RT ProExec

Dependent BI:
The Vendor You Didn't Insure

CONTACT
RT ProExec
rtproexecinfo@rtspecialty.com

Or contact your local RT ProExec broker at rtspecialty.com

INTRODUCTION

The biggest cyber losses many companies will ever face may not come from an attack on their own systems. They will come from an attack on someone else's.

In 2024, a faulty software update from cybersecurity vendor CrowdStrike crashed an estimated 8.5 million Windows devices worldwide, grounding flights, disrupting hospitals, and halting financial transactions. In early 2026, Iranian drone strikes damaged Amazon Web Services data centers in the Middle East, disrupting cloud infrastructure for companies across the region. Weeks later, a state-linked threat actor wiped over 200,000 devices at a Fortune 500 medical device manufacturer, disrupting surgical equipment supply chains for hospitals globally. And in March 2026, a North Korean actor compromised the Axios npm package, a software library with over 100 million weekly downloads, potentially exposing thousands of organizations that had no direct relationship with the threat actor.

Each of these events shares a common feature: the organizations that suffered operational and financial disruption were not the ones who were attacked. Their vendor was. The question for those downstream organizations is whether their own cyber insurance policy covers the loss.

That question — the scope and limitations of Dependent Business Interruption (Dependent BI) coverage in standalone cyber policies — is the subject of this article.

1. What Is Dependent BI?

Dependent Business Interruption — also referred to as Contingent Business Interruption in some policy forms — is a first-party coverage component that responds when the insured suffers lost income or extra expense as a result of a disruption at a third-party vendor or service provider. The insured's own systems are not compromised. The loss arises because a company the insured depends on experienced a cyber event, and that event disrupted the insured's ability to conduct business.

Most modern standalone cyber policies include some form of Dependent BI coverage. However, the scope of that coverage varies considerably across carriers. The key variables are: how the policy defines the covered third parties, what type of event at the third party triggers coverage, and what financial losses the insured can recover.

Why This Matters Now
The concentration of critical business functions in a small number of cloud providers, SaaS platforms, and technology vendors means that a single cyber event at one company can cascade across thousands of downstream organizations. The CrowdStrike outage in 2024 demonstrated this at global scale. The events of early 2026 have reinforced it. Dependent BI is no longer an edge case — it is a core exposure for virtually every organization with digital vendor dependencies.

2. Where the Definitions Diverge

With Dependent BI coverage, the question is rarely whether coverage exists, as it is typically included in most policies. The more important consideration is how that coverage is defined. Three definitional elements typically determine whether there is coverage for a Dependent BI claim:

Who Counts as a Covered Vendor?
Some policies define covered third parties broadly — any entity that provides services to the insured, or any entity on whose computer systems the insured depends. These broad definitions can encompass cloud providers, SaaS vendors, medical device manufacturers, payment processors, logistics companies, and software library maintainers alike.

Other policies define covered third parties narrowly. Common restrictions include limiting Dependent BI to disruptions at "IT service providers," "cloud computing providers," "managed service providers," or "network service providers." Under these narrower definitions, a medical device manufacturer whose systems are wiped may not qualify as a covered dependent entity even though the hospital that depends on its products has suffered a real financial loss.

What Event Triggers the Coverage?
Most Dependent BI coverage is triggered by a "security failure" or "network security event" at the third-party vendor. This raises questions in several recent scenarios:

Scenario	Dependent BI Coverage Question
State-linked wiper attack on a medical device manufacturer	Was the MDM-based remote wipe a "security failure" if it was executed through a legitimate administrative tool? Some policies may require the introduction of malware or unauthorized code, which was not present in this attack.
Iranian drone strikes on AWS data centers	A physical drone strike that damages cloud infrastructure is a kinetic attack, not a cyber event. Does a physical attack on a technology vendor trigger cyber Dependent BI, or does it fall under a traditional property policy?
CrowdStrike faulty software update (2024)	The outage was caused by a defective update, not a cyberattack. Most Dependent BI coverage requires a "security failure" at the vendor. A software defect is an operational failure, not a security failure. Some policies have since added "system failure" triggers to address this gap, but many have not.
Axios npm supply chain compromise	The attack compromised a software library that is a dependency in millions of applications. The affected "vendor" is an open-source maintainer, not a contracted service provider. Does the policy's definition of a covered third party extend to open-source software dependencies?

What Losses Are Recoverable?
Even when Dependent BI coverage is triggered, the recoverable losses may be limited. Common limitations include: waiting periods (typically 8 to 12 hours) before BI coverage begins accruing, sublimits that cap Dependent BI recovery at a fraction of the full policy limit, and periods of restoration that may be defined differently for dependent events than for direct attacks on the insured. Some policies also exclude extra expenses from Dependent BI, covering only lost net income, which can leave the insured uncompensated for the costs of implementing workarounds during the vendor's downtime.

