BARNES & THORNBURG LLP

The Cloud: Selected Benefits, Risks, And Insurance Coverage Issues (Part 1)

May 3, 2017 | | Policyholder Protection,Insurance,Data Security

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

The reality that business data of all kinds is now stored, managed, accessed and maintained in the cloud is inescapable. The reasons for this migration of data from within an organization's network computing system to a vended cloud provider are infinitely varied. In this two-part series, we will explore the benefits, risks and insurance coverage issues associated with the cloud.

Whatever the reason fueling the migration of data, one thing is certain - coupled with the movement of data and the use of cloud services is the introduction of additional risk. It's true that many companies will actually improve the security of their data by shifting to the cloud. In many cases, companies are obtaining better data security when in a cloud environment because they're working with cloud providers that make security a top priority.

It is clear that many of the cloud providers have invested in hardening the security available to customers and that they are at the forefront of addressing cyber risks. Certainly, the security of data in the cloud is of primary importance both to the cloud provider and the cloud user. Understanding the risks specific to utilizing cloud resources is essential to managing, insuring, and avoiding those risks.

One of the primary challenges of using cloud resources is that the services offered by the cloud providers establish a shared responsibility between the cloud provider and the cloud user. Both the cloud provider and the user must be aware of system and data security to prevent a breach in the security. In addition, when a risk is realized, it may not always be clear who is at fault for the system or security failure. There are a lot of misconceptions around the cloud and liability. (Insurance coverage issues specific to the cloud are discussed below.) Many companies assume that along with the transfer of their data, they have also transferred their risk to the cloud provider. Absent a clear agreement that shifts liability to the cloud provider, the practical reality is that in most cases, there's very little protection in terms of liability with cloud providers, unless parties are willing to engage in protracted litigation to determine otherwise.

The shifting of liability is not nearly as easy as the transfer of data and often it may be the case that the responsibility for a data breach rests with the party that collected and maintained the data originally. Perhaps the most notable

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

data protection
data protection
Data Security
Data Breach
Insurance Coverage Issues
migration of data

exception has been in the health care industry, where companies providing support often are classified as “business associates” under HIPAA and might be subject to the same obligations for protecting data as the entity with the original patient relationship. Even here, one could argue that liability transfer does not occur, but rather a liability expansion that includes the cloud provider.

B.Y.O.C.

It goes without saying that awareness of a risk is the first step necessary to begin managing and minimizing the risk. As mobile devices become ever more ubiquitous in the workplace, replete with applications that seek to improve worker efficiency and productivity, many, if not most, of these applications utilize cloud resources and the resulting data is being stored in the cloud application. This reality has spawned yet another new term: B.Y.O.C. or Bring Your Own Cloud.

In a perfect world, the company will be aware of the use of cloud resources by its employees, but companies nonetheless might not be fully aware of the extent of the internal use of cloud resources. Certain cloud providers make it simple to engage their cloud-based service with a mere exchange of credit card information. In those instances, the cloud user might not have reviewed a long and convoluted contract; rare is the employee who actually reviews the terms and conditions for such services when presented as a so-called click-wrap agreement.

It is likely that many of the individual employees are not even aware that when they use an application they are using the cloud to hold data. In the event of a breach of data from such an application, expect finger-pointing as to the issue of responsibility for the resulting liabilities. Another less friendly term used to describe the B.Y.O.C. scenario is “shadow IT.” So-called “shadow IT” often is born of good intentions. Well-meaning employees might use – both via their work computers and their mobile devices – applications that help them be more effective at their jobs. They might be wholly unaware of the risks created by storing corporate data in an unsecured application. The company might not know what applications and cloud providers that workers are using and what data is being stored in the cloud. The company, in such an instance, might not know what information is exposed, where it is going, and with whom it is being shared. They likely do not know if the data is being encrypted, commingled with many other customers, and at times even being mined further for useful data by the application vendor or cloud provider.

Significantly, it is common that contracts among business parties restrict not only the use of data, but also who can have access to the data. In addition, regulatory obligations also restrict the use and access to such data. When employees move restricted data into the cloud without authorization or adequate security, there is an increased risk of regulatory scrutiny involving the business and the employee, as well as the potential risk of legal action between business parties.

Multi-Tenancy

Another risk inherent in utilizing cloud resources arises as a result of multi-tenancy. Multi-tenancy means that multiple, usually unrelated cloud users share the same computing resources: CPU, storage, memory, namespace,

and physical building, which are provided by a cloud provider. The risk of multi-tenancy also includes the potential for the loss or misuse of data resulting from the sharing of equipment, software and resources. In a multi-tenancy cloud network, it could be possible for one flaw in the system used to partition cloud tenants' data could allow another tenant or attacker to see all other data or allow one tenant's data to accidentally leak into another tenant's data partition. It is also possible that a system flaw could allow a malicious tenant to assume the identity of other tenants. This sharing of equipment, software and resources also increases risk as a system malfunction, malware intrusion, hack, or virus experienced by one tenant could leak over to the other tenants' data or to event corrupt the entire system.

