towerwall

Table of **Contents**

From the **Towerwall** Team

The uncomfortable truth about this year's biggest breaches is that most of the organizations affected did nothing wrong. **Their vendor did.**

Third-party compromise has become one of the defining security stories of 2026. When a single shared platform is breached, the damage does not stay contained to the vendor. It cascades outward to every organization that trusted that vendor with data, access, or day-to-day operations.

This month, we look at what the recent wave of third-party compromises reveals, how attackers are exploiting the trusted connections between organizations and the platforms they rely on, and what a practical third-party risk program actually looks like. We also cover the CMMC Phase 2 deadline now on the horizon, and a **new podcast conversation** with our CEO, Michelle Drolet.

Resilience is built before the disruption, not during it. The same is true for the risk your vendors carry on your behalf.

News & Community

Third-Party Compromise Is Now **the Main Event**

A pattern has taken hold across this year's most significant incidents. Attackers are no longer working to breach thousands of organizations one at a time. They are breaching the single platform those organizations all depend on, and letting the damage cascade.

The Canvas compromise is the clearest recent example.
Earlier this year, the extortion group behind the attack reached the Instructure Canvas platform through a weakness in a free-tier account system, then used that foothold to reach data belonging to institutions worldwide. Reporting placed the exposure across roughly ***8,800 institutions and millions of individuals***, making it one of the largest incidents of its kind on record. The organizations affected did not have a flaw in their own environments. Their learning platform did.

That is the defining feature of third-party risk in 2026. Modern organizations have consolidated critical operations inside shared SaaS platforms and vendor relationships, and that concentration creates enormous risk in single points of failure. When one of those platforms goes down or gets breached, the scale of the disruption is a direct reflection of how deeply everyone depended on it.

The takeaway for security leaders is not to abandon the platforms that run the business. It is to **understand where those dependencies live, what data and access each one holds, and how large the blast radius would be** if any single one of them were compromised tomorrow.

Get The Whitepaper Now

Threat & Vulnerability Spotlight

Device Code Phishing Is Surging

If third-party compromise is the outcome, identity is increasingly the entry point. And one technique is accelerating fast enough to deserve its own attention this month: **device code phishing.**

Device code phishing abuses a legitimate authentication flow to capture access and refresh tokens without ever stealing a password. The mechanic is deceptively simple. Whoever initiates the authentication request receives the resulting tokens, and once an attacker holds those tokens, they can reach connected services, maintain persistent access, and quietly conduct reconnaissance and data extraction from inside what looks like a trusted session.

What makes this a business problem rather than a purely technical one is how accessible it has become. The capability is now built into commodity phishing kits sold as a service, which means even unskilled actors can launch these attacks at scale. Researchers tracking the trend note that kits surviving their first year tend to become ***significantly more dangerous*** in their second, adding automation and evasion as they mature.

Because these attacks ride on legitimate authentication and leave no stolen password to reset, they often slip past the defenses organizations assume are protecting them. Multi-factor authentication helps, but it is no longer sufficient on its own. Reviewing how authentication tokens are issued and monitored, tightening the access each account actually needs, and watching for unusual session behavior **all matter more than ever.**

Contact Towerwall to review how your organization issues, monitors, and secures authentication tokens before an attacker does.

Read the full report
on device code phishing from KnowBe4.

Valuable Information

Building a Third-Party Risk Program **That Actually Works**

Knowing third-party risk is real is the easy part. Building a program that meaningfully reduces it is where most organizations stall. A few principles consistently separate the organizations that weather a vendor compromise from the ones caught flat-footed.

Start by mapping where your critical data actually lives and who has access to it. One of the most common gaps we see is organizations that cannot say with confidence which vendors hold their sensitive data, or what those vendors would expose if they were breached. You cannot protect, or make good decisions about, what you have not mapped. Trying to protect everything equally usually means protecting nothing well.

