanced email security platform that protects users from phishing, malicious links, and impersonation attempts by analyzing emails after they arrive in the tenant—exactly where threats actually occur.

Why It's Useful:

- **Real-Time Phishing Detection:** INKY inspects emails after delivery and identifies phishing, business email compromise (BEC), and impersonation attacks that often bypass standard email filters.
- **Clear, Visual Warnings:** Dangerous emails are clearly labeled with banners explaining why the message is risky.
- **AI & Human Intelligence Combined:** Powered by machine learning and reinforced by human threat analysts, INKY continuously adapts to real-world attack techniques.
- **Works Behind the Scenes:** INKY integrates seamlessly with no changes to how users send or receive email.
- **User-Controlled Allow & Block Lists:** Each user has their own INKY allow/block account, allowing the ability to safely manage trusted senders and block unwanted or suspicious emails—without impacting other users.
- **Security Awareness Built In:** By explaining threats directly in the inbox, INKY actively improves user awareness and reduces risky clicking over time.

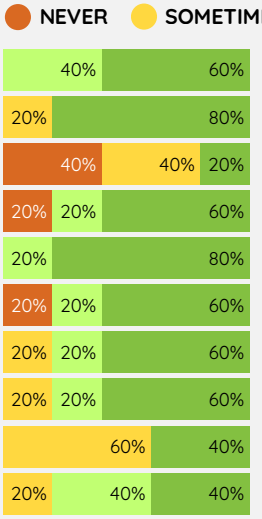
Protect your inbox today—ask to your MSP about INKY and experience smarter email security for you and your business.

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

Puzzle Phrase: Your First Line of Defence is Awareness

2026 Q1 SECURITY POLL: RESULTS & ANALYSIS

TOPIC: DEVICE & DATA SECURITY PRACTICES



- **Strong Device Hygiene Practices:** Most participants regularly back up files, use antivirus software, and keep their systems updated. These actions are crucial for preventing data loss, blocking malware, and patching security vulnerabilities, strengthening overall cybersecurity.
- **Inconsistent Management of Apps and Updates:** There is less consistency in removing unused apps/extensions. Neglecting this can leave devices exposed. Additionally, many participants are not confident in identifying legitimate software updates. This uncertainty can lead to accidental installation of fake updates, which are common vectors for malware and phishing attacks, thus undermining device security.
- **Opportunities for Improved Security Behaviour:** Many do not separate work and personal accounts/devices or regularly restart devices for updates. Failing to do so can blur security boundaries and delay critical updates, making systems more vulnerable to attacks.

A MESSAGE FROM YOUR CYBERSECURITY PARTNER

Spring is an ideal opportunity for organizations to reset—reviewing priorities, streamlining processes, and addressing items that may have been deferred during busier months.

Cybersecurity benefits from the same kind of focused attention.

Many cybersecurity incidents aren't triggered by a single major oversight, but from minor issues that quietly accumulate over time: access that was never removed, updates that were postponed, or controls that haven't kept pace as the business evolves. Routine, thorough attention to these details is essential for maintaining a reliable security posture.

From a leadership perspective, these details carry weight as they directly impact financial exposure, regulatory compliance, and operational resilience. Outdated permissions or untested backups can complicate audits, impact cyber insurance coverage and eligibility, or prolong downtime when something goes wrong. In many cases, the most costly incidents result not from sophisticated attacks, but from neglecting basic safeguards..

A periodic "spring cleaning" of cybersecurity controls is a practical way to mitigate risk. Reviewing who has access to critical systems, ensuring updates and patches are current, and confirming recovery plans reflect your current operations are all critical steps that contribute to a more reliable and resilient organization.

These regular proactive check-ins are not about finding fault or assigning blame, they're about fostering transparency, minimizing avoidable risk, and keeping your organization aligned with evolving regulatory standards and insurer expectations. This approach enables your executive team to make timely, well-informed decisions.

As always, we are here as your cybersecurity partner to provide guidance, answer questions, and help you approach cybersecurity in a way that is consistent, transparent, and supports the broader health of your business.

CYBERSECURITY LETTER TILE PUZZLE

- Unscramble the tiles to reveal a message.
- Each tile is used only once.
- Use spacing, punctuation and common words to find adjacent tiles.
- Some words may be split into two lines.

s A w	e s s	o f D	a r e n	F i r	c e I	i n e	s t L
e f e n	Y o u r						