Negotiating Technology Contracts – Insurance Requirements

By Stephen F. Pinson
Scott & Scott LLP



Image by Pictures of Money

One of the most overlooked sections in a technology-related contract is the insurance section. Whether that contract involves IT services, development, Software as a Service or Cloud Services, the insurance section is just as important as the other risk-allocating provisions contained in the contract. Yet, in most of the contracts in the industry, the original contract is silent on insurance and there is no insurance provision drafted. This leaves a business customer vulnerable to risks that are not covered by insurance. This discussion will help identify what provisions are actually needed in a contract to properly allocate the risks.

The following is a brief list of insurance provisions that parties should include in technology contracts for the different types of claims scenarios between contracting parties. This list describes how each provision works within the contract and what should be negotiated (this is not an exhaustive list). Parties should negotiate individual and aggregate limits for the types of risks involved.

1. Commercial General Liability – This type of insurance, commonly known as GL, is the most basic form of business

liability insurance. This type of insurance protects a business against claims due to injuries, accidents, and negligence. It can protect a business from costs related to bodily injury, property damage, medical expenses, legal costs, judgments, and personal injury claims such as libel and slander. GL is a staple requirement for both the service provider and the business customer, but it will not protect against all risks or threats. To protect a service provider or business customer from more specific types of emerging threats, each party may need to purchase additional liability policies.

2. Professional Liability Insurance, Errors and Omissions – This is also known as E&O insurance and will cover a service provider if it fails to perform according to the requirements in the contract. This coverage will help offset the costs associated with customer claims when the provider's mistake causes a customer loss. Customers may want to insist on E&O coverage to help bridge the gap between coverage offered by GL or other policies.

3. Automobile Liability – If a service provider will use an automobile in any phase of the work performed for the business, the business should require evidence of automobile insurance. In some cases, the service provider will own no automobiles and therefore may not purchase automobile liability coverage; however, the business customer should require evidence of coverage for exposure related to non-owned and hired automobiles. This coverage protects the service provider and business customer in claims arising from the use of personal or rented vehicles by the service provider's employees or principals. If dealing with a sole proprietor, proof of personal auto coverage should be required.

4. Workers' Compensation – If an employee experiences a job-related illness or injury, this policy can help pay for medical expenses and lost income. If a service provider plans to do work onsite at the business customer's location, the

business customer should require evidence of worker's compensation insurance. In some states, worker's compensations can be waived by following certain statutory protocols. The agreement should contain a provision that ensures the business customer will have no liability for the service provider's employees or independent contractors, even if the service provider opted out of workers' compensation. Additionally, if a service provider has no employees, then Workers' Compensation is not generally required by the State.

5. Employer's Liability Insurance – Employer's liability coverage, known as EPLI, is designed to cover claims like harassment, wrongful termination, and other claims that that are not covered by workers compensation or by a GL insurance policy. The primary goal for requiring this type of insurance is that a business customer will want likely claims the services provider may incur to be covered by insurance. Having uncovered risks may make the service provider less able to continuously provide services in the event of a claim by an employee.

6. Cyber Liability – Cyber liability includes numerous subsets of insurance coverage, and customers should carefully examine the particular coverage because it varies greatly among providers. Cyber Liability coverage should include both first-party liability coverage and third-party liability coverage.

- First-party liability coverage applies to direct costs for responding to a claim incident, such as: (1) notifying clients that their information was compromised or exposed, (2) purchasing credit monitoring services for customers affected by the breach or hacking incident, (3) launching a public relations campaign to restore the reputation of the company affected by the breach, (4) compensating the business for income that it isn't able to earn while it deals with the fallout of the data breach, and (5) paying a cyber-extortionist who holds data hostage or threatens an attack.

• Third-party liability insurance covers the people and service provider responsible for the systems that allowed a data breach to occur. It offers protection for the service provider and independent contractors who were responsible for the safe storage of the data. The following is a list of coverage types that should be included in some form or another as coverage for a service provider or business customer when they are seeking coverage for the different types of claims scenarios.

Regardless of whether the coverage is first-party or third-party, the contracting parties should examine whether they require the following categories of coverage:

- Network Security and Privacy Liability – This coverage protects the service provider against losses for the failure to protect a customer's personally identifiable information (SSN, credit card numbers, medical information, passwords, etc.) via theft, unauthorized access, viruses, or denial of service attack.
- Media Communications Liability / Reputation or Brand Protection – This coverage protects against allegations of defamation/libel/slander, invasion or violation of privacy, plagiarism/piracy, copyright/trademark infringement, and other wrongful media communication acts that can hurt a service provider or business customer that is associated with media communications in electronic, print, digital, or broadcast form.
- Data Breach – Data breaches come in many shapes and sizes, but many kinds of cyber incidents, including: malware attacks, malfunctions, insider data breaches, data theft by employees, ransomware, or employee mistakes. Data Breach Insurance may cover these breaches as well as when a hacker targets your service provider or a business customer.
- Data Loss / Interruption of Computer Operations – This type of insurance covers incidents where there is data

loss or interruption of computer operations from an inadequate backup or an insured loss, e.g., a disaster that destroys the computer system or virus. This type of coverage can also reimburse losses related to lost income that a service provider or business customer incurs ancillary to a data loss.

- Regulatory Response – Regulatory response insurance protects against fines and defense costs arising from proceedings brought by any regulatory body against either the service provider or those individuals performing regulatory functions within the business customer's firm when an incident occurs.
- Regulator Defense/Penalties – This insurance covers defense expenses and regulatory fines and penalties imposed by a regulatory agency in connection with a data breach.
- Systems Damage – This insurance covers computer systems that are damaged in retrieving, restoring or replacing any computer programs or other data media.
- Threats or Extortion – This insurance covers incidents where threats or extortion from a hacking attack or virus on a computer system.

7. Umbrella Liability Insurance – Umbrella coverage provides extra liability protection to help protect a service provider or business customer in the event that a loss exceeds the limits of the other policies. There are three basic reasons to maintain an umbrella policy: (1) professional liability insurance can be quickly exhausted by legal defense fees, (2) there are significant business assets to protect, and (3) there are risks of legal claims due to the nature of the products or services provided. This type of insurance is used in situations where "excess liability" kicks in after your commercial general liability coverage has been exhausted. Without this policy in place, a service provider or business customer would be responsible for the additional out of pocket amounts (which can reach into the millions of dollars). Unless

that money has been stashed away for such an incident, a lawsuit would have major financial repercussions, without the extra protection of a business umbrella policy.

8. Self-Insured – Some service providers are so well established that they elect to provide self-insurance against many of the risks identified above and to the extent they have third-party insurance, they do not make the third-party coverage available to the customers. In a situation where a service provider will not include insurance language because it is self-insured, the business customer should include language adjusting the limitations of liability sections and indemnification provisions to adequately provide protection in the event of a loss.

Parties to a technology contract should include a provision requiring the other party to provide evidence of the insurance contained in the contract.

Given the regulatory and privacy risks, it is increasingly important to seek advice from experienced counsel when negotiating a technology contract to make sure the risks are adequately assessed and each party’s interests are protected.