

[Home](#) > [Information Security Magazine](#) > [Columns](#) > Three cloud computing risks to consider

Information Security Magazine

 [EMAIL THIS](#)[CURRENT ISSUE](#)[FEATURES](#)[COLUMNS](#)[HOT PICK & PRODUCT REVIEWS](#)[ARCHIVES](#)[SUBSCRIBE/RENEW](#)

Three cloud computing risks to consider

Issue: [Jun 2009](#) [printer-friendly](#)

THE "CLOUD" is often used as a generic term for any type of Web-based application. It is most commonly used today to refer to the grid or utility computing model, where it replaces local hardware and storage input/output. Organizations are moving to the cloud, some faster than others. However, moving to the cloud presents the enterprise with a number of risks to assess. At the core of these risks is the inability of many cloud/Web 2.0 vendors to meet regulatory and legal requirements. Here are the top three risks:

1. Security: For many organizations, security of information is the most critical risk. This may be driven by a need to protect intellectual property, trade secrets, personally identifiable information, or other sensitive information. Making that sensitive information available on the Internet requires a significant investment in security controls and monitoring of access to the content and the pathways to the information. The logging and auditing controls provided by some vendors are not yet as robust as the logging provided within enterprises and enterprise applications. The challenge here is to ensure that, post incident, the organization has visibility to anyone who had access to the document and what might have been done to the document (edit, download, change access, etc.).

2. E-discovery: The current climate for e-discovery assumes for the most part that an enterprise knows specifically where its information is being stored, how it's being backed up, and how it's secured. The rules also assume that an enterprise will be able to physically examine storage devices and, when required, examine storage media for evidence of erased and/or deleted files. In the cloud environment, the enterprise may have little or no visibility to storage and backup processes and little or no physical access to storage devices. And, because the data from multiple customers may be stored in a single repository, forensic inspection of the storage media and a proper understanding of file access and deletion will be a significant challenge.

3. Computer forensics: For many organizations, computer forensics is a critical component of e-discovery efforts and internal investigations, and often requires physical access to the storage device or computing resource. Much can be learned from information stored by a computer's operating system in physical and volatile storage: information that is retained in a computer's random access memory that disappears almost immediately after a computer is turned off. When data and applications are moved off the local personal computer, the forensics investigator may lose the ability to access very critical information for the case. The provenance of a particular file or the time the file was last accessed can often be crucial in determining how the file was used and who had access to it. If the data storage shifts to the cloud, the ability to obtain uncontaminated copies of evidentiary data may be reduced, if not eliminated.

PREPARE IN ADVANCE

While these concerns may not be absolute barriers to moving data storage and applications to the cloud environment, clearly they are significant obstacles that will require an enterprise to carefully examine its contractual obligations, risk profile, security infrastructure and oversight ability. An enterprise should be prepared to present the vendor with detailed security and legal requirements applicable to their business needs and the nature of the information being stored or transacted.

A major challenge today is that case law involving information stored in the cloud is nearly non-existent. The enterprise must take measures to legally protect intellectual property and secure title over its information. Legal departments may be wary about moving intellectual property, trade secrets and legally privileged information to the cloud due to the lack of relevant case law in this space. In any event, the business must ensure that its security and legal requirements are made part of the contract and that it conducts periodic audits to ensure the vendor is meeting the requirements.

Patrick Cunningham, CRM, was previously a member of the board of directors for ARMA International, a records and information management professional association. Cunningham holds a master's degree in public history from Loyola University of Chicago and has been a Certified Records Manager since 1992. Send comments on this column to feedback@infosecuritymag.com.