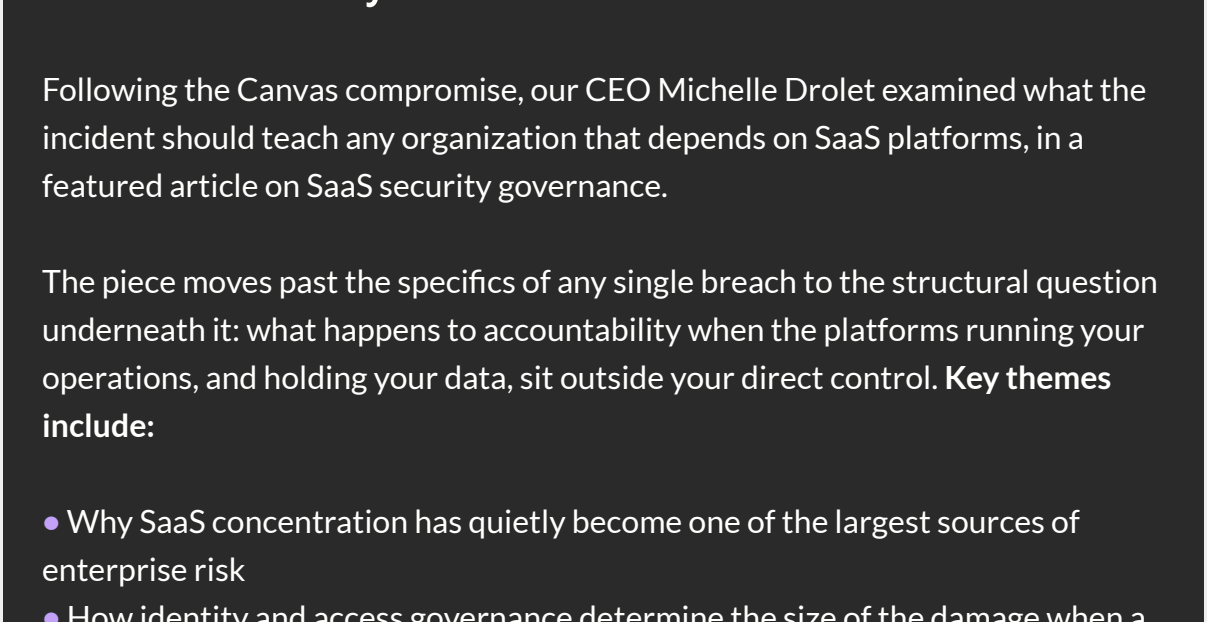
Treat vendor risk as an ongoing discipline, not a one-time questionnaire. The security questionnaires flowing between organizations and their prospects have become a real gate on business, and being able to answer them credibly increasingly determines whether deals close. That works in both directions. The same rigor you expect from your own answers is the rigor you should apply when evaluating the vendors you rely on.

Reduce the blast radius before you need to. Enforce multi-factor authentication everywhere, right-size the access each account and integration holds, rotate the keys and tokens tied to third-party connections, and keep visibility across the systems those vendors touch. The goal is not perfect prevention, which no one can promise. The goal is making sure that when something does go wrong, upstream or down, the damage is contained rather than catastrophic.

As we often put it, you are stewards of your data, not the only party who touches it. **Third-party risk management is how you stay accountable for information that lives, at least partly, in someone else's hands.**

For ongoing cybersecurity insights and commentary

Follow Michelle Drolet on LinkedIn



Leadership Perspective

What the Canvas Breach Teaches About SaaS Security Governance

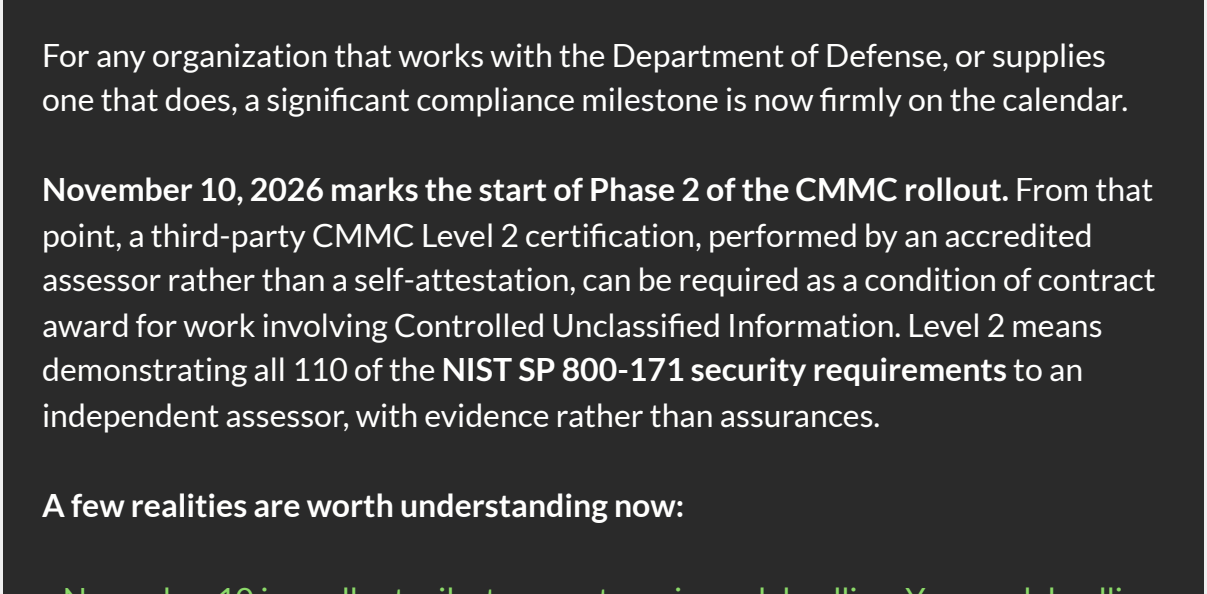
Following the Canvas compromise, our CEO Michelle Drolet examined what the incident should teach any organization that depends on SaaS platforms, in a featured article on SaaS security governance.

