Cloud Computing and Production Systems

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University

In the continuing series of additions to chapters in a security textbook, here's one of the sections I wrote about production controls and cloud computing.

The history of production computing is repeating itself: in the 1960s through the 1980s, computers were so physically large and hugely expensive that many smaller organizations contracted with *service bureaus* to access computing resources. Connections in physically close locations (e.g., city cores) were often through physical coaxial cable or twisted pair connections. For more distant connections, clients linked their *dumb terminals* to the *mainframes* through telephone lines using *modems*. Sometimes the switched telephone connections through the *plain old telephone service* (POTS) were fixed in place and dedicated to the connection – hence they were called *dedicated lines*.

Today, as we approach the middle of the 2010s, the speed of Internet connections is reaching 10 Gbps – an enormous bandwidth that facilitates remote access to banks of computing power of almost unimaginable power.[1] Organizations are capitalizing on the possibility of creating virtual machines (virtualization) that insulate concurrent processes from each other, allowing far more efficient sharing of centralized resources than running processes on dedicated systems in-house. Inexpensive computers (thin clients) with relatively little application software and local disk storage can be used to access all the necessary programs and data required for the organization's business through access to cloud services.

In March 2013, industry analysts said, "More than 60% of all enterprises will have adopted some form of cloud computing in 2013, according to Gartner Research. The cloud market is slated to grow to $131 billion worldwide this year, or 18.5% over the $111 billion last year. In its 2013 State of the Cloud Report that surveyed over 1200 IT professionals, IT-reseller CDW found 39% of organizations are already using some form of cloud solution, an 11% increase over 2011."[2]

IDC reported that "In coming years, the economic impact of cloud computing will be vast. Each year a greater percentage of businesses IT budgets are earmarked for cloud. An expansive study by the International Data Corporation (IDC)… reported that, in 2011, businesses spent $28 billion on public cloud IT services. Amazingly, the spending on public cloud expected to surpass $207 billion worldwide by 2016…." The researchers analysed trends in specific industries:

- Banking: increasing use of cloud computing

- Healthcare: slower adoption

- Manufacturing: particularly strong growth for customer relationship management (CRM) and among smaller businesses

- Insurance: increasing use

- Communications/media: particularly strong user of storage-on-demand.[3]

Gartner also predicted that, "… by 2015, 10% of overall IT security enterprise capabilities will be delivered in the cloud, with the focus today clearly on messaging, Web security and remote vulnerability assessment. However, there's also the expectation there will be more on the way, such as data-loss prevention, encryption, authentication available too as technologies aimed to support cloud computing mature."[4]

As with service bureaus of yesteryear, cloud computing poses special challenges for operations security and production controls.

- The reliability of employees hired to handle confidential and critically important data is out of the hands of the client organization.

- Management policies, monitoring, software maintenance, audits – all are potentially handled exclusively by employees of the cloud-computing provider.

- Bring-your-own-device (BYOD) practices are facilitated by access to remote cloud services.

- Quality of service (QoS) issues and details of the service-level agreements (SLAs) complicate the contractual relations between providers and customers.

Cloud computing, like service bureaus, can provide cost-effective growth paths for smaller business and can offload information technology used for IT functions that are not viewed as mission-critical, allowing IT staff to concentrate on innovative, highly productive applications that can differentiate an organization in its marketplace. They allow for graded increases in computing power without forcing organizations to follow step-functions with large investments in much bigger equipment and increased operational costs. However, extending one's IT infrastructure into centres run by separate entities with their own profit motives requires careful attention to security. At a minimum, organizations should implement the following recommendations for maintaining adequate controls over their production environment when it is in a remote site using cloud computing:

1. During evaluations of multiple vendors, be sure to contact clients of each firm to have personal discussions of their experience with the providers' service level agreements and performance, openness of communications about production controls, cooperation in site visits, and adequacy and cooperation in resolving problems.

2. Examine the adequacy of encryption for all stored proprietary data. No cleartext data should be accessible to employees of the cloud-hosting company at any time – including while decrypted on the virtual machines running on their servers.

3. Be sure that virtual private networks are in place for all Internet-based data transfers.

4. Explicitly discuss update standards for all the software your organization plans to run on the cloud service. Are you responsible for such updates or is the cloud vendor?

5. Be sure that all software running in the cloud on behalf of the customer organization

respects the terms of the vendors’ licenses. For example, be sure that a one-user license is not being applied to a thousand concurrent virtual machines on your behalf.

6. Understand and analyse the business-continuity planning (BCP) and disaster-recovery planning (DRP) in place to ensure continued operations on your behalf should there be problems at the cloud vendor’s site(s). Are the exact terms spelled out to your satisfaction in the contracts? Are there provisions for testing the adequacy of the BCP and DRP?

7. Ensure that the contract allows for external audits which can be initiated by the client. Independent evaluation of the security, QoS and continuity of operations (CoO) is essential for the protection of the client.

8. Discuss the vendors’ security policies and practices, including real-time monitoring for breaches (situational awareness), handling malware, and vulnerability analysis, including penetration testing.

9. Evaluate the billing processes carefully: what determines the periodic invoicing – concurrent users? Total number of sessions? Detailed algorithms measuring such elements as disk I/O, CPU cycles, swapping to and from virtual memory, or bandwidth utilization? Model the costs if possible using detailed information from your own existing systems.

NOTES

[1] Bandoim, L. “Growth of Cloud Computing and ERP Continues to Accelerate.” *Technorati | Technology | Cloud Computing* (2013-05-04). http://technorati.com/technology/cloud-computing/article/growth-of-cloud-computing-and-erp/

[2] Nain, A. “With The Cloud Market Set To Flirt With 20% Growth In 2013, How Can You Play It?” *Seeking Alpha*, 2013-03-20. http://seekingalpha.com/article/1291461-with-the-cloud-market-set-to-flirt-with-20-growth-in-2013-how-can-you-play-it

[3] Weeks, J. “Vertical Markets – 2013 Growth Predictions for Cloud Computing.” *US Signal Blog*, 2013-01-16. http://blog.ussignalcom.com/blog-1/bid/259630/Vertical-Markets-2013-Growth-Predictions-for-Cloud-Computing

[4] Messmer, E. “Gartner: Growth in cloud computing to shape 2013 security trends: Gartner predicts by 2015, 10% of overall IT security enterprise capabilities will be delivered in the cloud.” *Network World*, 2012-12-06. http://www.networkworld.com/news/2012/120612-gartner-cloud-security-264873.html

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *