

## Insurance Coverage Basics For Cloud Computing: 3 Cs To Remember

February 23, 2017 | | [Data Security](#), [Insurance](#), [Policyholder Protection](#)

Authored by [Scott Godes](#) and [Kara Cleary](#) The privacy and security of data continues to be a hot button issue for companies, with privacy and security events frequently in the news. What about for businesses that have moved to the cloud? Whether you are a cloud provider or a cloud user, data breaches and denial of service attacks are real risks. Have you considered whether and how your insurance program will respond to those risks? Here are three terms to remember that may help simplify some of the coverage issues:

**Computer System:** Some insurance policies, which provide coverage for cybersecurity and privacy risks, have coverage that could turn on whether there was an impact to your “computer system.” A best practice is to understand whether the insurance policy has a narrow definition of that term. Would it include your company’s use of the cloud or the third-party networks your company is using? For cloud users, consider whether your company should buy an insurance policy that specifically references cloud computing or networks run by third-parties as defined policy terms in order to provide broad coverage.

**Contracts:** How will your company’s obligations under contracts with cloud providers or users be handled under the respective insurance policies? Many cyberinsurance policies continue to contain exclusions for liability assumed by contract, though exceptions to such exclusions also are common. What does this mean for the cloud? Aggressive insurance claims handlers might cite such an exclusion as a reason to deny coverage for contractual indemnity obligations. This could be an important issue for those cloud providers that offer their clients indemnification in the event of a breach or denial of service. In such an instance, how will the insurance company view the contractual obligation to send out required notifications or defending against lawsuits? If your company has contracts with vendors or clients that require indemnification for lawsuits, notification letters, forensic investigation, or other issues, a best practice would be to consider whether your insurance policy would cover those obligations to cloud users specifically.

**Caps:** Even if your company holds insurance policies that provide broad coverage, are there limits on the total amounts of coverage for certain types of losses? Typically, those are referred to as sublimits, as they provide less than the total amount of the insurance policy’s aggregate limit. It is important to understand how your limits and sublimits work for different types of losses, before the event happens. For example, some cyberinsurance carriers use a sublimit in the policy for cloud-based risks. Without a careful review, a policyholder may think they have more coverage for cloud computing losses than what the policy provides due to the cap.

With an increasing number of companies relying on the cloud on a daily basis, it is difficult to overstate the importance of having insurance coverage in place that could help offset financial losses for cloud-based incidents. The three Cs we’ve outlined above serve as a starting point for an analysis of coverage and where there might be room for improved policy language

### RELATED PRACTICE AREAS

Commercial General Liability  
Copyright, Trademark, and Media Liability  
Credit and Mortgage Insurance  
Data Security and Privacy  
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

offered by the insurance company.

|