CONTACT US
Dave Perkins, RPLU
(508) 848-4263
dave.perkins@igpspecialty.com

What is Dependent Business Interruption (DBI) and System Failure?

Dependent Business Interruption (DBI)

Dependent business interruption (DBI) coverage in cyber insurance protects a business from financial losses when a cyberattack on a third-party vendor or supplier causes an interruption to the insured business's operations. For example, if an online retailer loses sales because its credit card processor is hit by a ransomware attack, the retailer could be compensated under its DBI policy. This type of coverage is crucial for businesses that rely on other companies for services, such as cloud hosting, supply chain logistics, or payment processing.

How it works

LOSS OF INCOME: DBI covers lost profits and revenue that occur because a third party's operations are interrupted by a cyber event.

SYSTEM FAILURE TRIGGER: A key feature is a "system failure trigger" which ensures coverage is triggered even if the third party's outage is not directly a cyberattack, but simply a system failure.

VULNERABILITY: It addresses the risk of a "supply chain cyber risk" where a cyberattack on a single software vendor can have a cascading effect on many downstream customers.

EXAMPLES: This coverage would apply if, for example, a company's website is down due to an outage at its outsourced web hosting provider, or a business cannot process payments because its payment processing company is targeted.

IMPORTANT CONSIDERATIONS: Standard BI vs. DBI: Standard business interruption (BI) coverage typically only protects against losses from a cyberattack on the insured's own network, not third parties. DBI is a separate and vital component for addressing supply chain risk, as highlighted by incidents involving third-party software vendors.

WHAT'S COVERED: DBI typically covers losses resulting from a third party's failure but not from a direct cyberattack on the insured's own property, which is covered by different policies.

Dependent System Failure Coverage

Dependent system failure coverage in cyber insurance provides financial protection for a business's income and extra expenses when its operations are disrupted by a failure in a third-party system or service it relies on, such as a cloud provider or web host. This type of coverage, also known as dependent business interruption (DBI), is distinct from standard business interruption insurance, which typically only covers failures of the business's own internal systems.

How it works

COVERAGE FOR THIRD-PARTY FAILURES: It extends protection beyond a company's own network to cover losses resulting from a service provider's system outage.

TRIGGERED BY SYSTEM FAILURE: Unlike traditional cyber insurance that focuses on cyberattacks, this coverage can be triggered by any system failure at the third party, not just a security breach.

FINANCIAL PROTECTION: It can help to offset financial losses, such as a loss of revenue and additional expenses, that occur because the company can't operate due to the third party's downtime.

EXAMPLES OF DEPENDENT SYSTEMS: These can include cloud services, web hosting providers, and other critical third-party vendors that a business relies on for its daily operations.

REQUIREMENT FOR WRITTEN CONTRACTS; Many policies require a written contract with the third-party vendor for coverage to apply in cases of dependent system failure.

Why It's Important

OUTSOURCING IS COMMON: As more companies rely on third-party providers for essential services, the risk of operational disruption due to an external failure increases.

ADDRESSES "SINGLE POINTS OF FAILURE": It addresses the risk that a failure in one crucial third-party service can have a massive cascading effect on many businesses, as seen in recent outages.

MITIGATES SUPPLY CHAIN RISK: It is an important tool for mitigating supply chain risk in a digital environment, protecting against disruptions caused by external failures.

©2026 Innovation Growth Partners Specialty, LLC | igpspecialty.com