From Trust to Assurance

Practical Supply Chain Security for Leaders

Senior leaders don't need convincing that cyber risk is real. What's changed is how often it comes via third parties.

More and more organisations are being impacted by incidents that start outside their perimeter, via a supplier, a managed service provider, a cloud platform, or software they rely on. Verizon's 2025 Data Breach Investigations Report (DBIR) found "*third-party involvement in 30% of all breaches, up from roughly 15% last year.*"

The UK's National Cyber Security Centre has been explicit too, issuing updated guidance following a "*recent rise in supply chain cyber attacks*", aimed at helping organisations strengthen the way they manage supplier cyber risk.

At Tickbox, we see why this resonates: modern delivery models create more dependencies, more connections, and more shared responsibility, and attackers are increasingly happy to exploit that.

What supply chain cyber risk actually means

Supply chain cyber risk is simply this: If a supplier is compromised (or fails), can it disrupt us or expose our data? It tends to show up in a few very recognisable ways:

1.Supplier access becomes the doorway: A partner has remote access, admin tooling, privileged accounts, or API keys. If they're compromised, that trust can be used against you.

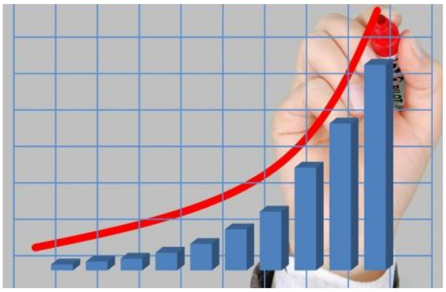
2.Supplier software becomes the delivery mechanism: Vulnerabilities, malicious updates, or insecure configurations in tools you consume.

3.Service disruption becomes your disruption: If a critical provider is hit, you can lose operational capability even if your own controls are strong.

4.Sub-suppliers sit out of sight: Your supplier relies on other suppliers, and you may not know who they are or what "good" looks like for them.

Why the problem is widening - and why it's not "someone's fault"

This risk is growing because organisations are doing rational things:



- adopting cloud services for speed and resilience
- outsourcing specialist functions to experts
- buying software instead of building everything
- integrating systems so services feel seamless to customers and staff

Those choices are sensible. The side effect is a bigger "trust network", and supply chain attacks are, at its core, attacks on trust.

What "good" looks like: practical, proportionate, evidence-based

Most organisations don't need a brand-new mega-programme. They need repeatable control over the suppliers that matter most.

The NCSC's supply chain security guidance is a strong foundation for "what good looks like" because it's written for real organisations, not theoretical ones, and it breaks the problem into practical principles and steps.

A leader-friendly approach that works.

1) Start with visibility and prioritisation (the risk-ranked supplier list)

Good looks like:

- A single list of suppliers (and key technologies), ranked by criticality:
    - *Could they impact our service delivery?*
    - *Do they handle sensitive data?*
    - *Do they have privileged access or connectivity?*
    - *Would recovery be hard if they went down?*

This is the step that unlocks proportionality. Without it, teams either:

- over-assess low-risk suppliers, or
- under-control the ones that could significantly impact you.

NCSC's supply chain security guidance explicitly emphasises knowing who your suppliers are and establishing effective oversight.

2) Set clear minimum expectations (the baseline suppliers must meet)

Good looks like:

- A short set of baseline controls you expect any relevant supplier to have, such as:
    - ▶ vulnerability management and patching
    - ▶ secure remote access
    - ▶ incident notification timeframes
    - ▶ data handling and retention expectations
    - ▶ clear subcontractor/sub-processor rules

The goal is to remove ambiguity and reduce avoidable risk.

NIST's Cybersecurity Supply Chain Risk Management guidance (SP 800-161 Rev.1) is a credible reference point for building a structured, repeatable approach.

3) Do due diligence that matches the risk (light touch vs deep check)

A tiered process that scales with impact and access:

- Low risk:
  Basic questionnaire + standard contract terms (e.g., confidentiality, data handling, incident notification where relevant).
- Medium risk:
  Evidence based check (key policies, relevant certifications, security controls summary) + follow-up on any gaps.
- High risk / critical:
  Deeper, practical assurance and operational readiness, recognising that not all supplier types can be audited in the same way:

  - Major cloud/SaaS providers:
    Obtain independent assurance (e.g., SOC 2 Type II and/or ISO audit reports/certificates via the supplier's trust portal), confirm the supplier's standard incident notification and sub processor transparency approach, and maintain your own remediation/exception log for any gaps or risks you decide to accept.
  - Managed Service Providers (MSPs)/outsourcers/integrators (with access to your environment):
    Deeper assessment is often feasible, including right to audit where appropriate, evidence that controls operate in practice (access management, monitoring, patching), clear incident readiness expectations, and tracked remediation.

This keeps effort where it pays off:
You go deepest where a supplier could materially impact operations, data, or security, and you use proportionate, realistic assurance methods by supplier category, aligned to national guidance on assessing and gaining confidence in your supply chain.

Example:
A critical managed service provider should be able to evidence access controls and incident processes. A low-risk supplier may only need basic assurance.

4) Reduce the blast radius (assume suppliers will have incidents)

This is the maturity leap: moving from “we trust them” to “we’ve designed for resilience”.

Good looks like:

- Least-privilege supplier access (only what’s needed)
- Separate supplier accounts (no shared accounts)
- Time-bound access for privileged tasks
- Monitoring for supplier account activity on critical systems
- A practical “what if the supplier is compromised?” response plan

This is where the Verizon DBIR stat becomes useful in leadership conversations: if third parties are involved in 30% of breaches analysed, designing for supplier incidents becomes a rational risk decision, not a fear-based one.

5) Make it governable (so it doesn’t rely on heroics)

Good looks like:

- Ownership: who’s accountable for supplier risk decisions?
- Reporting: a simple dashboard (critical suppliers, assurance status, open risks, exceptions)
- Evidence: decisions and follow-ups documented

A practical improvement plan (maturity path) for third-party and supply chain risk

Level 1: Getting the basics right

- Build a supplier inventory and apply risk tiers (based on access, data sensitivity, and operational dependency).
- Define baseline security expectations for suppliers (clear, proportionate “minimums”).
- Put basic contract clauses in place (e.g., security requirements, incident notification, data handling).

Level 2: Consistent and measurable

- Run standardised assessments by tier (lighter for low risk, deeper for higher risk).
- Maintain tracked remediation and exceptions (what you’ve asked suppliers to address, what you’ve accepted, and why).
- Strengthen supplier access controls (least privilege, MFA, separation of accounts, and removal processes where relevant).

Level 3: Resilient and optimised

- **Ongoing monitoring for critical suppliers**: periodic reassessment and review of supplier security performance and key signals (e.g., assurance refresh, changes that affect risk, and performance against agreed requirements).
- **Incident readiness exercises for key providers**: joint tabletop exercises where suppliers have meaningful operational involvement (e.g., MSPs/integrators), and internal scenario exercises for major SaaS/cloud providers using the supplier’s standard incident/notification approach.
- **Improved software transparency (where relevant)**: use Software Bill Of Materials (SBOM) and related guidance to improve visibility of software components/dependencies for higher-risk software, supporting faster response when vulnerabilities emerge.

For software supply chain transparency, CISA’s SBOM guidance (“Framing Software Component Transparency”) is a strong reference point.