CISO Guide: Third-Party Breaches — When Someone Else's Risk Becomes Yours

IThe supply chain you rely on could be the breach path you never see coming. Here's how to close the gaps.

In today's SaaS-first, cloud-integrated business environment, your organization is no longer an island. You depend on dozens—sometimes hundreds—of vendors, suppliers, and contractors. They handle sensitive data, integrate directly with your core systems, and often hold the same—or greater—access to critical functions as your own employees. And that's where the risk lies.

According to *IBM's Cost of a Data Breach Report 2025*:

- 14% of all breaches stem from third-party or supply chain compromises.
- They cost an average of $4.91M per incident.
- They take the longest to detect and contain—267 days on average—giving attackers almost nine months of free reign.

Recent high-profile breaches—like the Qantas data exposure of 5.7 million customers and the Snowflake/AT&T customer data compromise—prove that even when your internal defenses are world-class, you can still be pulled into a costly, public, and operationally disruptive incident because of someone else's mistakes.

This guide will help you understand the unique dynamics of third-party breaches, illustrate their impact through real-world examples, and provide practical steps to reduce exposure—without slowing down your business.

1. The Scope of the Problem

Modern enterprises are hyperconnected. You outsource payroll, customer support, marketing analytics, data storage, and dozens of other functions to third parties. In theory, this expands capability and efficiency. In practice, it expands your attack surface far beyond your own perimeter.

Here's why the problem is so persistent:

- **Vendors touch sensitive data:** SaaS CRMs, cloud storage, and analytics platforms often hold full customer datasets.
- **Partners integrate deeply:** API-based connections give external systems privileged access.
- **Visibility gaps:** Many CISOs lack a full inventory of all vendors and their level of access.
- **Regulatory overlap:** Even if a vendor is at fault, your organization may still be liable under GDPR, CCPA, HIPAA, or other frameworks.

And unlike phishing or malware—where you can directly control your defenses—third-party breaches are indirect. You can't patch another company's systems. You can't train their employees. But you're still accountable for the fallout.

2. Real World Examples

Qantas Airways

In 2024, a third-party provider breach exposed the personal information of 5.7 million customers. The airline's core systems were uncompromised, but brand trust took a direct hit. They faced a global PR crisis, regulatory questions, and a customer support surge—all triggered by a supplier's security lapse. Read more

AT&T & Snowflake

In 2024, attackers breached Snowflake environments used by AT&T, leading to the exposure of sensitive customer data. The breach highlighted the dangers of over-reliance on vendor security assurances without continuous verification. Read more

Target Breach (2013)

Hackers compromised a third-party HVAC vendor, using their credentials to access Target's internal network. The result? Data from 40 million credit and debit cards was stolen, costing Target hundreds of millions in settlements and brand recovery. Read more

MOVEit Breach (2023)

Exploitation of a zero-day vulnerability in the MOVEit file transfer platform impacted over 2,500 organizations globally, including Amazon, Metlife, HSBC, and many more. Many victims weren't even aware they used MOVEit—because it was embedded in a vendor's workflow. Read more

3. The Data Behind the Risk

IBM's Cost of a Data Breach Report 2025 shows:

- **$4.91M** – Average cost of a third-party/supply chain breach.
- **14%** – Share of breaches originating from third-party compromises.
- **267 days** – Longest average detection and containment time.

Compare this to phishing attacks, which average **$4.80M** in cost but are detected faster, or insider errors, which cost **$3.62M** on average. Supply chain breaches aren't the most frequent, but they're among the **most expensive and hardest to stop.**

Why detection is so slow:

- You rely on the vendor to identify and disclose the breach.
- Compromises may happen deep in automated integrations without obvious anomalies.
- Data often flows between multiple intermediaries before reaching you, making forensic tracking harder.

4. Why These Breaches Are So Hard to Stop

1. **You Can't See Inside Vendor Security** – Even with audits, much of a vendor's security posture is opaque.
2. **Inherited Weaknesses** – Their vulnerabilities become your vulnerabilities the moment systems connect.
3. **Delayed Notification** – Vendors may wait days, weeks, or even months to alert you—if they alert you at all.
4. **Trust Abuse** – Legitimate connections and credentials make it harder to detect malicious use.
5. **Complex Chains** – Your vendor's vendor can also be a breach vector, multiplying the risk.

5. Scenarios to Consider

Third-party breaches don't knock politely — they arrive through the side door, sometimes months after you thought it was locked.
Here are five real-world inspired scenarios every CISO should have on their radar:

1. Secure but Exposed

Your internal security posture is rock-solid. MFA everywhere. Privileged accounts locked down. Then your SaaS billing provider suffers a breach — and 100% of your customer payment records are exposed.

📌 *Think of the recent Qantas breach, where personal information of 5.7 million customers was compromised — not because passengers gave it away, but because the systems holding it were infiltrated.*

Impact: Loss of customer trust, mandatory disclosure, and an immediate hit to revenue even though your internal environment wasn't touched.

2. Dormant Access Abuse

You hire a **marketing agency** to manage your CRM for a 3-month campaign. They do good work. Contract ends. Everyone moves on. Except their **admin credentials** remain active in your environment six months later. Those credentials are stolen in another breach, sold on the dark web, and used to quietly siphon customer data for weeks before detection.

