

**Statement of
James Sheaffer, President
North American Public Sector, CSC**

**United States House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection,
and Security Technologies
October 6, 2011**

Mr. Chairman, Ranking Member Clarke, and Members of the Subcommittee, it is an honor to appear before you today to discuss security implications of cloud – or shared -- computing. The Subcommittee laid a good basis for today's discussion in its April 15 hearing on promoting Department of Homeland Security cybersecurity innovation and securing critical infrastructure, and its June 24 hearing on the homeland security impact of the Administration's cybersecurity proposal.

I am Jim Sheaffer, President of CSC's North American Public Sector. Recently I served as Vice-Chair for the Public Sector of the TechAmerica Foundation's Commission on the Leadership Opportunity in U.S. Deployment of the Cloud (CLOUD²). The mandate of the Commission was to provide recommendations on how the federal government could deploy and accelerate the adoption of cloud technologies, and to address public policies that would enable U.S. innovation in the cloud. In July, the Commission issued a report -- *Cloud First, Cloud Fast* -- that addresses some of the issues we are discussing today.

Let me begin by offering a brief word about CSC. Last year we had revenues of just over \$16 billion. Three-fifths derived from IT services provided to the private sector, and two-fifths from a range of services for the public sector. Acknowledged as a leading global provider of IT services, CSC delivers large-scale IT projects for both public and private sector clients. We provide cybersecurity to some of the world's largest companies, including critical infrastructure providers, and some of the most sensitive U.S. government agencies.

Cloud Computing

By leveraging shared computing resources, higher utilization rates of computing hardware, and economies of scale, cloud computing is ushering in an IT revolution which promises far lower costs while greatly improving capacity and performance. Cloud computing combines self-service provisioning of software applications and IT infrastructure with on-demand scaling of computing and storage in which users pay only for what they consume. Cloud computing and "as-a-service" delivery enable

organizations to slash unit costs of computing, and build capacity for rapidly growing volumes of data and burgeoning requirements for computation.

Cloud computing is a hot topic. In essence, it is just the latest evolutionary step that has taken us from custom-built computers to mainframes to personal computers to client-servers, and then to the Internet. What is different about cloud computing is the accelerating pace of change, rapid adoption rates, and global nature of its use.

Cloud innovation allows entrepreneurs and public sector innovators to create value at little to no capital expense in computing resources, unlike the previous waves. Cloud computing disrupts existing business models and enables wholly new ones. The explosion of mobile computing catalyzes even faster adoption of cloud computing.

Cloud computing hardware can reside on-premise at an organization's facility, or off-premise, such as at an IT provider's facility. The National Institute of Standards and Technology (NIST) defines four types of environments for cloud computing: (1) *Private cloud* that is operated by an organization and may exist on premise or off premise; (2) *Community cloud* that is shared by multiple organizations related to a specific community and may exist on premise or off premise; (3) *Public cloud* that is available to the general public, owned by a commercial vendor and located off premise; and (4) *Hybrid cloud* that is a combination of two or more clouds (private, community, or public).

Trust

Today's tight federal budget climate offers an added incentive to agencies to adopt the cloud. But while cloud computing offers substantial benefits, such as cost savings, speed, and responsiveness to mission needs, it also raises questions of trust. Trust encompasses such concepts as security, availability, reliability, transparency to the user, and ability to extract data.

The pace and degree of adoption of cloud delivery services will depend on establishing a basis of trust. This begins with understanding the risks and challenges. Can important data be entrusted to the cloud? Are there new risks and challenges to trust, especially the security of data?

Let us look at the new risks and challenges to trust. One, the speed of cloud technology advancement requires new security policies, and even new technologies and procedures, to keep pace with cloud advancements. Most current knowledge about IT security is based on a world in which most computer resources are under the direct control of a person or organization and in which physical and technical means exist, including software firewalls, to control access. Moreover, the Internet was originally designed without a primary focus on security; since then computer security specialists have played catch-up.

