Transcending the Cloud

A Legal Guide to the Risks and Rewards of Cloud Computing

Cloud Coverage

ReedSmith

reedsmith.com

Cloud Coverage

Authors

Richard P. Lewis, Partner – rlewis@reedsmith.com

Carolyn H. Rosenberg, Partner – crosenberg@reedsmith.com

Introduction

Where clouds form, rain follows. Insurance should be there to protect you. This article outlines steps to consider so that coverage holds when the rain hits.

Cloud Computing may create new risks and exposures, financially as well as reputationally. Traditional and more recent insurance coverage may come into play. On the traditional insurance front, property, and specifically business interruption coverage, may be a natural place to look. These policies are designed to cover first-party exposures—loss to business. Other coverage to consider for claims made by third parties against a company—by stockholders, consumers, the government or other entities—include commercial general liability ("CGL"), professional liability, director and officer liability, employment practices, and fiduciary liability policies. More recently, data privacy and security policies (sometimes called "cyber" policies) should be considered as well.

First-Party Coverage Issues

Cloud Computing Purchasers

The primary first-party exposure is to Cloud Computing consumers, where some event impacts their data or ability to access that data, causing them to lose income. Is this lost Business Income covered under standard first-party policies providing Business Income, Contingent Business Income or Service Interruption coverage?

Business Income coverage is designed to cover a policyholder for loss of profits and unavoidable continuing expenses—"Business Income"—during the period business is affected by damage to property through which the policyholder conducts operations. *Contingent Business Income* coverage is designed to cover a policyholder for lost Business Income when damage to property through which a third party conducts operations prevents that third party from providing services to the policyholder. *Service Interruption* coverage is designed to cover a policyholder for lost Business Income when certain enumerated services provided to the policyholder are interrupted, typically by damage to off-site transmission or generation equipment. Because it is unclear whether any of these coverages, as typically drafted, would cover a Cloud Computing consumer for lost Business Income from damage to, or inability to access, their data, new coverages will need to be drafted.

As to Business Income coverage, note first that such coverage is typically restricted to damage to property at (or within 1000 feet of) the premises, and it seems likely that any damage to property causing a Cloud Computing interruption would not be located at the premises of the policyholder: indeed, one of the prime advantages of Cloud Computing is that the "property" is off-site. It is hard to predict where damage to data would be deemed to have taken place. Indeed, courts may not consider data to be property, susceptible to damage, at all.[1] Relatedly, courts may find that data that simply cannot be accessed has not been damaged. Most courts, however, find that property that cannot be used for its intended purpose has been damaged.[2]

Because a claim based on the inability to access data as a result of problems of a Cloud Computing provider would likely involve data or equipment off-site, it would appear to fit more naturally as a Contingent Business Income claim. Again, however, the policyholder would have to prove that damage to property caused the interruption.

A claim under most Service Interruption provisions would fail because they are limited to the most common services provided a generation ago: electric, steam and telephone services. Further, most such provisions require property damage from a covered cause of loss.

As to all of these coverages, computer or data-related losses are frequently (1) excluded; (2) subject to strange limitations;[3] or (3) subject to extremely small sublimits. Relatedly, such coverages are frequently subject to dollar as well as time (*e.g.*, 24 or 72 hours) deductibles. Redundancies in the operations of Cloud Computing providers will likely limit the duration of the problem, meaning that the deductibles swallow the potential coverage. Nonetheless, any problem may completely shut down a Cloud Computing consumer, causing them to lose a great deal of income. It may also cause the policyholder's customers to turn elsewhere for a time after the interruption, perhaps permanently.

What likely is needed is for policyholders with large Cloud Computing exposure to purchase specialty insurance covering them for loss attributable to loss of, or inability to access, their data, above a clearly identified (and ideally small) deductible. Such coverage must include extensions for the period of time in which losses continue after the interruption because of loss of customer goodwill.

