



**Testimony of Tim Brown  
Senior Vice President and Chief Architect for Security  
CA Technologies**

**Before the Subcommittee on Cybersecurity, Infrastructure Protection,  
and Security Technologies  
House Committee on Homeland Security**

**Hearing on  
"Cloud Computing: What Are the Security Implications?"  
October 6, 2011**

Good morning Chairman Lungren, Ranking Member Clarke, and members of the Subcommittee. My name is Tim Brown, and I'm honored to be here today to testify on cloud computing security risks and opportunities. I am the Senior Vice President and Chief Architect for Security at CA Technologies. CA Technologies ([www.ca.com](http://www.ca.com)) is one of the world's largest information technology management software providers. The company has expertise across IT environments—from the mainframe and distributed computing to virtual and cloud technologies. CA Technologies manages and secures IT environments and enables customers to deliver more flexible IT services. The majority of the global Fortune 500 and most major federal and state government agencies rely extensively on CA Technologies software to manage their constantly evolving technology environments. Founded in 1976, CA Technologies is a global company with headquarters in New York, 150 offices in more than 47 countries, and thousands of developers and researchers worldwide.

CA Technologies was honored to serve on the TechAmerica Foundation's Commission on the Leadership Opportunity in U.S. Deployment of the Cloud (CLOUD<sup>2</sup>), and was heavily involved in the development of the Commission's recommendations. Since another member of the Commission is participating in the hearing today, I will focus the bulk of my remarks on a number of specific cloud security issues CA Technologies believes are critical to ensure secure adoption of cloud computing. However, CA Technologies supports the recommendations of the CLOUD<sup>2</sup> report and I address many of the issues covered in the Commission's report in my testimony today.

CA Technologies believes that cloud computing is neither inherently more nor less secure than other IT platforms, and that securing the cloud is a shared responsibility of both providers and consumers of cloud services. There are a number of policy issues that must be resolved to realize the cloud's potential and we will focus on those issues on our testimony today.

## **Introduction**

While both the hype and promise surrounding cloud computing continue to accelerate at a feverish rate, it is clear that significant confusion remains in global markets about what exactly cloud computing is and what the risks and benefits are associated with transitioning to this latest technology. Corporate and governmental organizations across the globe are anxious to reap the cost, performance and agility benefits that the cloud can offer, but at the same time are wary of a range of risks that accompany a different way of buying and consuming technology solutions.

Chief among concerns raised in survey after survey of both current and potential cloud customers is security. Security is often followed by related concerns about data privacy as well as interoperability, availability of cloud services, performance, and transparency of providers. When one considers the loss of direct control that accompanies cloud deployments, concerns about security risks associated with moving to the cloud are not only reasonable, but also expose critical operational risk management issues that must be discussed and addressed when determining if and when to move particular services to the cloud.

It is important to keep in mind that from a security professional's perspective, any service that runs outside of the operationally controlled environment of an IT organization is considered a cloud service. This is true in the case of commonly known cloud services like Salesforce.com, Google Docs, and cloud email, but also includes services like ADP, 401(k) programs, corporate travel sites, and health plans. No two applications or systems are alike, and pragmatic implementation of cloud technologies necessitates that risk-based processes be used to determine what services and applications may or may not be feasible to move to the cloud, their level of sensitivity, what platform is most suitable, whether a private or public cloud environment is appropriate, and the specific security and operational controls that are needed.

The use of cloud computing represents an exciting new opportunity for IT organizations and for CIO's in both business and government to remake the way in which they work together with their customers and the user communities that rely on IT-based services. Because cloud computing enables IT organizations to focus on business services rather than infrastructure, technology organizations will have increased agility to build new solutions to support their customers with minimal investment.

In my testimony today, I would like to focus on the four key areas that CA Technologies feels must be considered in evaluating both the opportunities and risks associated with the transition to cloud:

- The reality of new complexities introduced with the adoption of cloud computing;
- Security considerations for the cloud;
- The critical role that identity management and authentication play in enabling cloud security; and
- The importance of standards development and adoption to ensure interoperability and common implementation of cloud solutions globally.

