Innovation Growth Partners Specialty®

CONTACT US

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

Cyber Third-Party Risk Management Basics

Cyber insurance and vendor contracts are crucial for managing cyber risk because vendor agreements must include specific insurance requirements to protect your business. Key contractual clauses include demanding vendors carry sufficient cyber insurance, be named as an "additional insured," and have a waiver of subrogation. You also need to ensure their contracts have a specific clause stating that liability limitations do not apply to data breaches, as breaches should be covered by the insurance policy instead.

Key Elements for Vendor Contracts

Minimum Insurance Coverage
Specify the minimum cyber insurance limits a vendor must carry, such as for network security, privacy, and technology errors and omissions. Depending on the size and scope of the Vendor, Scope of Work being performed, access to critical data (PII/PHI) or other Network Security Services, the company should establish minimum limits of liability using various criteria.

Scope of Coverage
If the Vendor is a technology vendor, then the scope of coverage they must carry should include Technology E&O, Technology Products and Cyber Coverage. If a Non-Tech vendor, the broad Cyber Insurance should be required.

Additional Insured Status
Require the vendor to name your company as an additional insured on their policy so you are protected by their coverage.

Waiver of Subrogation
This clause prevents the vendor's insurance company from seeking to recover its costs from your company after a claim, which can be important for avoiding litigation.

Liability Limitations
Ensure the contract explicitly states that any limitations of liability do not apply to data breaches. The liability cap should be superseded by the insurance policy's limits for a breach.

Proof of Insurance
Require vendors to provide a certificate of insurance to prove they have the required coverage before and during the contract period.

Maintenance of Coverage
Include a requirement that the vendor maintains the specified insurance coverage for the duration of the service, and potentially for a period after the contract ends.

Indemnification
Include clauses for indemnification to cover your losses from a cybersecurity or data privacy incident caused by the vendor.

Specific Coverage Types
Instead of general terms, specify the types of coverage required, including first-party coverage for expenses like breach notification, data recovery, and forensic investigation, and third-party coverage for claims from others.

Vendor Cybersecurity Controls
An extensive checklist of minimum cybersecurity controls should be provided by the Vendor. Broad implementation of MFA, EDR, Backup Procedures, Patching Cadence and Employee Cybersecurity Training are just a few examples. If the Vendor has access to the company's network, requiring MFA for the Vendor's employees access to the network should be implemented from the company.

When to Be Especially Cautious

Business Associate Agreements (BAA):
If the vendor handles protected health information (PHI), ensure their BAA aligns with HIPAA and HITECH Act requirements.

Varying State Laws
If your vendor operates in multiple states or countries, understand that different privacy laws (like for Personally Identifiable Information or PII) may apply, requiring more comprehensive insurance coverage to comply with all relevant jurisdictions.

Vendor Is Critical
If the vendor provides critical software or support, you may need to negotiate higher insurance limits and more stringent contract terms and cybersecurity resilience. This is especially important for Supply Chain Vendors.

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