BARNES & THORNBURG LLP

The Cloud: Selected Benefits, Risks, And Insurance Coverage Issues (Part 2)

May 5, 2017 | | Policyholder Protection,Insurance,Data Security

Scott N. Godes
Partner
Data Security and Privacy Co-Chair, Insurance Recovery and Counseling Group Co-Chair

In part two of this series, we continuing exploring the benefits, risks and insurance coverage issues associated with the cloud. Read part one.

In addition to the insurance best practices mentioned in part one, the cloud can raise multiple insurance issues that should be considered carefully. For example, how would insurance provide coverage to the cloud provider or the user if there were a data breach or denial of service attack? But, there are other events in the cyberspace that both cloud providers and users should consider, such as the situation where users cannot access the cloud for data, applications, or other purposes and their business is impacted, as is their customers' businesses.

As a first step, it is a best practice to consider the risks involved with cloud computing that are particular to your business and use of the cloud.

The insurance issues specific to cloud users, depending upon the insurance policy at issue, might differ from the issues specific to cloud providers. It is also a best practice to consider what type of data will be hosted, such as whether the data contains personal identifying information, trade secrets, or other corporate information. Another aspect of that best practice would include consideration of whether and how the cloud contract addresses indemnification for a breach or interruption. Making a review of these issues as a best practice might help to identify the type and scope of coverage your company should consider purchasing.

Insurance carriers have started writing exclusions for cyber and privacy liabilities into "non-cyber" insurance policies, and directing policyholders to buy cyber insurance for those risks. The question of whether other insurance policies provide coverage is hotly contested, but can be an expensive dispute that also leads to financial uncertainty for companies. (That said, companies holding non-cyber insurance policies should consider closely whether they provide coverage for cyber-related events after an incident, even if the company also holds cyber insurance.)

Even if cloud users carry their own cyber insurance, consider requiring the cloud provider to carry cyber coverage as well to help fund a loss. They might be more willing to indemnify cloud users if the costs are not coming out of

RELATED PRACTICE AREAS

Commercial General Liability
Copyright, Trademark, and Media Liability
Credit and Mortgage Insurance
Directors and Officers Liability
Employment Practices Liability
Fidelity Bonds and Commercial Crime Policies
First-Party Property
Insurance Recovery and Counseling
Ocean Marine and Cargo Coverage
Professional Liability
Representations and Warranties
Workers' Compensation and Employers' Liability

RELATED TOPICS

Cyber Insurance
Cybersecurity
Data Breach
privacy risks

their own pocket. Moreover, payment by the cloud provider's insurance carrier might be able to be used to fund the cloud user's deductible or retention (although certain insurance carriers dispute that point) or pay excess costs if the user's own insurance limits are insufficient.

Being informed of the coverages offered is a best practice because cyber insurance policies come in many different forms, which requires a careful analysis of the policy language and exclusions. Beyond seeking broad coverage, with narrow exclusions, below are some basic tips and issues to consider:

For cloud users, look at whether cloud computing risks are a covered term addressed specifically and clearly in your policy.

If it is not, review the definition of terms like "computer system" and "network" to determine how broadly coverage is written.

This is a best practice to consider when evaluating so-called first party coverage, such as business interruption and extra expense. Understanding the scope of what is covered under your policy could be critical. For example, the policy may reference coverage for your "computer system." The definition of "computer system" in the policy, however, might exclude (or not reference specifically) the cloud or networks run by third parties.

If your policy definition is narrow for purposes of business interruption coverage, you still may be able to look to contingent business interruption coverage. Contingent business interruption provides coverage for damages impacting your business that are not owned by you – here, the third-party cloud or network. Unfortunately, contingent business interruption limits might be lower than the total policy limits. Therefore, it might be better to consider having a broader definition of "computer system" in your policy that covers the cloud and networks run by third parties than to rely on contingent business interruption coverage.

For cloud users and providers, review the total limits, sub-limits, and deductibles, particularly those applicable to cloud-related risks

Certain carriers have used lower limits of coverage ("sub-limits") that cap the amount of coverage available for claims specific to cloud-based risks for cloud users. Work with your broker to seek limits that your company believes are adequate for the risks, and pay close attention to any sub-limits that the carriers seek to impose.

For cloud providers, consider whether a single limit of coverage will be sufficient for multiple losses or a cascading loss that could affect multiple users. In other lines of coverage, such as general liability, insurance carriers will provide that a limit might apply multiple times (per occurrence limits), subject to an overall aggregate limit. Cloud providers should consider whether such limits could be appropriate for their business risks.

Confirm the geographic scope of coverage

Some policies limit coverage to the United States or put restrictions on how far from your place of business events or incidents must take place in order

to be covered. To the extent that cloud providers host information internationally, it will be a best practice to understand what your policy says about geographic limits.

Consider indemnification exclusions for third-party liability

Applicable to both users and providers, if the cloud is hacked and information is compromised, do you have coverage for sending out required notifications or defending against lawsuits from customers? Significantly, some cyber insurance policies have an exclusion for liability assumed by contract (though often with exceptions). Therefore, a best practice for buyers is to pay close attention to whether cloud-based indemnification losses might be impacted by such exclusions.

For cloud users, consider reviewing your contract with any cloud provider to understand which company bears the risk of a data breach and if there is indemnification for cloud unavailability. This is critical since not all cloud providers take the same sort of security measures.

For cloud providers, if the contract requires indemnification of users, due to the providers' fault, consider whether exclusions for indemnity agreements would impact the insurance.

If you are a provider, consider E&O insurance

If you are a cloud provider, it is also a best practice to review your E&O coverage to determine the company's comfort level as to catastrophic events and whether the policy limits would be sufficient in such a circumstance.