Fidelity bond coverage (which is required by regulation in some industries) is also important to assess. Theft, extortion, and cyber-related loss may be covered. Fidelity bond policies have strict requirements for reporting a loss and filing proofs of loss. Failure to adhere to the deadlines can preclude coverage.

Third-Party Coverage Issues

Third-party exposures may include claims related to websites, data control, errors in privacy protection, defamation, theft, consumer class actions, securities claims and government investigations. Claims may be brought domestically and internationally. The availability of third-party coverage will depend on the type of claim and other terms and conditions in the policies. A brief explanation of potential policies includes:

Director and Officer Liability Coverage—One can envision a potential claim against directors and officers of a company for failing to supervise a Cloud Computing initiative or for being "asleep at the switch," and thereby breaching their fiduciary duties. One can also imagine the Securities and Exchange Commission investigating, or shareholders suing, a company for insider trading, restatements, or financial misrepresentations in disclosures in connection with Cloud Computing investments, insider deals, or other exposures that cause a stock drop or serious financial problems. A D&O policy typically covers directors and officers for claims made against them when the company cannot indemnify them. The policy also reimburses a company for amounts it indemnifies the directors and officers and, if entity coverage is purchased, the policy is designed to cover securities claims made against the company. Coverage will depend on the specific terms, conditions, and exclusions in the policy. Companies should be vigilant in reviewing the coverage to narrow exclusions and seek coverage enhancements.

Professional Liability/Errors and Omission Coverage—Professional liability coverage is designed to cover claims made against the company and its employees for alleged acts or omissions in the context of doing their jobs. This coverage should also be examined and negotiated to avoid specific exclusions that could impair coverage.

Fiduciary and Employment Practices Liability Coverage—Employee benefit plans and stock option claims involving potential fiduciary and trustee liability may be covered under a fiduciary policy. And if employment practices claims such as discrimination, sexual harassment or hostile workplace environment are made, such coverage may be reviewed.

Comprehensive General Liability Coverage—A CGL policy typically provides coverage for bodily injury and property damage, as well as for advertising and personal injury. The definition of "property damage" may exclude electronic data in some policies, and should be addressed as it may be possible to negotiate an endorsement to provide such coverage. "Personal injury" claims may include publication or utterances that violate an individual's right of privacy or are defamatory or disparaging. Exclusions, however, may limit the breadth of coverage.

Data Privacy and Security Coverage

Data privacy and security policies may provide both first-party and third-party coverage. For example, some technology, media, data privacy breach and professional liability policies provide coverage for first-party loss, including internal hacker attacks or business interruption, or expenses to maintain or resurrect data. Coverage for third-party loss may include reimbursement of defense costs and indemnification for judgments and settlements. The claims may include allegations of violations of privacy

rights, and personal information, duties to secure confidential personal information under state and federal laws and regulations, breaches by employees or others, infringement of intellectual property rights, unfair competition, defamation and consumer protection, and deceptive trade practices statutes. The coverage may also include regulatory actions, lawsuits, and demands. Coverage may additionally apply to “breachless” claims, where a potential problem or disclosure can be fixed before it becomes a claim. The policies are relatively new, however, much as employment practices liability policies were 10 years ago. The data privacy and security policies are negotiable and should be analyzed with a coverage lens to reduce uncertainty and broaden coverage for targeted exposures.

Maximizing the Potential for Insurance Recovery

Although no policy is foolproof, the following steps can be taken to keep coverage umbrellas functioning. Working with knowledgeable coverage counsel:

- Inventory all potential policies now. Review any indemnification agreements with vendors or third parties who may owe contractual obligations to the company.
- Analyze the terms and conditions on a "what if" basis, so that companies can determine potential exclusions or terms and conditions that may impact recovery.
- Compare policy forms on the market and negotiate a "wish list" of potential items to clarify and enhance coverage.
- On an annual basis, take advantage of advances in the insurance market and be aware of coverage decisions in the courts.
- If a breach, loss, or claim occurs, know whether, when, how and why to report a claim or potential claim.
- Obtain consent to defense arrangements if the policy requires.
- Keep the insurers informed of claim developments and respond to reasonable requests for information and cooperation.
- Seek consent to settlements and payment of loss or judgments on a timely and informed basis.
- Know the dispute resolution and choice of law provisions in the policies, including the excess insurers.