Data Protection and Data Loss

The most obvious risk when using a cloud provider is that of data protection and data loss. Although the perception is that all the information uploaded to the cloud is secure, it nonetheless is now available to the cloud provider's staff. How available the data is will be determined by the cloud provider and the terms of the contract for services. Placing data into the cloud gives another entity full control of your data.

The basic risk that is often overlooked by both the cloud provider and the cloud user alike: the very human risk caused by the cloud provider's staff. It is a best practice to understand who and how many people on the cloud providers' team have access to the company's data. Once a company outsources a service and data to a third-party server, that company might consider risks arising from its own staff and also the risk posed by the cloud provider's staff. Through the cloud provider, more people now have access to the data and systems that support the cloud provider, which means extending trust to people whom the data holder has never met and over whom they have no control. One key factor that may affect the risk posed by the cloud provider staff is the use of data encryption. Some companies rely upon the cloud provider to encrypt the data upon receipt.

Arguably, this might make the data available to the cloud provider's staff, potentially adding another layer of potential human interaction. Many companies do not move data to the cloud without first encrypting all data. In that case, it is a best practice to know how data encryption is used and enforced and if private encryption keys are shared among tenants. Unless the company is certain files are encoded (either by choosing a provider that guarantees it or performing the encryption themselves), it is a chance taken with every file transferred into the custody of another entity.

An additional risk that is increased is that of possible government intrusion into confidential data. Some cloud providers refuse to provide a client company's data without a governmental order requiring compliance and notice to the company. Others may not follow this practice, so understanding how your cloud provider interprets their obligations would be a best practice.

Interruption of Data Availability

When data leaves a company's control, and is held by a third-party cloud provider, the expectation often is that the data will continue to be available when needed without interruption of access. Unless clearly delineated in the contract, however, there may not be suitable redundancy and fault tolerance systems in place to assure that access is not interrupted. At times, based on

the contractual terms, there may be differing levels of backup provided. Many contracts with cloud providers provide a limit on down time; the terms of service might provide recourse if the down time exceeds that limit resulting in an interruption of business.

In the event that the company relies upon the cloud provider to perform a component of the business transaction, and an unexpected security failure results in interruption of this business process, there may be a resulting loss of profits and additional expenses.

Cloud users should consider such a risk when evaluating the scope of insurance coverage they have and, when possible, ensure that their insurance policies would provide coverage for such a failure. Another issue to consider is an instance in which a company could lose data, either due to an issue with the cloud provider or with malicious attackers. It is a best practice to understand the extent of the cloud provider's disaster recovery policies to determine if they are adequate to protect, and if need be to restore, the data. Unfortunately, even in the best situations, there may be irretrievable data loss. A best practice is for the parties to address insurance for the risk of data loss when entering into the agreement for cloud based services.

Data Breach

The most obvious risk contemplated by companies that elect to use cloud services is that of data breach. Data breaches come in many forms, but at the very basic level they involve the disclosure of data to third parties not permitted to possess the data. Usually data breaches become an issue as the disclosed data includes either personal identifying information or protected health information. A data breach claim against a cloud provider might be viewed as an errors and omissions (E&O) claim against the provider. The cloud provider may be viewed as not having direct liability to the individuals whose data has been breached under the current state of the law, but there may be a claim from the company for failing in their performance of services, including the securing of the company's data.

A best practice for cloud providers is reviewing their E&O insurance (provided as a stand-alone insurance policy or as a coverage section within a cyber insurance policy) to determine whether it should provide coverage for privacy and cyber-related claims. A related best practice for cloud providers is to consider whether a company that experiences a breach of data held in the cloud due to an act, error, or omission by the cloud provider could demand indemnification based on the terms of the contract or under common law theories of recovery. The cloud provider should consider whether damages claimed by the company could include not only third-party liability claims, but also a claim for damages incurred in responding to the data breach.

Compromised Credentials and Broken Authentication

Data breaches and other malware-type issues are often the result of any number of security lapses, including, for example, the use of default passwords or flawed authentication methods. Many organizations struggle with the management of individual access and data permissions. Similarly, companies might not cut a user's access when they leave employment or when a job change occurs.

Denial of Service

Another attack on cloud providers involves a denial of service attack. Unfortunately, even if repelled, these assaults consume large amounts of processing power; ideally, for the cloud user, they will not be stuck with paying for the additional processing power required. Although many cloud providers may generally be more capable of handling a denial of service attack than the cloud user, they should be prepared with a mitigation plan if they face such an event.

Check back soon for part two of this series.