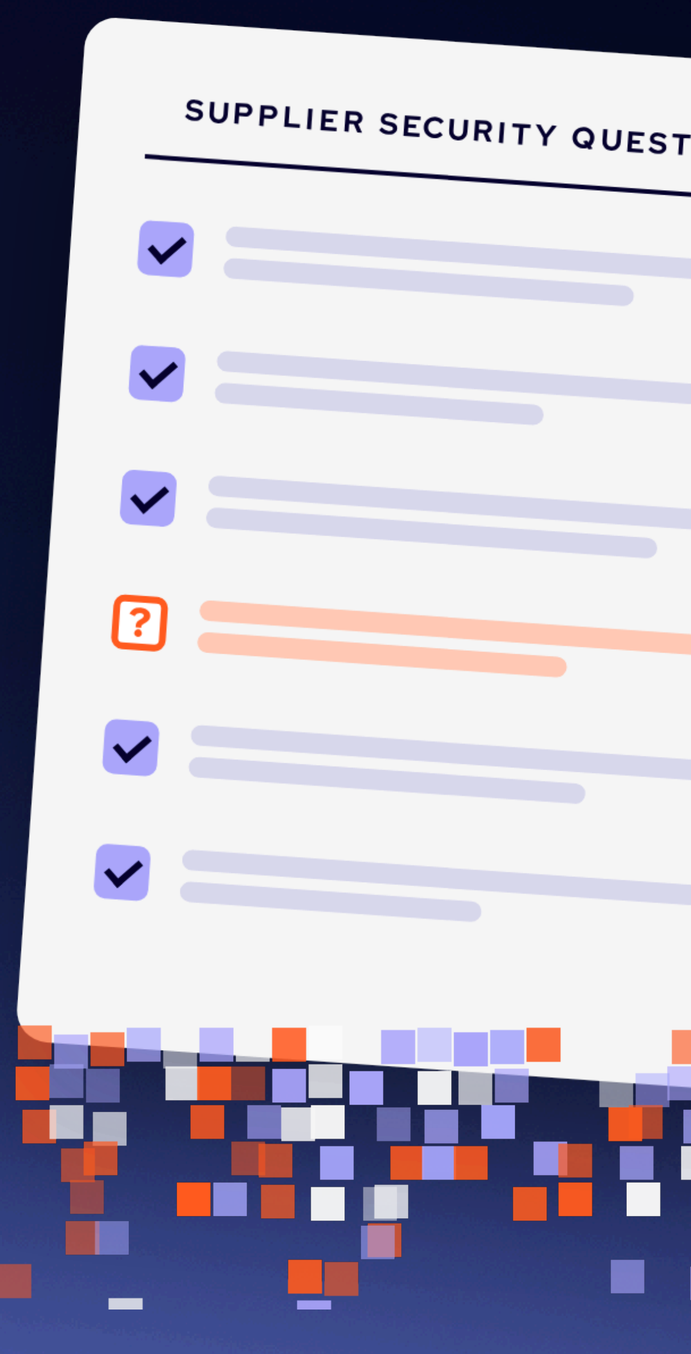
CLOUDGUARD
Security Done Different

BOARD BRIEFING | SUPPLY CHAIN CYBER RISK | CLOUDGUARD

Trust is not a supply chain control.

Four pages for boards, non-executives and risk committees in retail, logistics and manufacturing. What has changed, the ten questions to ask, and what good looks like in 90 days.



> A supplier's certificate tells you how they were assessed last year. It doesn't tell you whether their business had an issue this morning, whether the API they just shipped checks who is calling it, or whether the carrier collecting your pallets is who it says it is.

THE BOARD-LEVEL MESSAGE

01

What has changed

Why breaches now start one or two hops away from you.

02

Ten questions

For your next board or risk committee. Score yourself honestly.

03

The 90-day plan

From assurance to evidence: see it, control it, prove it.

Drawn from the CloudGuard white paper *Why Trust Is Not a Supply Chain Control* (November 2026).
Full paper at cloudguard.ai/resources/supply-chain-white-paper

Unrestricted

Breaches now start one or two hops away.

Until recently, supplier due diligence meant a questionnaire, a certificate and a contract clause. The 2026 evidence says that is no longer enough. Attackers go after the weakest trusted link: a supplier's help desk, a carrier's email account, a plug-in in your checkout, an AI agent with access to payments.

48%

of breaches in Verizon's 2026 DBIR involved a third party, up from 30% a year earlier[1]

15%

of UK organisations review the cyber risk of their immediate suppliers. Just 6% look at the wider chain[3]

£1.9bn

estimated cost of the JLR attack, which reached up to 5,000 organisations in its supply chain[5]

29%

of organisations say they are prepared to secure the agentic AI they are deploying[13]

Four shifts every board should understand

01 SPEED

Annual assurance answers last year's threat

Attackers exploited flaws on average seven days before public disclosure, and access passed from initial attacker to ransomware operator in a median of 22 seconds, down from eight hours in 2022.[2]

02 CODE

AI-built integrations ship unchecked

87% of organisations had an API security incident last year, and only 23% hold a complete inventory of the APIs that expose sensitive data. The most common critical flaw in AI-built apps is authorisation: who is allowed to see what.9,10

03 AGENTS

Software now acts with your credentials

Agents read supplier emails, book carriers and issue refunds. Nearly half of organisations cannot monitor what their agents are doing or tell a legitimate agent from a malicious bot.[11]

04 IMPERSONATION

Attackers pretend to be someone you trust

The M&S attack began with a call to a third-party service desk asking for a password reset. Deceptive cargo pickups using fake identities rose 31% year on year in the US.4,15

The UK lesson, in four incidents

APR 2025

M&S

Help desk social engineering at a service provider. Estimated cost c.£136m.4,6

Your supplier's help desk can reset your credentials.

