ncc group

Insuring in Turbulence: Supply Chains, Cyber Threats, and Risk Redefined

Supply Chain Complexity

Incident Response Insights

Legal and Regulatory

Risk Model Evolution

Q&A

Polling question 1:

Have you changed any of principles of your modelling over the last year, in response to advancing cyber threats?

1. Yes – Significant changes to the core principles
2. Yes – Minor adjustments have been made
3. No – Principles remain largely the same
4. Not applicable or Unsure

Polling question 2:
What measures have you taken to manage supply chain exposure?

1. Conduct vendor risk assessments
2. Adopted continuous monitoring ensuring all supply chain products are continually monitored
3. Implemented contractual controls, i.e. breach notification names
4. Incident Response integration, ensuring clear escalation paths
5. Conducted supply chain mapping to ensure understanding of critical suppliers

Polling question 3:

How many carriers / brokers are now asking specific risk-based questions in relation to third party security due diligence?

1. None - this is not something I/We have seen
2. Less than 25%
3. 25 to 50%
4. More than 50%

Overconfidence puts supply chain security at risk, warns NCC Group

92%

of organisations trust that their suppliers follow cyber security best practices.

1/3

of businesses do not conduct regular risk assessments on suppliers.

21%

believe they wouldn’t be affected if a key supplier was unable to operate for five days.

41%

of UK businesses were confident about how they monitor and assess their suppliers’ cyber security practices.

Key findings

The state of supply chain security 2025

68%

of organisations expect the severity and scale of supply chain attacks to escalate further.

45%

of respondents experienced a cyber security breach in the last 12 months.

59%

of respondents were concerned about visibility over their supply chain.

New report

The state of supply chain security

ncc group

The state of supply chain security

What's inside

- Global insights into supply chain security posture
- Details of the changing regulatory landscape
- Practical advice on enhancing supply chain security

nccgroup.com/the-state-of-supply-chain-secu

August 2

Scenario

Your organisation is a mid-sized insurer offering cyber risk policies to commercial clients. Third-party SaaS platforms are used for claims processing and underwriting analytics.

A vendor, who was assessed as low risk based on a compliance questionnaire, suffers a ransomware attack. Their systems are offline for 72 hours, preventing claims being settled across the business.

No contractual obligation exists for cyber incident reporting within 24 hours.

Discussion

- What are your first steps, actions and considerations in this circumstance?
- How do you manage the operational impact and customer expectations?
- What are the implications for your own cyber insurance coverage and liability?
- How do you communicate with regulators and policyholders?

Scenario

While addressing the outage, you discover that an AI-driven underwriting tool, provisioned by another supplier, has been compromised through data poisoning.

This has lead to incorrect risk scores and premium calculations for new policies.

Discussion

- How do you remediate the underwriting errors and prevent financial exposure?
- What steps would you take to review policy wording around AI-related risks?
- How do you strengthen supplier contracts and oversight to mitigate future AI-driven threats?