The piece moves past the specifics of any single breach to the structural question underneath it: what happens to accountability when the platforms running your operations, and holding your data, sit outside your direct control. **Key themes include:**

- Why SaaS concentration has quietly become one of the largest sources of enterprise risk
- How identity and access governance determine the size of the damage when a platform is breached
- What questions organizations should be asking vendors before they sign, not after an incident
- Why resilience and containment matter more than the belief that any platform is unbreachable

It is a clear, practical read for any leader weighing how much of their operation now runs on third-party platforms.

Read Michelle's full article
on the Canvas breach and SaaS security governance



Compliance & Regulation Update

CMMC Phase 2 Is on the Clock: What November 10 Means

For any organization that works with the Department of Defense, or supplies one that does, a significant compliance milestone is now firmly on the calendar.

November 10, 2026 marks the start of Phase 2 of the CMMC rollout. From that point, a third-party CMMC Level 2 certification, performed by an accredited assessor rather than a self-attestation, can be required as a condition of contract award for work involving Controlled Unclassified Information. Level 2 means demonstrating all 110 of the **NIST SP 800-171 security requirements** to an independent assessor, with evidence rather than assurances.

A few realities are worth understanding now:

- November 10 is a rollout milestone, not a universal deadline. Your real deadline is tied to when your specific contracts are solicited and awarded, which for many contractors is already here.
- The requirement flows down the supply chain. If a prime contractor passes Controlled Unclassified Information to your organization, the certification obligation travels with it, whether or not anyone has told you directly.
- Assessor capacity is limited. Readiness commonly takes many months of preparation, and third-party assessment scheduling is already stretched, so waiting until the requirement appears in a contract you want is waiting too long.

This is third-party risk written into federal regulation. It exists precisely because the government recognized that a chain is only as secure as its least prepared supplier. Used well, the requirement becomes a measurable way to prove your security posture, not just another box to check.

To understand where you stand against CMMC and what the most sensible next step looks like for your organization,

Contact Us

Podcast Spotlight

Michelle on the Secure & Simple Podcast: How CISOs Should Talk to Corporate Boards

Our Founder and CEO, **Michelle Drolet**, recently joined host Dejan Kosutic on the Secure & Simple podcast for a conversation on one of the hardest parts of the modern security leader's job: talking to the board.

Drawing on more than 25 years on the front line of cybersecurity, Michelle breaks down how to reframe security metrics around business impact rather than vulnerabilities, why cybersecurity belongs in the conversation as a business enabler and not a cost center, and how CISOs can earn a real, recurring seat at the boardroom table. She also tackles the question every board eventually asks, *"Are we secure?"*, and how to answer it with confidence and without leaning on fear.

It is a practical listen for security leaders, and for the executives and board members who work alongside them.

How CISOs Should Talk to Corporate Boards
Interview with Michelle Drolet | EP38

Watch the full episode

Someone Else's Risk **Is Still Your Responsibility**

The through-line this month is a simple one.
In an environment where your data, your operations, and your obligations increasingly live inside platforms and partners you do not directly control, security can no longer stop at your own perimeter.

The organizations that will weather what is ahead are the ones treating third-party risk the way they treat their own: mapped, governed, tested, and planned for well before an incident forces the conversation.

Assume compromise. Reduce the blast radius. Build resilience before you need it. ***Thank you for being part of the Towerwall community.***

— The Towerwall Team.

Book a consultation with Towerwall

Explore our Resource Center

About **Towerwall**

Towerwall is a **trusted, woman-owned information security partner** serving organizations across industries including healthcare, retail, education, technology, and financial services. For over 30 years, our mission has been to help organizations operationalize security, achieve compliance, and protect what matters most.

towerwall

Towerwall, 10 Speen Street, 4th Floor Suite 4-01, Framingham, MA 01701, United States, 774-204-0700