MANAGING THE LEGAL AND COMPLIANCE RISKS OF CLOUD COMPUTING

Sophisticated business users and ordinary consumers take "cloud computing" for granted. For consumers, computing "in the cloud" is an everyday occurrence through such means as social networking and email platforms. The consumer's concerns mainly involve protecting the privacy of their data. For businesses, however, the concerns of cloud computing go beyond privacy. This article discusses some of the legal and compliance concerns which cloud computing produces, and suggests how such concerns can be minimized.

What is Cloud Computing?

Cloud computing consists of huge pools of computers which are made available to perform computer processing and information technology responsibilities for clients.[1] Clients essentially outsource their data and processing to "clouds" and are able to bypass their in-house servers.[2] The National Institute of Standards and Technology defines "cloud computing" as having these characteristics:

1. On-demand, customer-initiated service that provides server time and network storage "as needed automatically";

2. Ubiquitous network access from thin or thick cloud platforms (e.g. mobile phones, laptops, and personal computing devices);

3. Computing resources that are pooled to serve all customers with "different resources dynamically assigned and reassigned" according to customer's demand;

4. Computing capabilities that can be rapidly and elastically provisioned allowing the customer to scale up or down its use of such capabilities according to its needs and paid for on an as-used basis; and

5. Measured services that can be monitored, controlled and reported to the provider and the customer of the utilized service.[3]

What are the Benefits of Cloud Computing?

Cloud computing enables the user to access their data and applications from either desktop or mobile devices. Services such as Amazon, Google, YouTube, Facebook, and Yahoo are all examples of cloud platforms which are accessible from any location or device. These vendors provide services such as data storage, application development, and software hosting.

Benefits of cloud computing include reduced costs, economies of scale, ubiquitous availability of data and records, and availability of enhanced computing power.[4] Rather than maintaining an over-capacity of computing power, businesses using the cloud can maintain variable capacity levels to match their immediate needs.

How Can Managers Meet Cloud Computing's Compliance Challenges?

Cloud computing affects compliance requirements under federal laws such as Sarbanos - Oxley, Gramm-Leach-Bliley, HIPAA, and Payment Card Industry Data Security Standards. The federal securities laws in general and Sarbanes-Oxley in particular require senior managers to establish and assess the effectiveness of internal controls. Such controls protect the integrity of the company's assets and the accuracy of its financial reporting. Information security controls are a key part of the overall compliance frameworks; without them, internal controls cannot be effective.[5]

Businesses which outsource their data processing to a cloud vendor nevertheless remain responsible for internal control.[6] In fulfilling this responsibility, extraordinary due diligence must be exercised by management in the selection of a cloud vendor. Potential users should examine the qualifications, technology, staff, management style, and past work of prospective vendors. Management should carefully evaluate the third-party's security policies and procedures, data segregation practices, records management regime, audit trail documentation, overall vulnerability, as well as the interoperability of services and portability of data.[7]

Management should also take care to obtain SAS-70 audits by properly qualified auditors. Such audits can assess whether the cloud provider's internal controls are sufficient to ensure that:

- employees are aware of their responsibilities related to the confidentiality, intergrity, and availability of data and information systems;
- there are adequate segregation of duties within the organization to manage responsibilities effectively;
- physical access to computer hardware, network devices, and telecommunications equipment is restricted to properly authorized persons;
- servers and workstations are protected against malicious software; and
- system problems are identified, tracked and resolved on a timely basis.[8]

Moreover, Service Level Agreements should be negotiated which require the vendor to meet specified internal control standards.

CONCLUSION

Cloud computing offers exciting and cost-effective ways for businesses to enhance their computing capacity while also lowering their costs. Yet the risks presented by outsourcing computing capacity come with significant legal and compliance implications. The key to managing such risks is effective due diligence by management and its auditors.

Notes

1. Roland L. Trope and Claudia Ray, "The Realities of Cloud Computing: Ethical Issues of Lawyers, Law Firms, and Judges", p. 6 ("Real Realities").

2. Id.

3. "Real Realities", p. 6.

4. Id., p. 9.

5. Fiona Williams, "Sarbanes, Oxley and You," CSO Security and Risk, www.csoonline.com, October 1, 2003.

6. "The Impact of Cloud Computing of SAS-70 Compliance Issues" www.clob.com ("Impact of Cloud Computing").

7. James Bone, "Developing a Matrix for Cloud Computing Compliance," Compliance Week, published August 4, 2009.

8. "Impact of Cloud Computing", p. 2.