3. The System Failure Gap

The CrowdStrike outage in July 2024 highlighted a key structural issue in Dependent BI coverage: the distinction between a "security failure" and a "system failure."

The CrowdStrike event was not a cyberattack. It was a defective software update that caused millions of Windows devices to crash. No threat actor was involved. No malicious code was deployed. The disruption was caused by an operational error at a cybersecurity vendor. Yet the downstream impact on airlines, hospitals, banks, and businesses worldwide was indistinguishable from a cyberattack in terms of financial loss and operational disruption.

At the time of the CrowdStrike outage in 2024, most standalone cyber policies required a "security failure" to trigger Dependent BI coverage. Because a software defect may fall outside that definition, many organizations that suffered significant business interruption may have found their coverage did not respond.

Since then, some carriers have introduced "system failure" triggers either as part of the base Dependent BI coverage or as an optional endorsement. System failure coverage responds when the third-party vendor's systems fail for any reason, including operational

errors, software defects, and hardware malfunctions, not just security breaches. This is a meaningful expansion of coverage, but it is not yet universal across the market, and where it exists, it often carries its own sublimit and waiting period.

Retail brokers should be considering whether their clients' policies include system failure coverage alongside security failure coverage. In a world where the next major vendor disruption is as likely to come from a faulty update as from a cyberattack, the distinction can be material.

4. Concentration Risk and the Cloud

The growing concentration of enterprise workloads in a small number of cloud providers creates a Dependent BI exposure that is systemic in nature. Amazon Web Services, Microsoft Azure, and Google Cloud Platform collectively host a substantial share of the world's enterprise computing infrastructure. A significant outage or attack affecting any one of these providers could disrupt thousands of companies simultaneously.

The early 2026 drone strikes on AWS data centers in the Middle East illustrate the risk in its most literal form — physical destruction of cloud infrastructure caused by geopolitical conflict. But the risk is not limited to kinetic attacks. Cloud providers experience outages from configuration errors, capacity failures, and software bugs. When they do, every customer on the affected infrastructure is impacted.

This creates a challenge for the cyber insurance market. A single cloud provider event can generate thousands of simultaneous Dependent BI claims from unrelated policyholders. Some carriers have responded by introducing specific cloud provider sublimits or aggregate caps on Dependent BI arising from a single service provider event. Others have maintained broad coverage but adjusted pricing and retention levels to account for the aggregation risk.

For policyholders, the practical question is whether their Dependent BI coverage includes or excludes their primary cloud providers, and whether any cloud-specific sublimits or waiting periods apply. A policyholder with $5 million in cyber coverage but a $1 million Dependent BI sublimit for cloud provider events may have less protection than they assume.

5. Software Supply Chain: The Invisible Vendor

The March 2026 Axios npm compromise introduced yet another dimension to the Dependent BI question. The attack targeted an open-source JavaScript library used by millions of applications worldwide. Organizations that had never heard of Axios and had no contractual relationship with its maintainers were exposed to a Remote Access Trojan because the library was embedded somewhere in their software dependency chain.

This is a fundamentally different vendor relationship than a contracted cloud provider or a medical device manufacturer. Open-source software maintainers are not "service providers" in any traditional sense. There is no contract, no Service Level Agreement (SLA), no vendor management process. Yet the downstream impact of a compromise can be just as severe as a disruption to a contracted vendor or worse, because the blast radius is effectively unlimited.

Most cyber policy Dependent BI definitions are not written with this scenario in mind. Policies that limit covered third parties to entities that provide "services" to the insured, or that require a contractual or commercial relationship, may not cover losses arising from a compromised open-source dependency. Even policies with broader language may face ambiguity about whether the open-source project qualifies as a "service provider" or "technology provider" under the policy terms.

The SolarWinds supply chain attack in 2020 and the MOVEit file transfer compromise in 2023 foreshadowed this issue. The Axios compromise in 2026 confirmed it at a scale that is difficult to ignore. As software supply chain attacks continue to grow in frequency and sophistication, Dependent BI definitions may need to evolve to address a category of vendor that most policies were not originally designed to cover.

6. Broker Considerations

Dependent BI is one of the most underexamined coverage components in a standalone cyber policy. The following points may warrant review in connection with current and upcoming placements:

1. Covered Third-Party Definitions
Review whether the policy defines covered vendors broadly (any entity on whose systems the insured depends) or narrowly (IT service providers, cloud providers, managed service providers only). Clients with dependencies on medical device manufacturers, equipment suppliers, logistics companies, or other non-IT vendors should confirm that those relationships fall within the coverage grant.