With knowledge, vigilance, and persistence, cloud coverage—protection when it rains—is possible.

— Biographies of Authors —

Richard P. Lewis, Partner – New York +1 212 205 6063 · rlewis@reedsmith.com

Richard has experience litigating a wide variety of first- and third-party insurance coverage issues. He also has experience in international arbitrations, assisting policyholders in securing coverage under Bermuda forms. Richard frequently speaks and writes on insurance coverage issues. He is a Member of the faculty of the Practising Law Institute, focusing on property and business interruption issues. In addition, he co-authored the book "Business Income Insurance Disputes," (Aspen 2006).

Carolyn H. Rosenberg, Partner – Chicago +1 312 207 6472 · crosenberg@reedsmith.com

Carolyn frequently advises corporations, directors and officers, risk managers, insurance brokers, lawyers and other professionals on insurance coverage, corporate indemnification, and litigation matters nationwide and internationally. Carolyn also assists clients in evaluating insurance coverage and other protections when negotiating transactions and represents them in resolving coverage disputes. In addition, Carolyn is a member of the Social and Digital Media Task Force. She authored the Insurance Recovery chapter of the Social Media White Paper entitled "A Legal Guide to the Commercial Risks and Rewards of the Social Media Phenomenon." She is on the firm's Executive Committee, is Chair of the Audit Committee, and also serves on the firm's Talent Committee. Carolyn was selected by Corporate Board Member magazine as one of the country's 12 Legal Superstars and the top D&O liability insurance lawyer in August 2001 and was confirmed as the nation's top D&O liability insurance lawyer by Corporate Board Member magazine in a feature on superstar corporate attorneys in July 2004. In addition, Carolyn has been recognized by Chambers USA 2008-2010: America's Leading Lawyers for Business.

— Cloud Computing Task Force Leaders—

Joseph I. Rosenbaum
Partner and Chair, Advertising Technology & Media Law Group
jrosenbaum@reedsmith.com
+1 212 702 1303

Adam W. Snukal
Senior Associate, Advertising Technology & Media Law Group
Business & Finance - Corporate & Securities
asnukal@reedsmith.com
+1 212 549 0333

— Endnotes —

[1] *Ward Gen. Ins. Serves., Inc. v. Employers Fire Ins. Co.*, 7 Cal. Rptr. 3d 844, 850-51 (Cal. App. 2003) ("We fail to see how *information, qua* information, can be said to have a material existence, be formed out of tangible matter, or be perceptible to the sense of touch. To be sure, information is stored in a physical medium, such as a magnetic disc or tape, or even as papers in three-ring binders or a file cabinet, but the information itself remains intangible. Here, the loss suffered by plaintiff was a loss of information, *i.e.*, the *sequence* of ones and zeroes stored by aligning small domains of magnetic material on the computer's hard drive in a machine readable manner. Plaintiff did not lose the tangible material of the storage medium. Rather, plaintiff lost the stored *information.* The sequence of ones and zeros can be altered, rearranged, or erased, without losing or damaging the tangible material of the storage medium."); *but see Hambrecht & Assocs., Inc. v. State Farm Lloyd's*, 119 S.W.3d 16 (Tex. App. Ct. 2003).

[2] *American Guar. & Liab. Ins. Co. v. Ingram Micro, Inc.*, NO. 99-185, 2000 WL 726789 (D. Ariz. Apr. 18, 2000).

[3] *Greco & Traficante v. Fidelity & Guar. Ins. Co.*, No. O52179, 2009 WL 162068, at *4-5 (Cal. App. Jan. 26, 2009) (concluding that mysterious loss of billing data, in absence of evidence that it had ever been "stored" on storage media, as required by the policy, and in the absence of damage to any computer equipment, was not direct physical loss to covered property).