How to Protect Data in the Cloud

by Joshua Gold

Data security never gets easier. The current trajectory of technological innovation creates an ever-more challenging security environment, and the cloud computing revolution is no different. A recent survey indicated that a recurring problem these days emanates from company employees and departments placing data onto the cloud outside the confines established by corporate IT officers. Nearly three-fourths of those surveyed say they have been affected by this so-called "rogue cloud" computing.

As it is, many businesses already find themselves faced with a tricky decision on whether to embrace this technology and migrate their data to the cloud. Even those companies using the cloud extensively have had to decide which categories of information are suitable for cloud migration. Now, some of that strategy has been undermined by employees, divisions and departments making decisions about cloud usage that may or may not align with the corporate view.

All this makes it imperative that data be mapped to make sure the company's IT unit knows what is stored and in what location. Only authorized information should be stored in the cloud. By following this policy — along with routine audits, employee education and company-wide reminders — most companies should be able to enjoy the benefits of the cloud without falling victim to its pitfalls.

Cloud Perils and Risk Management

We have already seen two major cloud firms hacked for customer data. If companies in the cloud want to minimize the adverse consequences of such an incident, it is critical for them to map their data and to ensure company-wide compliance with cloud security protocols. When cloud computing goes as planned, it can be an efficient way to outsource the management of electronically captured information. It may also yield savings like other out-sourcing strategies. When cloud computing goes "off the rails," however, the consequences can be devastating.

If sensitive information is being considered for the cloud, then a central question becomes the level of due diligence that the firm will perform to ensure that the cloud is both suitable and safe to house and manage this data. Due diligence can be conducted at many levels, including questionnaires, assessments of the cloud firm's track record and third-party security audits. The more sensitive the data in question is, the more comprehensive the due diligence effort must be. As part of this process, firms should also consider obtaining representations, warranties, insurance and indemnity protection from the cloud service companies.

Data Security Strategy

Those using the cloud need to create a checklist to deal with all the data security risks. One to-do item should be obtaining the contractual right to enable security audits. If this is a deal breaker to the cloud firm, because they fear security issues in multi-tenant cloud platforms, then it may be reasonable to agree on an independent third-party certification. But if this is the approach used, it is equally important to make sure that the third-party security assessment firm is both genuinely independent and competent.

Additionally, it is critical to encrypt any sensitive data. There may be resistance to encrypting all data placed on the cloud, but if any data is hacked or otherwise exposed, that is going to raise an automatic red flag for regulators and law enforcement. When in doubt, the default should be to encrypt the data before it goes to the cloud.

Furthermore, even encrypted data that finds its way into a data breach has become a source of controversy. Some will second-guess security decisions where more-sophisticated encryption could have been used but was not. So it is advisable for businesses to use state-of-the-art security technology.

A checklist of due diligence and contractual items will vary from company to company, but should typically include:

- establishing clear understandings and obligations for the prompt notice of a security breach (even if the breach affects other customers of the cloud firm)
- interviewing references about their experiences with the cloud firm
- seeking indemnification and hold harmless rights from the cloud firm
- addressing issues of who pays for breach notification costs and forensic work if a breach does occur
- addressing what insurance protection the cloud firm purchases (this is especially important if contracting with a smaller cloud vendor)

Disclosure and Insurance Coverage

Businesses should also explore whether they would have to disclose that data has been supplied, shared or transmitted to a third party for storage or processing. In some cases, this disclosure would be towards clients while in others the stakeholders would be the company's employees.

Businesses will also want to make sure that their insurance (whether under cyberpolicies, business package policies, E&O policies or crime bonds/policies) will respond if they use the cloud. Most insurance coverage can be adapted to cover cloud computing risks, but the devil is in the details. For example, coverage may be contingent on definitions set forth in your insurance policies, which makes it important to ensure the policy terms match the manner in which the business manages its data.

Joshua Gold *is a shareholder in the New York office of Anderson Kill & Olick, P.C. and regularly represents policyholders in insurance coverage matters and disputes concerning arbitration, time element insurance, electronic data and other property insurance coverage issues.*