I will also make some recommendations on the role Congress can play in fostering the secure uptake and adoption of cloud computing solutions.

### **The "New Normal" of Cloud Computing**

A theme that CA Technologies keeps hearing from our customers is that they want to use cloud computing as a real game-changer. The layers and layers of complexity in IT have made it increasingly more challenging to deliver new services to the business in a rapid manner. The global downturn in markets across the globe has resulted in flat and/or declining IT budgets in both the commercial and public sectors. But the demand for new technology-based services inside large organizations has not slowed, so IT organizations are constantly challenged to provide more business technologies faster with reduced resources.

These factors have all contributed to the perfect storm that has emerged for cloud uptake across the globe.

It is important to note that while many would have you believe that cloud technologies will replace all on premise IT, in reality the transition to cloud technologies will be gradual and the need to develop and support on premise solutions will remain for the foreseeable future. The introduction of cloud technologies will create greater complexities for IT organizations to manage and support. With cloud solutions, a single business service may include a combination of physical, virtual, and cloud components that all must work together to deliver the functionality that users expect.

Consumers of cloud technologies will find themselves in a hybrid technology environment for a long time. Existing solutions and technologies will still need to be maintained, and cloud technologies will most often serve as a natural extension of existing IT environments. As such, the cloud introduce a new heterogeneity to IT environments, one that will require coordinated and orchestrated management, transition plans, and risk-based security evaluations.

This can be a real boon to IT organizations that can harness the enthusiasm and momentum of the cloud to drive changes that have been needed in the management process for technology generally. One of the most promising aspects of cloud computing is its ability to fill the gap between technology supply and demand and help organizations focus less on commodity IT services and more on what is unique to their particular business or government program. Offloading standard services and functions to the cloud can save money and resources that can be better utilized to drive change and tackle problems that are more foundational and transformative to businesses and governments. At CA Technologies, we call this opportunity the innovation dividend.

To gain this dividend, however, IT organizations must take a very focused and methodical approach to evaluating what should or should not be moved to the cloud. This means that organizations need to evaluate people, processes, technology, and perhaps most importantly, risk involved with each potential opportunity move to the cloud. Organizations may determine that certain services, applications and data are too critical or sensitive to be moved to the cloud, which can be an appropriate risk management decision. The cloud is not a panacea, and may not be appropriate for all workloads. Organizations must take a measured approach that is driven by substantive analysis of the risks and opportunities associated with each opportunity to migrate services to the cloud.

Once decisions have been made to move a particular service or application to the cloud, organizations must evaluate what providers and what services will meet their needs. All of these analyses have impacts on and contribute to the security posture of the organization. Some of the considerations that CA Technologies advises our customers to use in evaluating providers include the following, which have been developed through the Cloud Service Measurement Initiative Consortium (CSMIC) that I provide additional details on later in my testimony:

- **Accountability:** can we count on the provider to deliver the promised service?
- **Agility:** can the service be changed, and how quickly?
- **Assurance:** how likely is it that the service will work as expected?
- **Cost:** how much is it, including both start-up and on-going costs?

- **Performance:** does the service do what we need?
- **Usability:** Is it easy to learn and use?
- **Portability:** Can I move my data and application from one provider to another?
- **Security and Privacy:** is the service safe and privacy protected?

## Security Issues in the Cloud

Just like when you buy a car, an appliance, or any other service, the reputation of cloud providers and their ability to deliver on the service promised is a key consideration when making a purchase of cloud solutions. The Cloud Service Provider ecosystem is just as diverse as any other industry. Responsible providers want to do all they can to demonstrate trust and accountability to their customers and that security services are built in and not bolted on to their solutions. These providers will be in the cloud marketplace for the long-run and will continue to drive innovation and excellence in the industry. But it is important to keep in mind that new and innovative cloud service providers are emerging daily. We are in the midst of a significant expansion period in the cloud market, and the ever expanding number of providers who want to move into the cloud market may not have long-term interest or commitment to the technology, which in turn may create risks for customers who want to embrace the cloud. Customers must have assurance their provider of choice will be there when they need service modifications or need to move their data and applications elsewhere, and that they take the responsibility of securing their data as seriously as they do as the owner of that data.