2025

Co-op

Similar technique. Data on 6.5m members stolen.4,6

Rehearsed response shortens recovery.

AUG 2025

Jaguar Land Rover

Category 3 systemic event. Six-week production halt.[5]

One outage becomes every supplier's cash-flow crisis.

2025

Peter Green Chilled

Ransomware halted chilled deliveries to UK supermarkets.[6]

One logistics provider can empty the shelves.

Unrestricted

CLOUDGUARD
Security Done Different

Ten questions. Evidence, not assurance.

Answer each one as you could today, on a bad day. If you can only answer with a policy, a questionnaire or a certificate, tick "not yet".

	QUESTION	EVIDENCED	PARTLY	NOT YET
1	**Which five suppliers or platforms could stop us trading, and what do we know about their security today?** DEPENDENCIES	☐	☐	☐
2	**How would we learn that one of them had been breached, and how fast?** DEPENDENCIES	☐	☐	☐
3	**Do we hold an inventory of our APIs, including undocumented ones?** CODE AND APIS	☐	☐	☐
4	**Who reviews AI-generated code before it reaches production?** CODE AND APIS	☐	☐	☐
5	**Where are our secrets, and how quickly can we revoke them all?** CODE AND APIS	☐	☐	☐
6	**Which AI agents can act on our behalf, and what can they touch?** AI AGENTS	☐	☐	☐
7	**Can one phone call change who we pay or who collects our goods?** IMPERSONATION	☐	☐	☐
8	**How does our outsourced help desk verify a password reset?** IMPERSONATION	☐	☐	☐
9	**When did we last rehearse a supplier compromise with suppliers in the room?** RESILIENCE	☐	☐	☐
10	**What evidence, not assurance, would we show an insurer or regulator tomorrow?** RESILIENCE	☐	☐	☐

Three or more "not yet"? That is your Security Confidence Gap.

It is the distance between the assurance you hold and the evidence you could produce on a bad day. Contracts were signed, questionnaires returned, certificates filed. But best-practice supplier questionnaires reportedly get around a 30% response rate.[2] A control most suppliers ignore is not a control.

How to use this page

Take it to your next board or risk committee. Ask the executive who owns each question to bring evidence, not a status update. Revisit every six months, because the threat will have moved.

Unrestricted

From assurance to evidence in 90 days.

Know what you depend on. Give every identity, human or machine, the least access it needs. Verify before you trust, and keep verifying. Rehearse the response before you need it.

DAYS 1 TO 30

See it

- Rank critical suppliers, carriers, platforms and integrations by business impact
- Inventory APIs, pipelines, AI agents and tools in use, sanctioned or not
- Review help desk and payment-change procedures

BOARD SEES

A ranked dependency map and an API and agent inventory

DAYS 31 TO 60

Control it

- Human approval for bank, address and refund changes, including those made by agents
- Phishing-resistant sign-in for privileged and supplier-facing accounts
- Authorisation review built into every API release

BOARD SEES

Policy enforced in tooling, not documents, and a signed-off agent permissions register

DAYS 61 TO 90

Prove it

- Tabletop a compromised supplier, with suppliers in the room
- Test a help desk impersonation and a fake carrier pickup end to end
- Ask suppliers for continuous signals, not annual questionnaires

BOARD SEES

Exercise findings and a board-ready view of residual supply chain risk

Four rules before any AI agent touches money, stock or customer data

1

Its own identity, least privilege

No shared service accounts, no standing admin, credentials that expire.

2

A human on irreversible actions

Bank details, delivery destinations, refunds and carrier onboarding need out-of-band approval.

3

Everything it reads is untrusted

Separate instructions from data, restrict tools by task, log every tool call.

4

Govern the agent supply chain

Approve connectors and skills like software, pin versions, re-review on change.

NEXT STEP

Book a supply chain security conversation.

We'll walk through the ten questions with you, show where your assurance and your evidence diverge, and agree your first 30 days.

Secure Your Supply Chain

Use the Speak to an Expert form on the page.

NCSC Assured Service Provider (CIR)
CREST-accredited SOC | ISO 27001
24/7 SOCs in Manchester and Belfast

Sources. [1] Verizon 2026 DBIR, as summarised by Security Scientist. [2] Black Kite, 2026 Supply Chain Vulnerability Report, citing Mandiant M-Trends 2026. [3] UK Cyber Security Breaches Survey 2026 (DSIT). [4] Computer Weekly, "One year on from the M&S cyber attack". [5] Cyber Monitoring Centre assessment, via Prolific North. [6] ServNet UK, NAO warning on food supply chain risk (Sept 2026). [9] Cloud Security Alliance Labs, Vibe Coding Security Debt (Apr 2026). [10] Akamai 2026 API Security survey, via Zuplo. [11] Salt Security, 1H 2026 State of AI and API Security. [13] Cisco State of AI Security 2026, via Help Net Security. [15] Overhaul Q1 2026 US Cargo Theft Report, via Carrier Management. Several sources are vendor research; full references and evidence notes are in the white paper.

Unrestricted