Many of those security concepts must be reconsidered for a world in which cloud computing enables a much broader spectrum of solutions and much greater cost savings derived from the sharing of computing, storage, and network resources, bringing new economies of scale. For example, firewall technologies designed for operating inside the virtual fabric of cloud architectures -- the design of cloud computing systems -- are just now becoming available, and they remain largely untested.

A second risk is that all of the required security standards for cloud computing are not yet in place. Clear, understandable, and verifiable standards are essential for building trust. The National Institute of Standards and Technology and the Cloud Security Alliance -- a non-profit coalition of practitioners, companies, and associations -- are conducting research and developing new cloud security standards.

Third, while not specific to cloud computing but relevant to it, cyber threats are serious and dynamic -- and becoming more pernicious. Business and government alike face threats much more severe than in the past, and more likely to change and do so swiftly.

Advanced Persistent Threats tend to be state-sponsored and target especially sensitive information, such as military and financial data and intellectual property. Such information lies at the heart of America's security and economic well-being.

The risks and challenges to cloud computing are substantial but not insurmountable. Of fundamental importance, cybersecurity must be integral to cloud computing architectures and not be "bolted-on" after the fact. CSC participates in various forums that develop standards. CSC's rigorous validation and testing programs promote innovation for security solutions.

On balance, we are confident that prudent cloud computing will satisfy stringent security requirements. USCYBERCOM Commander General Keith Alexander said it best to a House Armed Services Subcommittee last March:

"The idea is to reduce vulnerabilities inherent in the current architecture and to exploit the advantages of cloud computing and thin-client networks, moving the programs and the data that users need away from the thousands of desktops we now use -- up to a centralized configuration that will give us wider availability of applications and data combined with tighter control over accesses and vulnerabilities and more timely mitigation of the latter."

Ways to Enhance Security

How should security risks and challenges be addressed? The key is to align risk profiles of varying types of data and uses with levels of protection required.

Understanding the risk profiles of data being considered for the cloud is key to determining the required levels, and hence costs of security. One-size-fits-all

approaches provide neither effective security nor the lowest cost solution. Each software application and data set must be evaluated to identify its specific security requirements. For example, published scientific research may be suitable for less stringent cloud computing environments than are needed for classified intelligence data on potential terrorists. CSC is assisting federal agencies to develop roadmaps that outline risk profiles of data sets and identify appropriate cloud solutions.

It will be important to gain feedback and learn lessons from implementations of cloud computing. They can help identify best practices and improve security for future uses.

Federal Policy

Federal policy on cloud computing and its security has evolved rapidly. In 2002 the Federal Information Security Management Act, or FISMA, came into force. It establishes a “comprehensive framework designed to protect government information, operations and assets against natural and man-made threats,” and requires program officials, chief information officers, and inspectors general to conduct annual reviews of information security.

The Federal Risk and Authorization Management Program, or FedRAMP, was initiated in 2010 to provide a standard approach across the federal government for assessing and authorizing cloud computing services and products. A common security risk model enables the federal government to “approve once, and use often.”

In the *25-Point Implementation Plan to Reform Federal Information Technology Management*, issued on December 9, 2010, the Office of Management and Budget called for reducing the number of federal data centers by at least 800 by 2015 and creating a federal-wide marketplace for data center availability. Curiously, not one of OMB’s 25 points focused on cybersecurity.

On February 9, 2011, OMB issued a *Federal Cloud Computing Strategy*, which gives more attention to security. It cautions that cloud security is an exercise in risk management, “identifying and assessing risk, and taking the steps to reduce it to an acceptable level.” Risk management based on intelligent risk assessment enhances the protection of the most valuable information and is more cost-effective than compliance-based approaches.

The *Federal Strategy* points to several potential security benefits of cloud computing. The first is the ability of the cloud provider to focus centralized resources on security services. Second, the greater uniformity and homogeneity of the cloud platform eases security management and improves response times. A third benefit is the improved resource availability of the cloud provider through scalability, redundancy, and disaster recovery capability. Fourth are the improved backup and recovery capabilities and procedures that a cloud provider can offer. A fifth potential benefit of cloud computing is the ability to leverage, as needed, services from other data centers.

