ADVISEN Productivity & Insight for Insurance Professionals

THE LIABILITY ISSUES of CLOUD COMPUTING SERVICE PROVIDERS

January 2012

Sponsored by:

CNA
For All the Commitments You Make®

THE LIABILITY ISSUES of CLOUD COMPUTING SERVICE PROVIDERS

Executive Summary

"The Cloud" is where many technology companies now reside. Cloud Computing enables individuals and businesses to communicate and operate more efficiently. The technology has helped close the resource gap between small and large companies, leveling the playing field by providing the ability to remotely store and process data. Applications include internal communications, customer relationship management, sales and marketing initiatives. Benefits include overall responsiveness in the marketplace and substantially reducing the time and cost of IT resources required for on-premise software.

As companies increasingly look to benefit from cloud technology, more providers will enter the field, seeking to capitalize on the increased demand. However, a growing list of unique threats has created a host of potential security and privacy issues that can have major implications for both cloud computing providers and their clients.

The term "cloud computing" refers to accessing services or information from third party data centers remotely over the Internet from any location (as if the data were in a cloud).

Introduction

The term "cloud computing" refers to accessing services or information from third party data centers remotely over the Internet from any location (as if the data were in a cloud). Cloud computing is an industry that continues to experience significant growth. Expectations are that it will grow at an annual rate of twenty five percent to $55 billion by 2014. [1]

By enabling organizations to outsource database or software hosting to third parties, companies can achieve significant cost savings. Outsourcing these services allows organizations to bypass purchasing or developing their own infrastructure or software and hiring people for

In the cloud realm, system breaches increasingly represent significant security threats as highly motivated thieves attempt to gain access to valuable information

maintenance and upgrades. Few would argue that this method of computing does not offer businesses potential benefits, however, the service provider and its clients are also exposed to a host of risks including data security, privacy and business interruption, all of which have the potential for financial liability.

State and federal governments have passed legislation pertaining to sensitive or private information, many of which have had implications for cloud providers. These government regulations and an expanding library of case law have and will continue to lead to new exposures. Additionally, the technology industry has experienced changing standards of contracts, which often now have fewer safeguards for cloud providers, therefore increasing the potential for liability. As a result, cloud service providers are more often relying on comprehensive technology errors & omissions policies to help both finance and mitigate their increased risk.

Risks of Cloud Computing

Among the factors that contribute to the risks of cloud computing are vulnerability to hacking, storage of sensitive information by multiple organizations on common servers, access to data by multiple organizations in various locations and varying privacy and data protection laws in different geographic locations.[2]

In the cloud realm, system breaches increasingly represent significant security threats as highly motivated thieves attempt to gain access to valuable information and malevolent hackers seek to cause damage. Examples include unauthorized access to online systems, denial of service attacks and introduction of viruses and malicious code, all of which could result in data being lost, destroyed or improperly disseminated. A breach can also result in business interruption losses, privacy law violations and disclosure of confidential information and can have significant financial consequences for both the cloud provider and its client.[3]

Additionally, both the provider and its clients can be exposed to risks unique to cloud computing. For example, in the cloud environment, hackers attacking the data of one company can also put other companies' that are sharing server space at risk. Or as in the case with Liquid Motors, a Dallas company that provides inventory management and marketing services to national automobile dealers, the illegal activities of a totally unrelated company can have dire consequences.

A highly publicized case involving Amazon brought to light yet another risk of cloud computing.

In this case, the FBI raided Core IP Networks, a Dallas Internet Service Provider. The law enforcement agency was investigating VoIP fraud, and seized servers and backup tapes. Liquid Motors, while totally unrelated, was one of 50 companies whose data and equipment were confiscated. As a result, Liquid Motors was essentially put out of business and was in breach of nearly all of its contracts with automobile vendors throughout the country.[4]

A case involving Sony (in this case, a cloud provider of entertainment services) provides a more traditional example of what most consider a data breach threat. In this example, an ambitious cyber thief breached Sony Corporation's online entertainment networks. The breach exposed the personal data of nearly 100 million users of Sony's PlayStation Network, Sony Online Entertainment and Qriocity film and music service. Sony claimed that the hackers potentially accessed credit card numbers and expiration dates and other personal information including, names, addresses, gender and birth dates among others, all of which is information that could be used to falsify a person's identity. The financial impact of the breach is estimated to be around $50 million as a result of credit-card fraud, repairs to its network, marketing costs and reputational costs.[5]

