Managing Cyber Insurance Clauses in Vendor Contracts

September 2022

Doing business in today's digital ecosystem brings a host of challenges, including presenting issues related to cyber risk allocation. As cyberattacks have multiplied and intensified in severity, negotiating contractual cyber risk transfer provisions has become more difficult.

Organizations that purchase goods and services but fail to adequately review and negotiate vendor contract provisions often learn — far too late — that a vendor's service agreement severely limits the vendor's liability for a security or data breach. In some cases, a contract may completely absolve a vendor of responsibility, unless the purchaser can demonstrate that the vendor acted intentionally or recklessly.

Such less-than-ideal contractual language may effectively transfer a vendor's cybersecurity risk to the purchaser and its insurers, even though the purchaser may have little access to and virtually no control over the vendor's information security.

Overview of major clauses

While a variety of contractual devices can be implemented to transfer or mitigate cyber risk, four major clause types merit particular attention:

01	02	03	04
The liability limitation or cap	The insurance clause	The indemnification clause	Contractual warranties and representations

Liability caps

Of the four major provision types, the liability cap is frequently the most concerning. A typical liability cap will attempt to limit a vendor's liability to the aggregate annual fees the purchaser pays the vendor for its services.

Cyber breach response costs, ransom demands and business interruption losses frequently reach seven figures. A vendor liability cap can thus prove quite problematic for a purchaser that is impacted by a vendor incident. While a cap may be somewhat less concerning if the vendor is earning tens of millions of dollars in annual fees from the purchaser, the vendor usually earns substantially less.

It is not unusual for a vendor system breach to affect the purchaser's ability to conduct business. When a breach is discovered or malicious code interrupts network operations, both a vendor and its clients may be forced to shut down networks and dependent operations. This can lead to a loss of income and a variety of extra expenses.

In addition, vendors that house clients' customer and other sensitive data may expose those clients to notice and reporting obligations under state or federal law. The exposure of that data may lead to customer claims against the purchaser or inquiries by regulators. These losses can quickly add up; aggregate seven- to eight-figure losses are now quite common.

If the purchaser has agreed to a liability cap of fees paid, it may soon discover that it has to fund hundreds of thousands, if not millions, of dollars of its own losses and those owed to third parties, without any recourse against the vendor whose security deficiency led to the incident. Even if the vendor has insurance limits exceeding the amount of the cap, the cap effectively prevents the customer from receiving the benefit of that insurance.

To guard against this possibility, organizations should try to eliminate vendor liability caps prior to commencing relationships. If that is not feasible, organizations can consider asking for an exception to the cap for losses arising from a cyber incident.

When all else fails, the purchaser should attempt to negotiate as high of a cap as possible. This is because significant losses can be incurred by even the smallest of organizations, and any losses exceeding the cap are likely to be borne by the purchaser. If your organization isn't comfortable with the risk posed by a specific vendor's proposed cap, it may be wise to consider another vendor.

Insurance clause

The insurance clause is typically designed to state the type and amount of insurance that a party is required to carry in furtherance of the contract's business objectives. Historically, many insurance clauses were written broadly and would often only require a vendor to have "commercially reasonable" cyber, privacy or network liability insurance up to a stated policy limit. This sometimes led to misunderstandings among the contracting parties about the type of insurance required. It also left open the possibility of coverage gaps.

As cyber insurance has evolved, parties to contracts often now more specifically describe the required coverages. It is no longer unusual for purchasers to specifically require that vendors carry liability coverage for not only third-party claims for data privacy, computer network security breaches, regulatory penalties and electronic media, but also first-party coverage such as cyber extortion, breach notification, forensic and investigative expenses, security, business interruption, credit monitoring and reputational harm.

Specifically describing the desired coverages in a contract helps ensure a vendor has adequate resources to mitigate cyber incident losses. It also helps ensure a vendor can meet its obligation to indemnify the purchaser for damages sustained due to the vendor's negligence or failure of its cybersecurity.

Because cyber risks and cyber insurance coverage are continually changing, it is advisable to periodically review vendor insurance clauses to ensure that contractual requirements match the coverage currently available in the marketplace. This affords the purchaser the opportunity to maximize the protection it receives from a vendor, and reduces the potential for misunderstandings about outdated coverage requirements.

If a vendor provides technical services or products, such as cloud services, software and computer hardware, it is usually a good idea to require the vendor to carry technology errors and omissions coverage. Traditional cyber policies generally do not cover losses due to failures in software, hardware or technology services.

The insurance clause also typically describes the limits a vendor is required to carry. With ever-increasing cybersecurity incidents and escalating response and liability costs, purchasers should require that their vendors maintain as much limit as reasonably possible.

Ideally, a contract should identify the specific limits a vendor is required to maintain. Because some insurers sublimit the amount available to cover certain losses, such as dependent business interruption, the purchaser should make sure it understands the coverage and limits that are available to a vendor and that the contract accurately reflects each vendor's actual coverage. Limits should also be periodically reviewed to ensure they adequately reflect changes in a vendor's risk profile, the size of its operations or level of service it provides to the purchaser.