At the same time, the *Federal Strategy* highlights potential vulnerabilities of cloud computing. One is the inherent system complexity of a cloud computing environment. A second vulnerability is dependency on the service provider to maintain secure logical separation in a shared computing resource, or what is called a multi-tenant environment. A third potential vulnerability is the cloud user's need to have sufficient knowledge of potential threats and vulnerabilities to know how to make decisions and set priorities on security and privacy.

Increasing experience in the implementation of cloud computing, with careful attention to security, will help validate and refine our collective understanding of its benefits and risks.

The Department of Homeland Security is laudably reaching out across the federal government and the private sector to foster a more secure and resilient cybersecurity environment. The DHS Chief information Officer is leaning forward to show leadership in cloud adoption.

In moving data from twenty-two separate components into the primary DHS Stennis data center and a secondary backup center, DHS has increased the productivity of its capital investment in computing. While migrating into the two consolidated data centers, DHS has also implemented a private cloud behind a DHS-controlled firewall and security systems. As new security standards are developed and effectively verified, more data will be ready to move to the cloud. In addition to private cloud implementation, DHS is moving certain public-facing websites, such as DHS.gov and FEMA.gov, into a public cloud in order to increase efficiency and productivity. DHS is an early and prudent adopter of cloud computing and its experience may be instructive for others.

Cloud Examples

Let me outline three examples of how cloud computing can be implemented in a homeland security context.

First, CSC helps a global chemical company that is part of America's critical infrastructure. Its research unit must allow access to scientists and others from inside and outside the company to foster collaboration for new discoveries. Researchers require high performance computing and surge IT capacity, and they store highly sensitive intellectual property. The research unit must accommodate projects that start and stop abruptly and then restart.

CSC has installed a private cloud that the chemical company manages to satisfy its own special security requirements. The company has deployed cloud access at each of its laboratories around the world, and CSC federates and orchestrates cloud services across the chemical company's global IT infrastructure.

In a second example, DHS wanted more responsive computing. It opted for cloud computing for the development and testing of new computer application systems. This eliminates costly and time-consuming tasks of procuring, installing, and testing new computer hardware and software every time a software development team starts a new project.

To support DHS, CSC designed and is implementing a private cloud that will reduce the time to provision new development and test environments from months to just a couple of days. We are also assisting with a strategy and plan for helping DHS encourage management and cultural changes required to take best advantage of the cloud.

A third example is the potential for increased use of unmanned aerial vehicles to help DHS monitor U.S. borders. Evolving technology will allow aerial platforms to collect greatly increasing amounts of ground imagery. As this develops, cloud computing could assist DHS to expand data collection and processing while holding down computing costs.

Recommendations

I wish to call special attention to four important recommendations from the TechAmerica Commission Report, and offer a fifth recommendation.

First, the federal government and the private sector should support the creation of international standardized frameworks for securing, assessing, certifying, and accrediting cloud computing.

Second, the public sector and the federal government should accelerate the development of an identity management ecosystem to facilitate the adoption of strong authentication technologies, enabling more secure access to cloud services and websites.

Third, a law is needed to clarify responsibilities of companies to notify customers in the event of data breaches, and strengthened criminal laws are required against those who attack computer systems, including cloud services.

Fourth, the federal government and the private sector should develop and execute a more robust joint research agenda for cloud computing.

Fifth, verification and continuous monitoring of cloud security ought to be standardized. Independent, professional third-party audit of cloud providers should become standard practice, along with real-time transparency in the security posture of cloud-based systems.

Conclusion

In conclusion, as the use of cloud computing accelerates, better security must go hand-in-hand with saving money and improving performance. Cybersecurity must be integrated into cloud computing architectures at the outset, rather than be left to “catch up.” This will enhance trust in the information revolution that underlies so much of America’s prosperity and homeland security.

I welcome your questions and comments. Thank you.