## Technology/Cyber Contracts

March, 2014

The Rough Notes Company, Inc.

*Risk managers need to carefully review contracts with technology providers*

It is very important for a risk manager to - 1- preview, negotiate, and coordinate the terms of all contracts before entering into them to determine how they impact current insurance programs. And today, that includes technology and cyber contracts that the enterprise currently has in place or that will be signed in the future. The risk manager must also evaluate the impact on professional liability coverage programs in place for cyber liability and technology errors and omissions.

Noninsurance transfer, often referred to as contractual risk transfer, involves using an organization's common law right to enter into contracts to contractually shift all or part of the financial consequences of a loss to another party that is not an insurer. This transfer does not necessarily transfer the underlying loss exposure to the third party, but transfers the obligation to pay for a loss, either on behalf of or through reimbursement of the organization. The most prevalent forms of noninsurance transfer are hold harmless agreements and risk transfer to the transferee's insurer.

However, noninsurance transfers have disadvantages. The major disadvantage is that if the party to whom the loss is transferred is unable to pay the loss, the organization is still responsible. Transfers may also fail if deemed to be against public policy or if the contract language is held to be ambiguous.

When dealing with technology companies and individuals that sell technology products and/or provide technology services, you need to look carefully at the contract. Many technology companies have made substantial changes in standard terms of service contracts that govern their products and services. This includes cloud service providers, as well. The following are general clauses that should be reviewed to determine the impact on current insurance coverage programs for technology and cyber exposures within an enterprise.

Limiting liability

Most agreements will have a "General Indemnity or Hold Harmless Clause" that will state that indemnification for losses by the technology professional, service provider, or vendor is limited to bodily injury and property damage to tangible personal property and that data is not considered to be tangible personal property. In other words, if the technology professional, service provider, or vendor were to accidentally erase a client's data, there would be no liability for their enterprise, if such an indemnity agreement were in place. This type of hold harmless clause is not acceptable to the enterprise hiring the technology professional, service provider, or vendor and is generally being removed before allowing the vendor to start work. However, numerous enterprises are not reviewing their contacts and they have accepted this clause without negotiation.

More technology professional service provider contracts are including an "Intellectual Property Indemnity Clause" or "Confidentiality Breach Clause." Generally, these clauses state that the technology professional, service provider, or vendor will not be liable for intellectual property infringement claims arising out of:

• Products that have been manufactured to the specifications of the customer. For example, assume a client provides detailed instructions to a technology consultant about the content of a Web site that the consultant has been hired to design. If, as a result of these specifications, the client is sued for infringing on the trademarks of a competitor, the consultant is absolved of any liability under these circumstances.

• Unauthorized alteration of the product by the customer. Assume that after a Web site design firm has turned over its design to a client, the client modifies it substantially and, within this modification, includes defamatory material about

a competitor that disparages the competitor's products. Accordingly, the contract would require the client to hold the Web site designer harmless if the competitor sues the designer.

• Continued use of the product by the customer, after the technology professional has provided notice of potential Intellectual Property infringement. There are sometimes situations in which a technology professional has designed a product that, for example, unintentionally infringes on an existing patent. Assume that a technology professional, after designing a product for a client, recognizes such an infringement and immediately advises the client to stop using the product. If the client fails to do so, a contract provision to this effect will substantially reduce the technology professional's liability.

Several of the contracts will also state that the technology professional, service provider, or vendor will not be liable for the confidentiality, integrity, and availability of data and applications essential to the operations of the enterprise. Some contracts will state that the technology provider is not responsible for response times, bandwidth limitations, error correction or resolution, and technology upgrades. Needless to say, these issues need to be resolved in the negotiation phase of the contract and the enterprise should seek a commitment and response to all of the above issues. If not addressed, they will become loss exposures that may or may not be covered by the technology or cyber insurance program purchased by the enterprise.