📌 *A common pattern seen in post-breach forensics: long-forgotten accounts from "trusted partners" becoming the initial entry point.*

Impact: Data theft, regulatory scrutiny, and embarrassing questions from the board about basic offboarding hygiene.

3. Supply Chain Domino Effect

Your Tier 1 supplier has strong controls. But they rely on a smaller **subcontractor** that doesn't. Attackers compromise the subcontractor, pivot into the Tier 1 supplier, and eventually find a direct route into your shared systems.

📌 *This mirrors the **Snowflake–AT&T incident**, where compromise of a supplier's environment created ripples into major enterprises.*

Impact: A breach far removed from your own systems becomes your headline, costing millions in investigation, remediation, and lost business.

4. Shadow Vendor Connections

A department head signs up for a **"free trial" SaaS tool** to speed up their workflows — no IT involvement, no vetting. Months later, that service suffers a breach. The attacker uses its **OAuth connection** to your sanctioned systems as a backdoor.

📌 *Shadow IT isn't just an internal visibility problem; it's an open door to third-party compromise.*

Impact: Attackers bypass your perimeter entirely by exploiting a connection no one in security even knew existed.

5. Regulatory Crossfire

A niche analytics vendor you use is breached. They store EU citizen data for you, and under GDPR, **you** are the data controller. Even though the breach originated entirely outside your systems, you face the **same fines and regulatory investigations** as if you'd been breached directly.

📌 *The IBM Cost of a Data Breach Report 2025 shows that supply chain breaches cost an average of **$4.91M**, and made up **14% of all breaches** studied.*

Impact: Fines, legal battles, and PR damage — all for a breach that wasn't "yours" in the technical sense.

6. Reducing the Risk - CISO Checklist

☐ **Maintain a complete vendor inventory**. Track every supplier, contractor, integration, API connection, and data-sharing agreement. Shadow vendors are the ones that hurt most — you can't secure what you don't know exists.

☐ **Classify vendors by risk level.** Identify which partners handle **sensitive data, privileged credentials, or network-level access**. Focus monitoring resources here first.

☐ **Demand and verify security certifications.** SOC 2, ISO 27001, or equivalent should be table stakes. Follow up with your own security questionnaire — certifications expire, risk doesn't.

☐ **Embed contractual breach notification clauses.** Require vendors to disclose breaches within 24 hours, with enough technical detail for you to act.

☐ **Continuously monitor external user activity.** Track vendor accounts *inside* your environment in real time. Spot unusual behavior — different geos, odd time zones, unexpected access patterns — before it becomes a breach. *(Context-based monitoring is far stronger than static checks.)*

☐ **Monitor for stolen credentials on the dark web.** Detect when a vendor's credentials linked to your systems show up in criminal marketplaces — it's often the first sign they've been compromised.

☐ **Revoke unused access immediately.** Contractors, agencies, and seasonal vendors should lose access the moment the engagement ends. No exceptions.

☐ **Map all SaaS connections.** Build and maintain an up-to-date map of every OAuth or API connection to your environment. This makes it clear where third-party risk enters your perimeter.

☐ **Limit vendor data exposure.** Share only the minimum necessary data with each vendor, and review regularly whether they still need it.

☐ **Test incident response plans with vendors.** Run joint breach simulations annually to ensure both sides know their role and timelines.

7. Where FrontierZero Helps

FrontierZero eliminates the blind spots that make third-party breaches so dangerous by giving you:

- **Full SaaS inventory visibility** — Know every connected vendor, approved or not.
- **Behavioral monitoring** — Spot abnormal activity in third-party access before it escalates.
- **MFA & context enforcement** — Lock down external integrations with stronger identity controls.
- **Rapid response mapping** — Identify exactly which vendor connections to sever in a breach scenario.

You can't secure what you can't see—and you can't respond to what you don't know exists. FrontierZero gives you both the visibility and control to keep third-party risk from becoming your next headline.

About FrontierZero

FrontierZero is the only SaaS Security Posture Management (SSPM) platform built in the UAE, created to solve a problem every modern organization faces: SaaS sprawl without visibility or control.

Founded to help compliance-driven sectors protect their most valuable assets, FrontierZero was awarded Rising Star in Cyber Defence 2025 for its innovation in securing SaaS environments in real time. Our mission is simple: give organizations the visibility and control they need to stop threats before they escalate.

With FrontierZero, you can:

- See everything — Full SaaS inventory visibility, including shadow and unapproved apps.
- Spot risks early — Detect abnormal activity, risky permissions, and MFA bypasses before they become breaches.
- Enforce security — Lock down external integrations with stronger identity and context-based controls.
- Respond instantly — Map exactly which vendor connections to cut in a breach scenario.
- Stay compliant — Continuously meet audit requirements without adding complexity or overhead.

From hidden AI tools to forgotten accounts, we reveal the blind spots others miss—helping you stay compliant, resilient, and ready for what's next.

✅ **Want to see what your real SaaS perimeter looks like?**

Start Your Free Trial Today