Insurance available to a vendor will depend on a variety of factors, including revenue security controls, loss history, risk profile and management's commitment to cybersecurity. Therefore, organizations should carefully vet their prospective vendors to ensure they have the track record, capacity and wherewithal to protect their clients from catastrophic cyber events.

Startups and companies without deep pockets may be unable to procure adequate coverage. Those that elect to move forward with these organizations should anticipate bearing some, if not all, of the loss stemming from a cyber incident regardless of the vendor's cybersecurity competency. Fortunately, a good cyber policy issued to the purchaser can cover losses caused by a vendor.

Last but not least, a purchaser should insist that a vendor's insurance coverage be primary and noncontributory. This means that the vendor's policy will be the first to respond to a claim and must be exhausted before any other available coverage — such as the customer's policy — responds. It also means that the vendor's carrier should not be able to seek contribution from the customer's insurance policy. A waiver of subrogation clause in the purchaser's favor may also be desirable, as it will preclude the vendor's insurance carriers from asserting claims for reimbursement for third-party payouts against the client.

Indemnification clause

The indemnification clause in a vendor's contract should be carefully scrutinized and broadly written to indemnify the purchaser for all losses it may incur as a result of the vendor's acts, omissions, services or products. It should also give the purchaser the option to tender the defense of any third-party claims arising from the vendor's activities and products to the vendor and allow the customer to participate and control the defense.

Some vendors may attempt to limit their indemnification obligations to claims arising from their intentional or grossly negligent acts. These clauses may effectively shift the cyber liability risks arising from the vendor's simple negligence to the purchaser and leave the corporate customer with no recourse against the vendor for third-party claims that it pays out or first-party losses that it sustains.

Information security compliance & practices clauses

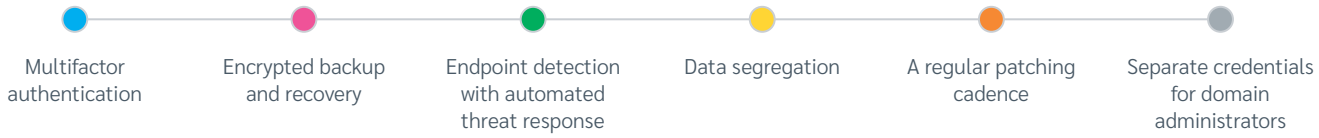
A more recent development, detailed information security compliance clauses are designed to ensure that a party's information security practices meet commercially reasonable standards. Vendors sometimes place these clauses in their service contracts when they want to show a purchaser that it has a robust information security program and to give the purchaser confidence that its confidential information and connected networks will be protected by the vendor. Such clauses may also be designed to prevent the purchaser from imposing more stringent compliance provisions. Purchasers must consider whether more stringent provisions are needed.

Before signing a vendor agreement, a purchaser should consider performing a cyber risk assessment of the vendor's information security programs to test the adequacy of its information security practices and environment. Written vendor representations regarding information security may be incorporated into a contract; purchasers can negotiate the vendor's warranty about its compliance with those practices.

A purchaser should also consider asking the vendor to provide it with audit rights, so that it may periodically review the vendor's information security program to ensure it meets the required standards and any agreed upon key performance indicators throughout the duration of the contract.

Organizations can require a vendor to demonstrate compliance with recognized information security standards, such as ISO 27001 and 27002. Not every vendor will have the financial and organizational capability to do so, however.

It may also be desirable to require a vendor to expressly warrant that it has certain enumerated information security controls in place to guard against potential intrusions, including:



Some purchasers require a vendor to warrant that it has not had any cybersecurity incidents or been the subject of any cyber-related regulatory investigations that have not been disclosed to the purchaser.

A breach notification provision is also often necessary. This clause requires a vendor to notify a customer of a suspected security or data breach within 24-48 hours of its occurrence. This clause is desirable because the purchaser customer is often the controller of the compromised information and may be legally obligated to notify its affected customers within a very short period following its occurrence.

AUTHOR

Paul Lynch
Vice President
Executive Risk Insurance and
Claims Counsel
303.414.6300
paul.lynch@lockton.com

Securing insurance coverage

While robust vendor contracting practices help guard against and mitigate loss, there will invariably be situations where a vendor simply doesn't have enough coverage. Some vendors aren't financially able to obtain sufficiently high limits to protect against a catastrophic cyber event that affects numerous customers and third parties.

For this reason, it is critically important that purchasers obtain robust cyber, crime and technology errors and omissions coverage of their own, with limits suitable to their operations and risk.

For more information or help managing your cyber risks, contact your Lockton advisor or cyber@lockton.com.

This guide is not intended to provide legal advice.

It is intended to provide a brief, high-level overview of the contractual risk transfer provisions that companies should consider examining when negotiating contracts with vendors that handle sensitive information or that provide information technology or security services. It does not, however, address every risk transfer clause, contract provision, or mechanism that may address cybersecurity risk, privacy concerns, technology services or data management.

Because this content does not represent legal advice, qualified counsel should be engaged to review, craft and negotiate contractual cyber risk transfer and services provisions suitable to a company's risk tolerance, available insurance, operations and business objectives.