

Third-Party Risk Management

Your suppliers, software and cloud services are now part of your attack surface. Here is what third-party risk management is and the controls that keep a supplier's breach from becoming yours.

WHAT IT IS

Third-party risk management is how you find, assess and control the security and operational risks created by the outside parties you depend on, from software vendors and cloud services to contractors and their subcontractors. The goal is simple. Stop a partner's breach or failure from turning into your own incident, exposure or downtime.

WHY IT MATTERS

48%

Of breaches in 2025 data involved a third party, up from 30% a year earlier.

Verizon 2026 DBIR

4.91 million dollars

Average cost of a breach involving a third party or supply chain.

IBM, 2025

267 days

To identify and contain a third-party breach, the longest of any type.

IBM, 2025

WHAT HAPPENED

In August 2025 ransomware hit Miljödata, a Swedish supplier whose HR and sick-leave systems serve around 80% of the country's municipalities. Services across roughly 200 of Sweden's 290 municipalities and regions went down and sensitive data may have been exposed, yet no municipality was breached directly. Years earlier, attackers reached Target through an air-conditioning contractor's login. Each time the way in was a supplier. (The Record, 2025)

RED FLAGS TO WATCH FOR

You cannot judge a supplier's security by its size or reputation, so watch the access and the answers, not the brand name.

- A supplier that wants broad or standing access when the job needs very little.
- No security certification, no recent audit and vague answers on how they protect data.
- No clear breach-notification commitment or named security contact in the contract.
- A critical service concentrated in one supplier, or one supplier's supplier, with no fallback.

THE ONE RULE THAT STOPS IT

Give every third party the least access it needs and no more, and know exactly what each one can reach. Most supplier breaches spread only because that access was wider than the job required.

THEN BUILD THE HABIT AROUND IT

- Keep a live list of every supplier and what each one can access.

- Tier suppliers by risk and check the high-risk ones hardest before you sign.
- Put security standards, breach-notification timelines and exit terms in every contract.
- Reassess suppliers on a schedule and again after any major change or incident.

MYTHS AND FACTS

MYTH

If a supplier is breached, that is their problem.

FACT

The data and the service are still yours, so the fallout and the regulators are too.

MYTH

A signed contract and a questionnaire mean the vendor is secure.

FACT

Both are snapshots. SolarWinds and MOVEit were trusted, vetted vendors when attackers got in. Only monitoring tells you if a supplier is still safe.

MYTH

We only need to check our direct suppliers.

FACT

Your suppliers depend on their own suppliers, and those weaknesses become yours. Look past the first link.

THE LEGAL DUTY

Third-party risk management is now a legal duty. In Sweden NIS2 applies as Cybersäkerhetslagen from 15 January 2026, requiring supply-chain security and making boards personally accountable under Article 20. DORA and GDPR Article 28 add further duties.

GET HELP

eBuilder Security runs Sweden-based security awareness training that helps the people who onboard vendors, approve access and handle supplier requests treat third-party risk as part of their everyday work. Read the full guide at the link below.

[Read the Full Article →](#)