Cloudy Daze

Steven J. Ross, CISA, MBCP, CISSP, a retired director from Deloitte, is the founder of Risk Masters Inc. He can be reached at *stross@riskmastersinc.com.*

Is cloud computing[1] really the revolutionary expansion of computing capabilities its proponents claim it to be? Or, is it the natural evolution of outsourcing trends that have been developing for decades? Is cloud computing more secure, or less?

Yes.

PLUS CA RESTE LA MÊME CHOSE…[2]

Most of the concerns about cloud computing that I have read and discussed center on one fact: the data and the software no longer reside in an organization's data center. It would appear that for many there is an internal calculation that possession equals control equals security, but is this equation meaningful? If the big change in cloud computing is the disappearance of data center walls, it is no change at all.

Almost as long as there have been computers there have been services that separate the processing of information from the possession of the equipment to do it. In the 1950s, IBM created the Service Bureau Corp. (SBC) to run programs on SBC's computers on behalf of corporate customers. It was some time before the term outsourcing came into vogue, but Ross Perot's Electronic Data Systems (EDS) was doing just that, beginning in 1962. The economies available through labor arbitrage drove many companies in the West to outsource information technology functions to organizations in Asia. Perhaps the perceptions of the problems with previous outsourcing efforts have raised fears about outsourcing to a cloud computing provider, but they are not new concerns.

Essentially, management's qualms about cloud computing can be reduced to two worries:

- My information is being processed somewhere, but I do not know where.
- My information is in the custody of someone, but I do not know who.

Scary to some, perhaps, but not much different from the fears encountered in another generation when the paper files in a desk drawer were translated to invisible bits in a data center elsewhere. Each time distance is put between the owners and processors of information, the same lessons must be relearned: transfer of custody does not equate to transfer of ownership. The basics of security and control for computing services have never changed:

- The ownership of the information (and its security) remains with the customer.
- The responsibility for executing security is shared between the owner and service provider.
- The owner of the information bears the responsibility for assuring that the provider executes and enforces security over the information.

Just because an organization does not own a data center or pay the operators does not mean that it loses control over the information and software. Reliance on physical controls over the instantiation of information is overrated. Except for backup tapes,[3] which present their own challenges, the data are neither tangible nor portable. Operators as privileged users are indeed a concern, but in today's technology—and tomorrow's—an operator does not need physical access to manipulate the data.

…PLUS CA CHANGE[4]

And yet, there are some substantial differences between older forms of outsourcing and cloud computing. The most obvious is that information is accessed via the Internet, with all that implies with regard to confidentiality and integrity. More subtle, but ultimately demanding more security, is that information technology is transformed into a dynamically scalable service, made possible by virtualization. If the promise of cloud computing is realized, an organization can rapidly expand and contract the software, infrastructure, network and storage it uses. The security that is appropriate for one set of computing resources, especially application data, may be inappropriate for another. With the context switching rapidly, it is difficult to match security with risk on a dynamic basis.[5]

There has been quite a lot written on cloud computing security that does not address this contextual change. The focus instead has been on the security threats that accompany outsourcing:

control over privileged access, difficulties with regulatory compliance, unknown location of data, segregating data among customers, investigative support and vendor viability.[6] There are a number of security considerations that go beyond outsourcing and are unique to the cloud:

- **Risk management is complicated by the dynamics of the services**. Inherent in all risk management approaches is the stability of the resources, if not their value, to be managed. If, for example, cloud computing is to be used by an online retailer for advertising most of the year and expanded for sales in peak periods, the inherent risks are quite different at various times of the year. The risks might be somewhat identifiable if the switch from advertising to sales were carried out at once, but would be much more difficult to determine if the change were effected irregularly over time.
- **Because applications and information are accessed over the Internet, browsers become access control mechanisms, in general, beyond the capabilities of most commercial browsers today.** It is possible to limit destinations and activities with many browsers, but few have the capability to identify users reliably or to limit access with sufficient granularity. Integration of browsers with identification and access management systems is a necessary precursor to widespread use of cloud computing for commercial purposes.
- **It is difficult to quantify and transfer risk through insurance.** Cloud computing providers carry insurance, to be sure, but not for consequential damages to their customers. Owners of information cannot abdicate responsibility to their servicers. At the same time, insurers cannot provide coverage for an unknown and irregularly changeable set of information resources, necessitating either over- or underinsurance. Given those two choices, it is easy to predict that management in many cases would choose the lowest premium and accept (ignore?) the remaining risk.
- **A robust encryption scheme, supported by an equally robust public key infrastructure (PKI), is necessary to achieve confidentiality and integrity for Internet-based services.** With data commingled on a provider's far-flung virtual and actual systems, encryption needs to be employed not only for data deemed sensitive, but for all data in the cloud. (Unfortunately, this opens a vulnerability to loss of data and service availability.) While there are strong encryption algorithms and key management schemes available today, cloud computing demands a global, institutionalized public key management system. Currently, the experience in using both encryption and PKI is hardly universal. There are bound to be serious missteps on the road to gaining that experience.

Information security for cloud computing, as always, comes at a cost. The difficulties mentioned with risk management also make determinations of the cost-effectiveness of security controls problematic. We are still very much in the infancy of cloud computing, and the economics of scale are running counter to this new technology being used broadly by large enterprises. Based on the experience with other new technologies, I expect that cloud computing will proceed with inadequate security, then losses will occur, and finally security will be viewed less as overhead and more as an enabler.

The greatest risk in using cloud computing, in my opinion, is the possibility of corporate amnesia, the loss of information without the possibility of recovering it.[7] This raises the whole issue of recoverability in the cloud, a subject to be addressed in a future column.

ENDNOTES

[1] An entire article could be written on definitions of cloud computing. (In fact, there are already quite a few. For example: Kennedy, Niall, "The Anatomy of Cloud Computing," 14 March 2009, *http://www.niallkennedy.com/blog/2009/03/cloud-computing-stack.html*. Bulkely, William; "How Well Do You Know…The Cloud," *The Wall Street Journal*, 12 October 2009.) For purposes of level setting, I shall define it as dynamically scalable, virtualized computing services offered internally and as a commercial service, using Internet technology for access.

[2] Jean-Baptiste Alphonso Karr (1808-1890), "plus ca change, plus ca reste la même chose," "the more things change, the more things stay the same."

[3] Ross, Steven J.; "Falling Off the Truck," *Information Systems Control Journal*, vol. 3, 2006

[4] *Op cit*, Jean-Baptiste Alphonso Karr

[5] Readers might find value in a podcast I made, "Cloud computing data security creates challenges for compliance officers," *http://itknowledgeexchange.techtarget.com/it-compliance/cloud-computing-data-security-creates-challenges-for-compliance-officers/*, 29 July 2009

[6] There are many sources for these views. See Heiser, Jay; Mark Nicolett; "Assessing the Security Risks of Cloud Computing," Gartner Inc., June 2008. I am not giving short shrift to this Gartner publication. Rather, it is representative of much that is currently published.

[7] As of the time of writing, customers of T-Mobile and Microsoft's Sidekick are experiencing a significant data loss. See "Some Users May Lose Data on a T-Mobile Smartphone," *New York Times*, 11 October 2009.