The Cloud Security Alliance (CSA), a major industry consortium focused on cloud security issues, has identified 14 critical focus areas for organizations deploying cloud computing resources<sup>1</sup>. A CA Technologies/Ponemon Institute survey of the cloud service provider community made use of these 14 areas in a report released earlier this year. The survey data uncovered a wide range of viewpoints on the role that cloud service providers have in providing security for their solutions. With lower costs and faster deployment being the main drivers for moving to cloud services, some providers feel that security is more the responsibility of cloud customers than it is of providers.

In reality, not all cloud services require the same level of security. It will be appropriate for certain workloads to be deployed in the cloud with different security levels than others. But the goal of cost savings that is so often identified as the main driver for cloud adoption sometimes masks the importance of security risk management. Security must remain at the forefront of all cloud strategy discussions to ensure the right sets of security controls are applied to the right services. What is important is that security, performance, cost, and accountability decisions are clear and transparent to the users of cloud services.

CA Technologies believes that the responsibility for securing the cloud lies with both the providers and the consumers of cloud solutions. The cloud is neither inherently more nor less secure than other IT services and solutions. Generalized concerns over cloud security on the one hand, and arguments that the security risks in the cloud are overblown on the other hand, have muddied the waters to the point that policymakers and practitioners are

---

<sup>1</sup> The 14 focus areas identified by the Cloud Security Alliance are the following: Governance and enterprise risk management; legal and contracting issues; procedures for electronic discovery; compliance and audit; information lifecycle management; portability and interoperability; business continuity and disaster recovery; data center operations; incident response, notification and remediation; application security; encryption and key management; identity and access management; storage operations; and virtualization operations.

experiencing security schizophrenia. Should I overlook legitimate security concerns and plunge headfirst into the cloud, or should fear and uncertainty of these risks stop me from doing anything that even remotely resembles cloud computing? Like most responsible decisions, the answer lies somewhere in the middle of these two extremes.

Cyber criminals, state and non-state actors, and other cyber adversaries move rapidly and adeptly to exploit weaknesses and vulnerabilities in systems, networks, applications, and practices. They are successful at taking control of machines and stealing data. But done right, the movement to the cloud is an opportunity for organizations to enhance operational security.

As such, potential consumers of cloud solutions must be mindful of the wide range of providers and the security risk management controls they have implemented for the solutions they host or provide in the cloud. A key for cloud customers will be to evaluate both the sensitivities of the services and data they hope to deploy to the cloud, and a vendor's security practices, long-term viability, references, and the depth of their solutions.

Cloud customers must insist on built-in security and transparency from the providers they select. They need to create compliance plans and closely scrutinize their contracts, Service Level Agreements (SLAs), and the security and disaster recovery plans of their providers to ensure they are making sound choices on who to partner with in moving services to the cloud. A key consideration here is to trust, but verify. CA Technologies recommends that cloud customers meet their responsibility to audit and monitor their providers, including the use of inspection programs, testing and monitoring compliance with SLAs, and assessing the security of critical systems.

### **Identity and Access Management as a Foundation of Cloud Security**

While there are certainly myriad operational issues to consider when architecting cloud solutions to deliver strong and robust security, CA Technologies believes that identity and access management (IAM) issues deserve particular attention. Our surveys of cloud providers and the views from leading industry analysts and organizations find that identity and access management is the most important issue that companies considering moving to the cloud face today. A strong trusted identity system that enables the right people to have the right access to the right information is critical to the protection and enablement of the cloud.

Cloud service providers and customers generally feel comfortable that they have highly qualified IT personnel and tools which can prevent or curtail viruses from infecting their services, and that they can effectively secure data flowing in and out of cloud services. They are less comfortable with the process of identifying and authenticating the users, systems, and devices that need access to their services and managing access to specific information or data when using cloud services.

