VENDOR OUTAGE QUICK CARD: DOES YOUR CYBER POLICY RESPOND?

The executive summary for brokers and risk managers: whether a policy responds to a shared cloud, software, or AI vendor outage is decided by contractual wording, not the disruption itself.

THE FUNDAMENTAL COVERAGE RULE: CONTRACT WORDING GOVERNS, NOT SYMPATHY

The client whose operation halts when a major cloud provider or software vendor fails will not be filing an unusual claim. They will be filing the identical claim as thousands of other businesses that morning, into the same claims departments, behind the same vendor status page. What the policy wording specifies — not the severity of the vendor's downtime — decides whether the claim is paid or denied.

THE MARKET SHIFT Insurers Underwrite Correlation

- **Loss Ratio Scar Tissue:** Canadian cyber insurers' combined loss ratios averaged ~155% between 2019 and 2023. Recent stability was bought with rigid underwriting discipline, not luck (IBC).
- **Massive Market Growth:** Premiums grew from $18M (2015) to $550M (2023). More premium on identical shared technology multiplies portfolio concentration.
- **Shared Rails:** Disruption at one widely used provider lands on thousands of balance sheets at the identical moment.

THE CORE EXPOSURE AI Stacks a Second Concentration

- **Layered Dependencies:** Companies adopting the same AI foundation models and APIs repeat cloud infrastructure concentration (IBC & Moody's Ratings).
- **Third-Party Vulnerability:** Reliance on common vendor models creates new pathways for losses to spread across entire books simultaneously.
- **Asymmetric Risk:** AI scales fraud and phishing externally while shared operational rails create single-point systemic failure risks.

THE JULY 2024 PRECEDENT: SYSTEM FAILURE VS. SECURITY FAILURE

In July 2024, a defective software update crashed millions of Windows devices globally, halting airlines, hospitals, banks, and businesses. Operational losses mirrored a massive attack, but **no cyberattack occurred**. Most dependent business interruption forms strictly require a *security failure* at the vendor. Because an update defect is an operational *system failure*, policies lacking an explicit system-failure trigger pay zero. Two clients with identical downtime see opposite coverage outcomes based entirely on this definition.

THE STAKES Contingent Business Interruption in Numbers

Metric	Reported Benchmark	Operational Significance for Insureds
Contingent BI Share	**15% of large cyber claims** by value (1H 2025, Allianz)	Up from 6% in 2024. Vendor downtime is no longer an outlier tail risk — it is a leading loss driver.
SME Cyber Take-Up	**Only 22%** carry cyber insurance at all (IBC 2025)	78% of Canadian small-to-medium businesses absorb 100% of vendor outages out of pocket.
Stand-Alone Cover	**Just 12%** have stand-alone cyber policies (IBC 2025)	The remaining 10% rely on package endorsements whose contingent BI terms are severely curtailed.

THE FIVE COVERAGE CHECKS: FIELD AUDIT REFERENCE

Every dependent business interruption claim outcome turns on five specific policy clauses. Check each on the client's actual specimen form, never the broker summary or proposal sheet.

Check	Key Policy Distinction to Inspect	Claim Implication & Common Trap
1. The Trigger	**Security Failure vs. System Failure:** Does dependent coverage require a malicious breach/hack at the vendor, or does it also answer operational/system downtime?	**The Trap:** Security-failure-only triggers reject claims stemming from defective updates, misconfigurations, or accidental vendor server crashes (July 2024 scenario).
2. The Vendor List	**Blanket vs. Named vs. Infrastructure Excluded:** Does coverage extend to any dependent business, only specifically scheduled vendors, or are utilities/backbones excluded?	**The Trap:** A critical cloud, payroll, or AI vendor missing from a named schedule is completely uninsured. Exclusions for core internet infrastructure (DNS, backbone routing) deny cloud outages.
3. Waiting Period	**Time Retention Threshold:** Typically **6 to 12 hours** before contingent business interruption loss begins accruing.	**The Trap:** An 8-hour outage under a 12-hour waiting period yields $0 recovery, despite causing complete operational paralysis and thousands in lost revenue.
4. The Sublimit	**Contingent Sublimit vs. Main BI Limit:** Dependent BI is commonly sublimited to a small fraction of the aggregate policy limit.	**The Trap:** A $5M aggregate policy declarations page may conceal a $250k contingent BI sublimit that is exhausted after 48 hours of enterprise downtime.
5. What Counts	**Net Income vs. Extra Expense:** Does the wording pay net profit only, or include emergency workarounds (overtime, manual workarounds, rush migration)?	**The Trap:** Restrictive forms exclude workaround costs. Furthermore, the "period of restoration" for dependent events may terminate the instant the vendor reboots, ignoring client backlog.

THE 4 RENEWAL QUESTIONS TO ASK WHILE THE MARKET IS STILL SOFT

Insurers are currently competing for well-controlled risks while pricing strictly on controls. Use these four questions to open the renewal conversation before underwriters raise them:

1. **If each cloud, software, and AI provider went dark for 24 hours, what stops?** (Reveals actual operational dependency list).
2. **Is each of those providers a covered dependent business under current wording?** (Named vs. unnamed vs. excluded on form).
3. **What are the waiting period and sublimit against the client's real daily downtime cost?** (Identifies uninsured financial gaps).
4. **Who owns the AI tools entering the business?** (Prevents uninventoried shadow AI vendors from escaping coverage reviews).

UNDERWRITER CONTROLS Controls That Underwriters Price On

- **MFA Everywhere:** Required on email, remote access, admin portals.
- **Tested Backups:** Offline, immutable, verifiable recovery timetables.
- **Incident Response Plan:** Documented, tested vendor outage runbooks.
- **Third-Party Risk Management:** Vendor SLA tracking & audits.
- **AI Governance:** Centralized inventory & data privacy boundaries.

RENEWAL NEXT STEPS Practical Broker Checklist

1. Pull actual policy forms & dependent BI endorsements from existing binder.
2. Verify system failure triggers are endorsed onto the contract.
3. Map operational dependency roster with departmental IT leads.
4. Compare 24h downtime cost against policy waiting period and sublimit.
5. Present completed control attestations to secure competitive renewal terms.