The Metropolitan
Corporate Counsel®

www.metrocorpcounsel.com

Volume 20, No. 3 March 2012

Cloud-Computing Risks: Due Diligence And Insurance

Joshua Gold

ANDERSON KILL & OLICK, P.C.

Presently, there is heavy pressure to migrate company data to the cloud. Individuals already shift a large amount of their data to "the cloud" in the form of family photos, vacation videos, contact information, and music. Shifting sensitive business information to the cloud, however, brings with it more complex considerations. Should a company be sending information to a third-party cloud site that hosts data for other businesses? And just what specific information is being sent: customer information? Trade secrets? Employee health information?

Those selling cloud-computing services point to the numerous advantages of cloud computing, including claims of cost savings and enhanced data security. There has been some debate regarding the accuracy of these claims, especially involving promises of heightened data security. It is important to recognize that individuals, small businesses and large institutions opting for cloud computing give up something very important: direct control and oversight of the stored or processed information. As such, it is important that those considering cloud computing size up the risks of relinquishing that control over data to a third party. Customers, employees and co-workers will assume that safeguards and a substantial amount of due diligence will have accompanied the decision and process by which information is stored and handled externally up on the cloud.

***Joshua Gold** is a Shareholder in the New York office of Anderson Kill & Olick, P.C. Mr. Gold regularly represents policyholders, including gaming and hospitality businesses, software companies, financial institutions, and retailers in insurance coverage matters and disputes concerning liability, arbitration, time element insurance, electronic data and other property-casualty insurance coverage issues. Mr. Gold can be reached at (212) 278-1886.*

Joshua Gold

Fueling the debate over the safety of cloud computing are two major data breaches that found their way into mainstream news accounts. One cloud provider was hacked by criminals to the tune of one hundred million customer account files (which included credit and debit card information) according to reports of the incident. The hackers infiltrated the cloud site and improperly accessed the sensitive account information. Unusually, the hackers actually had a legitimate account set up with the cloud-computing site (albeit with phony identifying information and fraudulent intentions), in contrast to the more common scenario of hackers anonymously penetrating another network or system.

For those considering cloud computing, the data security risks described above should lead to a checklist, at a minimum, before the company jumps in with both feet. First, determine how the cloud-computing company erects safety walls between the data stored and processed for one client versus that supplied by another customer. Next, negotiate and resolve issues of indemnification and insurance in the event of a data breach. If a cloud provider will not permit security audits or give meaningful assurances of data safety, then consider seriously whether the projected cost savings is worth the risks incurred – or whether a vendor providing more satisfactory protection is available.

"If a cloud provider will not permit security audits or give meaningful assurances of data safety, then consider seriously whether the projected cost savings is worth the risk incurred."

Also, determine whether your business will have to disclose to its customers, employees and potentially others that certain data that they might have an interest in has been supplied, shared or transmitted to a third party for storage or processing. If you do decide that cloud computing makes sense for some operations, consider whether there are certain categories of information that are simply too sensitive to provide to an external source and, therefore, must remain off the cloud.

Risk Management: Safeguarding Data

Businesses can help make informed decisions regarding the extent to which they use cloud computing by having risk

managers working in tandem with their IT departments and in-house attorneys to protect data created by the business or entrusted to it by outside entities and individuals. A starting point is developing a data security protocol that establishes clear directives regarding the handling of and access to information within the organization, as well as that information that might be transmitted outside the institution as part of cloud computing. Virtually any company that has customers (especially retailers) will have not only its own business and employee information electronically captured but will also have the e-data of its customers, including contact information and customer account information. An important step in the process is to inventory the information possessed and determine its sensitivity. Certain categories of information call out for heightened protection, including health information, personally identifying information of customers and employees, certain types of non-public financial information, trade secrets, customer lists and business processes that yield competitive advantages. Decisions should be made as to whether this information is to be part of the business's cloud-computing plan or not. If it is, then perform due diligence with regard to the cloud-computing vendor's security, insurance and indemnification obligations.

Once such information is identified for heightened protection, it usually is not enough simply to guard against external threats of unauthorized access. It is also important to make intelligent decisions about internal access to protected classes of information. It can be risky (and unnecessary) to grant company-wide access to sensitive business information. Instead, under most circumstances, limiting the access internally to such information based upon necessity and security clearance reduces the risk of unauthorized or improper disclosure of sensitive information.

When using a cloud-computing vendor, businesses should find out what levels of employees within that firm have access to hosted information. Not surprisingly, some cloud-computing firms have several other divisions and business enterprises. It is important to know who has access to the hosted data (and to which categories of data) to get a handle on both the external and internal hacking threat.

You should also maintain the ability to audit a cloud provider. Your investors, employees, customers and business partners will expect such due diligence as part of your decision to (essentially) outsource data hosting and management. While you may be able to outsource the function of purchasing and maintaining computer servers, it is very difficult to delegate the responsibility of data security. At least one firm that used a cloud-computing platform found that out the hard way, as they now confront all sorts of litigation from various stakeholders.

Insurance Coverage Considerations

Insurance coverage is available for losses arising from computer fraud or theft under both traditional and new stand-alone insurance products. While some of this coverage is quite valuable, do not expect it to be customer-friendly.

Closely scrutinize policy terms to determine whether the use of cloud computing would alter or reduce coverage. For example, a common feature of recent network security policies involves clauses that purport to condition coverage on the absence of errors or omissions in the data security measures employed by the policyholder. Such policy clauses may be exploited by insurance companies arguing that the policyholder was somehow derelict in safeguarding computer data from hackers, among others. Furthermore, some policies may attempt to limit insurance coverage if the data breach occurs when a computer is not actively connected to a network. Accordingly, policyholders should steer toward selecting insurance policy forms that are devoid of as many coverage exclusions (aka the fine print) as possible.

Indemnity And Hold Harmless Clauses

Those using cloud-computing services should also seek protection from the cloud firms they consider using. Tools to obtain such protection include contractual indemnity/hold harmless provisions and additional insured status. Seek indemnification from the cloud firm in the event of a security breach that is their fault. You may further be able to condition your business with a cloud firm by becoming an additional insured under the insurance policies of the counter-party. Neither of these steps ensures complete protection against a security breach. Nevertheless, it is better to have these protections as an option than not to have them at all. At a minimum, a company should always seek contractual representations and warranties regarding the cloud firm's security measures and compliance with basic data safety practices.

"Data security measures coupled with risk transfer in the form of insurance coverage … can further a business's risk strategy."

Conclusion

Risk abounds when dealing with electronically captured information. It is therefore no surprise that cloud computing entails risk as well. Data security measures coupled with risk transfer in the form of insurance coverage and indemnification from the cloud-computing firm can further a business's risk management strategy. Due diligence is key here, as no company can truly delegate its data security obligations.