A highly publicized case involving Amazon brought to light yet another risk of cloud computing. An industry leader, Amazon offers businesses computing resources from its expansive network of data centers. Due to a technical malfunction, hundreds of Amazon's corporate cloud customers experienced service troubles. The issues included the inability to access data, service interruptions and even websites being shut down entirely.[6] As a result, many Amazon cloud clients were unable to access their valuable data resulting in an interruption to their business and significant financial loss. Many customers were surprised to find that Amazon's customer agreement absolved the company for any liability for their "inability to use the services." The incident brought to light a potential consequence of cloud computing and highlighted the importance of, and the complexities in, negotiating safeguards in cloud service contracts.[7]

These and similar incidents have left some businesses questioning whether the benefits of cloud technology are worth the risk. For many, their most significant concern is data security: a survey of organizations using cloud computing services found that 62 percent regarded data security as one of their most significant concerns about cloud adoption, and 55 percent said they were worried about data privacy.[8] Organizations that experience a data breach not only may be exposed to notification, credit monitoring and other direct expenses associated with a breach, they also may be subject to fines and penalties, and can be exposed to lawsuits. Security initially was not the highest priority of cloud service providers, but increasingly the onus is on vendors to address the security concerns of their clients.

While concerns about the privacy and security of personal information have been around for decades, the emergence of the Internet amplified the issue by creating countless situations by which personal information can find its way into the hands of individuals it was not intended for.

Regulatory Requirements and Cloud Computing

Hardly a day goes by that the media are not covering the topic of privacy and security of personal information in some capacity. While concerns about the privacy and security of personal information have been around for decades, the emergence of the Internet amplified the issue by creating countless situations by which personal information can find its way into the hands of individuals it was not intended for. Some of the larger cloud service providers such as Amazon, Google, Facebook and Apple, often find themselves in the center of debates pertaining to privacy and data security. Legislation has been passed both in the United States and abroad regulating how companies are required to store and protect personal information.

In the United States, there is not one all-encompassing data privacy law. Instead, it is a patchwork of laws that contain privacy and data security provisions. These laws relate to specific business sectors and specific populations. A few prominent pieces of legislation include:

- Health Insurance Portability & Accountability Act (HIPPA) (Healthcare)
- Health Information Technology for Economic & Clinical Health Act (HITECH) (Healthcare)
- Gramm-Leach Bliley (Financial)
- Children's Online Privacy Protection Act (COPPA) (Applies to data of children under 13 collected online)
- USA Patriot Act (applies to data that resides or flows through the U.S.)

Additional bills were introduced in the U.S House and Senate in 2011 that also addressed data security and privacy issues. One significant piece of legislation was the Commercial Privacy Bill of Rights Act of 2011 that was introduced by Senators John Kerry and John McCain in April. The Kerry-McCain act would have established "the rights to protect every American when it comes to collection, use, and dissemination of their personally identifiable information (PII).[9]" Similar legislation is likely to be introduced in the future.

Most federal privacy and data security laws address the responsibilities of data owners, but the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009 (The Stimulus Act), specifically addresses the responsibilities and potential liabilities of "business associates," which can include cloud vendors. Subtitle D of the HITECH Act addresses privacy and security

Data security experts often remind customers that it is their responsibility to assure that vendors meet necessary security standards, including regulatory requirements for their industry.

concerns associated with the electronic transmission of health information, in part, through provisions that strengthen the civil and criminal enforcement of HIPAA rules.

In addition to federal laws, forty-six states plus the District-of-Columbia, Puerto Rico and the Virgin Islands have passed legislation requiring notification of security breaches involving personal information.[10] Data security laws provide direction for how organizations are required to keep sensitive information safe as well as instructions on what do in the event of a breach. The data breach notification laws are applicable to all companies, including cloud service providers and their customers.

Data security experts often remind customers that it is their responsibility to assure that vendors meet necessary security standards, including regulatory requirements for their industry. Larger companies may audit key vendors, and companies of all sizes increasingly are pushing for provisions in contracts warranting the maintenance of predetermined standards. Some states now have data security laws that mandate such contractual provisions. The Massachusetts Data Security Regulations, for example, require companies to take "reasonable steps" to select and retain vendors that have the capacity to maintain appropriate security measures for personal information. Vendors also must be contractually required to maintain safeguards.