2. Security Failure vs. System Failure
Determine whether Dependent BI is triggered only by a "security failure" at the vendor, or whether "system failure" is also a covered trigger. After the CrowdStrike outage, this distinction has become one of the most important variables in Dependent BI coverage. Clients who depend heavily on third-party software or cloud infrastructure may want to prioritize carriers that offer system failure coverage.

3. Cloud Provider Sublimits
Identify whether the policy includes specific sublimits, waiting periods, or aggregate caps for Dependent BI arising from cloud provider events. A major cloud outage could affect every company on the platform simultaneously, and some carriers have introduced limitations to manage that aggregation risk.

4. Supply Chain and Open-Source Exposure
For clients with significant software development operations or reliance on third-party software, consider whether the Dependent BI definition extends to open-source software dependencies and supply chain compromises. This is an emerging exposure that most policies do not explicitly address.

5. Waiting Periods and Periods of Restoration
Compare the Dependent BI waiting period and period of restoration to those for direct first-party coverage. Some policies apply longer waiting periods or shorter restoration periods to dependent events, which can reduce the recoverable loss. Clients with thin margins or time-sensitive operations may be disproportionately affected by these limitations.

6. Extra Expense Coverage
Confirm whether Dependent BI includes extra expense coverage or is limited to lost net income only. When a critical vendor goes down, the insured may incur significant costs to implement manual workarounds, engage alternative suppliers, or maintain operations through the disruption. If extra expense is excluded from Dependent BI, those costs typically fall outside the policy.

CONCLUSION

The cyber insurance market has spent years refining its approach to first-party coverage for direct attacks on the insured. Ransomware response, data breach notification, forensic investigation, and business interruption coverage have matured into well-understood components of the standalone cyber policy.

Dependent BI has not received the same attention. And yet the events of 2024 and 2026 suggest that vendor-driven disruptions may represent the most significant and most frequent source of cyber-related financial loss for many organizations. The company that never gets hacked can still lose millions when its cloud provider goes down, its software vendor pushes a faulty update, or its medical equipment supplier gets wiped by a state-linked threat actor.

Retail brokers who understand the definitional nuances of Dependent BI, including covered third parties, triggering events, the distinction between system failure and security failure, sublimits, waiting periods, and supply chain exposure, are better positioned to identify potential issues before they develop into claims disputes. In a market where vendor dependencies continue to grow, this understanding is increasingly important and should form part of the coverage discussions clients have with their brokers.

SOURCES AND CITATIONS

The factual assertions in this article are based on the following publicly available sources and the author's analysis of cyber insurance coverage structures.

CrowdStrike. "Remediation and Guidance Hub: Falcon Content Update for Windows Hosts." July 2024. https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/

Microsoft. "Helping Our Customers Through the CrowdStrike Outage." Microsoft Blog. July 20, 2024. https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/

CBS News. "Iran Says Major U.S. Tech Firms Are Targets in the Middle East, with Drone and Cyberattacks Already Underway." March 13, 2026. https://www.cbsnews.com/news/iran-war-tehran-us-tech-companies-targets-middle-east-drones-cyberattacks/

Associated Press. "Iran-Linked Hackers Take Aim at US and Other Targets, Raising Risk of Cyberattacks During War." PBS News / AP. March 12, 2026. https://www.pbs.org/newshour/world/iran-linked-hackers-take-aim-at-u-s-and-other-targets-raising-risk-of-cyberattacks-during-war

Microsoft Threat Intelligence. "Mitigating the Axios npm Supply Chain Compromise." Microsoft Security Blog. April 1, 2026. https://www.microsoft.com/en-us/security/blog/2026/04/01/mitigating-the-axios-npm-supply-chain-compromise/

Huntress. "Supply Chain Compromise of axios npm Package." March 31, 2026. https://www.huntress.com/blog/supply-chain-compromise-axios-npm-package

Elastic Security Labs. "Inside the Axios Supply Chain Compromise." April 1, 2026. https://www.elastic.co/security-labs/axios-one-rat-to-rule-them-all

Krebs, Brian. "Iran-Backed Hackers Claim Wiper Attack on Medtech Firm." KrebsOnSecurity. March 12, 2026. https://krebsonsecurity.com/2026/03/iran-backed-hackers-claim-wiper-attack-on-medtech-firm-stryker/

Collier, Kevin. "Iran Appears to Have Conducted a Significant Cyberattack Against a U.S. Company." NBC News. March 11, 2026. https://www.nbcnews.com/world/iran/iran-appears-conducted-significant-cyberattack-us-company-first-war-st-rcna263084

Mula, James. "Iran, Cyber War, and Your Policy: War Exclusions, Coverage Implications, and What Policyholders Need to Know Now." RT ProExec. March 2026. https://blog.ryanspecialty.com/iran-cyber-war-and-your-policy

All sources were accessed between March 11 and April 2, 2026. This article does not reproduce copyrighted material; all factual claims are paraphrased from the cited sources.