Limitations on liability or pure financial loss indemnity clauses will exist in these contracts. The technology professional, service provider, or vendor will resist contract provisions requiring the professional to provide an indemnity for pure financial losses since they are unlimited. An enterprise can suffer loss of revenues by system outages, data breaches, data loss, and inoperative systems. Ways that losses are limited vary:

• Some contracts may limit the cap to "available-insurance-only" recourse clause. Here, the technology professional's, service provider's, or vendor's liability for pure financial losses is capped at the amount for which his or her liability insurance policy will indemnify a client that suffers a loss as a result of the professional's products or services.

• Some contracts may set or seek a specific monetary cap. The contract could note a specific maximum amount for which the technology professional, service provider, or vendor can be held liable to the enterprise. In other words, a stipulated monetary limit could be agreed upon for loss arising from the tech professional's products/services.

• Some contracts may seek a loss limited to a specific period of time, usually six to 12 months. Here, for instance, an agreement could be made that limits the technology professional's , service provider's, or vendor's liability to losses occurring within a specific period, such as one (1) year, following the installation of a system of computers or a software program for a client.

Indemnity clauses

Information security, privacy, and regulatory obligation indemnity clauses are growing in numbers and require careful attention. The clauses will address the collection, access, use, storage, disposal, and disclosure of personal information, personal financial information, personal health information, and corporate confidential information. Generally, the clause will require compliance to international, federal, and state privacy and data protection statutes and regulations.

The general language will include statements concerning (1) limiting access to authorized employees; (2) security of data centers for off-site storage; (3) security of physical file storage areas; (4) security for networks, device applications, database, and platform security for the cloud systems; (5) security for information transmission, storage, and disposal; and (6) security of authentication and access controls for all media, applications, operating systems, and computer system equipment.

Last, in many cloud service provider contracts, the enterprise will be allowed to conduct an annual audit of the information technology and information security controls used in supplying cloud services to the enterprise. There should be language in the agreement that the cloud service provider should provide certain reports such as compliance to the Payment Card Industry (PCI) Compliance Report, SOC 2 or SOC 3 reports, and any other reports required under the ISO/ICE 27001 certification.

In addition, the enterprise will need to work through the "Insurance Coverage Clauses (Insurance Recourse)" within the agreements. The clauses may require specific coverage for Technology Errors and Omissions, Commercial General Liability, Cyber Liability, Intellectual Property first- and third-party coverages, Media Liability, Cyber Crime with Extortion Coverage, Regulatory Proceeding Coverage, and Incident Response Team coverage. The clause may specify certain coverage limits, waiver of subrogation, primary non-contributory, and additional insured status for the enterprise. These must all be dealt with as per typical contractual liability approaches in the past.

Last, since data is becoming a "cradle to grave" issue for enterprises, the "Termination of Services or Exit Clauses" are becoming an important management issue. Many agreements state that termination cannot occur first without providing the other party with notice and consent. The agreement should address the return of the enterprise's data in a pre-arranged format and that the technology professional, service provider, or vendor will assist with the transition

to the new provider, if necessary. The agreement should also require that the cloud provider include a complete and secure (encrypted) download file of the enterprise's data in the cloud.

Conclusion

These contracts are continuing to evolve. Sometimes these contracts involve several agreements that must be reviewed such as: (1) Terms of Service Agreement; (2) Service Level Agreement; (3) Acceptable Use Agreement or Policy; (4) Privacy Policy and Intellectual Property Agreement or Notices; and (5) General Services Agreement with Fees and Service Schedules. Therefore, it is incumbent upon the risk manager and the agent/broker team to be aware of all the contracts that will be signed. These contracts must be coordinated and be consistent for the noninsurance transfer program of the enterprise to fulfill the legal and business requirements of the enterprise. Last, they must coordinate with the insurance transfer program in place for the enterprise.



**Forward this article to a colleague**

Address To | Recipient Name

Subject

Message

Send | Reset