In contrast to the United States, rather than a patchwork of legislation, the European Union has a comprehensive privacy framework. Through the Information Directive of 1995 and the Directive on Privacy and Electronic Communications of 2002, the European's have taken a more complete approach to setting and enforcing privacy standards and require each member state to have its own law executing the Directive. A draft bill that overhauls the 1995 law, widely known as the "right to be forgotten" bill, recently has been introduced.

The European Union Data Protection Directive and corresponding member state laws can have legal implications when it comes to cloud computing. The biggest implication being trans-border data flow of personal information of European Union residents. Under the Directive, companies are prohibited from transferring personal information of EU residents to countries that do not provide an equal level of protection regarding personal information, including the United States.

In the cloud environment this can have legal implications. The cloud is not constrained by physical geographical boundaries. Data can be stored and/or distributed in one or many data centers around the world which essentially means that data in the cloud can be transferred across several jurisdictions. If the data includes personal information of EU residents the

According to a survey conducted by the Ponemon Institute, the majority of cloud service providers believe that security is the responsibility of their customers.

cloud service provider and its client can be found in violation of European law.[11] To avoid this potential legal pitfall, cloud providers should look into the following:[12]

- *International Safe Harbor Certification* which allows data transfer from the EU to the US, but not from the EU to other countries
- *Model Contracts* which allow data transfer from the EU to non-US countries
- *Binding Corporate Rules* initially designed for multinationals so may not be applicable to cloud providers

Liability in the Cloud

With the risks of cloud technologies becoming more apparent, many are asking who is responsible for security in the cloud. Some cloud clients are currently of the belief that along with the transfer of computing resources and responsibilities also come the transference of financial liabilities for data loss, corruption or business interruption. However, this is rarely the case unless contract negotiations render the vendors contractually responsible. Cloud clients often are left without a financial remedy.[13]

According to a survey conducted by the Ponemon Institute, the majority of cloud service providers believe that security is the responsibility of their customers. Most providers view the availability of their services, lower cost and ease of use as their primary concerns, not security. According to the same survey, this disconnect can have significant financial implications because the majority of service providers contractually place the responsibility of security on their customers and only approximately one third of cloud customers are concerned about the security of their data.[14] As more organizations become aware of this disconnect and review the fine print of the service contracts, those that are concerned about security are going to become more likely to negotiate with cloud providers that assume more of the data security risk.

Changing Standards of Cloud Contracts

Companies are increasingly recognizing that their data is being entrusted to a third party vendor, and that they have few legal recourses against the vendor for the significant financial liabilities that can result from damaged or destroyed data, or from a data breach. Cloud computing agreements typically have been based on traditional outsourcing or technology licens-

Some insurance companies are now supplementing Tech E&O policies by endorsing them with first party cyber liability coverage, therefore becoming a hybrid Tech E&O/ Cyber Liability policy.

ing models that significantly limit the vendor's liability. The Amazon case brought increased attention to this issue. While Amazon provided credits to its effected users, the terms of its contract denied liability for outages and data loss.

For this reason more businesses are reviewing the fine print of vendor agreements and negotiating with vendors to contractually limit the customer's liabilities and to define the vendors' responsibilities for damaged, lost or stolen data. Often the potential liability dwarfs the value of the contract, creating enormous financial exposures for vendors. While some cloud providers may view their agreements as non-negotiable and are unwilling to accept any additional risk, others are open to negotiation and are accepting a portion of the potential liability.

Cloud Insurance

Insurance companies have responded to the increased exposure of cloud service providers by developing insurance products that address their unique risks. A typical commercial general liability (CGL) and a traditional errors & omissions (E&O) insurance policy (especially the newer ones) will exclude claims due to electronic data loss and privacy breaches. The primary insurance protection for these exposures is a technology errors & omissions policy (Tech E&O). Tech E&O policies are intended to provide coverage for financial loss of a third party due to the failure of the insured's products to perform as intended, and for financial loss of a third party for an act error or omission committed in the course of the insured's performance of service for another.[15]

A caveat for cloud service providers, however, is that the typical Tech E&O policy excludes any contractual liability assumed by the insured. For cloud providers this exclusion would essentially eliminate coverage as most liability is assumed via contracts. For this reason it is essential that Tech E&O policies carve-back these exclusions and assume some contractual liability through amendments.

Some insurance companies are now supplementing Tech E&O policies by endorsing them with first party cyber liability coverage, therefore becoming a hybrid Tech E&O/Cyber Liability policy. Examples of losses often covered by this endorsement include breach notification expenses, privacy monitoring services (credit checks) and E-business interruption to name a few. This in addition to an expansive list of proactive services offered by many carriers including forensic experts and consultants, legal experts, public relations support and around the clock IT support will assist in making the provider more attractive to prospective clients.

Finally, for cloud providers with significant liability exposures, insurance capacity is generally not an issue in this segment. It is not uncommon to aggregate tens of millions of dollars of limits in large towers of insurance with a combination of primary and excess coverages.

Conclusion

The success of cloud technology, most notably due to its potential for costs saving, is proof of demand in the marketplace for such services. The primary concern that has potential to hinder growth is how the industry addresses a host of security and privacy issues. A combination of client demands and government regulations are already beginning to force the hands of cloud service providers by causing them to assume more of the data security risk.

As cloud providers are required to assume more risk, insurance will play a more prominent role as a risk financing option. However, the cloud model, which is very different from the traditional outsourcing model, has a unique set of exposures that have not yet been uniformly addressed throughout the insurance industry. For this reason it is important that cloud service providers consult with insurance and risk management professionals with proven track records in this segment. With the proper guidance, insurance programs can be tailored to address the unique exposures of cloud service providers and ultimately make them a more attractive option to both their clients and prospects.

1. Steve Lohr, The New York Times, "Amazon's Trouble Raises Cloud Computing Doubts" (April, 2011) http://www.nytimes.com/2011/04/23/technology/23cloud.html?_r=1&pagewanted=print
2. Saron Klein & Tabitha Sullivan, Pepper Hamilton LLP, "Cloud Services Contracts: Cloud Computing's Dark Lining" (September 2011) http://www.pepperlaw.com/publications_article.aspx?ArticleKey=2193
3. Bruce Cleveland "Cyber Liability Insurance – As a Cloud Provider Can You Afford Not TO Have It?" (August 2010)
4. Kim Zetter, Wired.com "Company Caught in Texas Data Center Raid Loses Suit against FBI" (April 2009) http://www.wired.com/threatlevel/2009/04/company-caught/
5. Cliff Edwards and Michael Riley, Bloomberg Business Week, "Sony Data Breach Exoses Users to Years of Identity-Theft Risk (May 2011) http://www.businessweek.com/news/2011-05-03/sony-data-breach-exposes-users-to-years-of-identity-theft-risk.html
6. Steve Lohr, The New York Times, "Amazon's Trouble Raises Cloud Computing Doubts" (April, 2011) http://www.nytimes.com/2011/04/23/technology/23cloud.html?_r=1&pagewanted=print
7. Andrew Geyer and Melinda McLellan, Bloomberg Law Reports, "Strategies for Evaluating Cloud Computing Agreements" (2011) http://www.huntonprivacyblog.com/uploads/file/Strategies_for_Evaluating_Cloud_Computing_Agreements.pdf
8. Sophie Curtis, "Cloud Industry Forum blames FUD for security concerns," Techworld, republished in ITworld Today http://www.itworld.com/virtualization/244071/cloud-industry-forum-blames-fud-security-concerns
9. "The Commercial Privacy Bill of Rights Act of 2011" Summary, http://kerry.senate.gov/imo/media/doc/Commercial%20Privacy%20Bill%20of%20Rights%20Summary.pdf
10. National Conference of State Legislatures "State Security Breach Notification Laws" http://www.ncsl.org/default.aspx?tabid=13489
11. David Navetta, LLRX.Com, "Legal Implications of Cloud Computing – Part One (the Basics and Framing the Issues) (September 2009) http://www.llrx.com/node/2198/print
12. David Navetta, LLRX.Com, "Legal Implications of Cloud Computing – Part One (the Basics and Framing the Issues) (September 2009) http://www.llrx.com/node/2198/print
13. Drew Bartkiewicz & Meghan McAuley Hannes "Risk Evaporation? Part 1" http://www.cloudbook.net/resources/stories/risk-evaporation-part-1
14. Ponemon Institute, "Security of Cloud Computing Providers Survey" (April 2011) http://www.ca.com/~/media/Files/IndustryResearch/security-of-cloud-computing-providers-final-april-2011.pdf
15. IRMI.com, "Technology Errors & Omissions Insurance (Tech E&O)", http://www.irmi.com/online/insurance-glossary/terms/t/technology-errors-and-omissions-insurance-tech-eo.aspx