One of the greatest challenges facing the IT sector today is fostering online trust, including the important trust components of security and privacy. The fact is that most online threats and successful data breaches of late have been based on and exploit access control and identity management failures in systems. The Government Accountability Office has written to Congress about unauthorized access issues as recently as Monday of this week (October 3, 2011). Identity management and access management controls are central to the secure

adoption of cloud services. Identity and access management practices within the cloud provide the foundation for effective security by ensuring that all users have only the appropriate level of access rights to protected resources, and that those rights are effectively enforced. IT organizations generally as well as cloud service providers, both public and private, struggle to keep up with the explosion in the number of users from multiple systems, applications and user communities that are consuming their services and the complexity of managing access rights for these users.

With the transition to cloud solutions, employees and applications will continue to move outside the walls of the customer enterprise. This introduces new risks for unauthorized access and the loss of information. Cloud applications are new services that users must have access to, and managing that access without creating new vulnerabilities or new silos of identity are incredibly daunting challenges. Managing the on-boarding and off-boarding of users to cloud services and integrating those access rights with the overall IAM strategy for on premise solutions requires that cloud providers and customers answer the following questions:

- Who has and needs access to what?
- What can they do with that access?
- What can they do with the information they obtain?
- What did they do with that information?

These questions reinforce that managing access and authorization is but one part of the challenge. To be successful, identity security strategies must also focus on the specific data being accessed and what individual users can do with it. CA Technologies refers to this process and approach as content-aware identity and access management

Cloud computing creates opportunities for government agencies and commercial organizations alike to make certain that new silos of identity don't emerge that increase vulnerabilities and complexities for users. For government programs and systems, we recommend that federal agencies enhance their IAM capabilities to provide for risk-based authentication, the use of multi-factor authentication solutions, and leverage the investments they have already made in Personal Identity Verification (PIV) cards.

An example of how many of these integrated identity controls are used today can be found in the financial services sector. CA Technologies counts the majority of the world's major financial services organizations as customers, and we have worked closely with these organizations to implement strong and flexible IAM solutions that provide their customers with ease of use in the most secure fashion possible. Financial services firms have taken a security first approach because of the economic risks of the transactions they conduct. Enhancing the security of those transactions helps meet regulatory requirements, but first and foremost focuses on providing Defense in Depth in ways that enhance security and provide ease of use for consumers that include IAM solutions as a core component. Financial institutions are doing a great job of analyzing not only the risk of individuals and their access rights, but also the unique risks of individual transactions. This is a trend that we believe the overall cloud security market must and will embrace.

Most of us are already comfortable with the concept of signing on to the website of our bank to access our account information. This usually requires that users provide an account number, username, and password. If you want to move money around from one bank account to another at the same financial institution, the bank may require you to provide a

secondary identifier, like a PIN, because that transaction involves more risk. If you want to use your bank's bill pay service and authorize the movement of money from your bank to your credit card company or your local utility, the transaction becomes more complicated and introduces additional risk to both parties involved.

In many cases, when you initiate a transaction like this from your bank, the experience to the user will be seamless. But behind the scenes a complex transaction whereby the user is redirected to a billpay website and has their identity credentials passed to the billpay provider without needing to sign on or provide their credentials again has taken place securely and transparently. The identity authentication taking place in this scenario is being accomplished via a cloud service. This type of transaction is an illustration of how user experience and sound security can be implemented across the very diverse technology environments present today. We believe that this represents the direction future secure transactions across public, private and hybrid cloud environments will progress.

### **The Role and Need for Standards in Fostering Cloud Security**

I believe this example also highlights the importance of standards development and the valuable contributions of industry-led, recognized standards development organizations (SDOs) and consortia. The adoption of standards and their integration into the innovative security solutions offered by the vendor community make possible predictable, interoperable, secure implementations in enterprise and cloud-based services. Such standards are vital to the management of cloud security risks. As I noted earlier, existing security technologies implemented in the enterprise are the building blocks of cloud security. And to a huge extent those technologies, and the practices and controls which they support, are standards based.

Such building block standards are now foundational for cloud computing environments, and where gaps exist, new standards are under development. CA Technologies and other major IT companies contribute actively to these efforts. For example, the Organization for the Advancement of Structured Information Standards (OASIS) has developed important security standards such as Extensible Access Control Markup Language (XACML), Security Assertion Markup Language (SAML), and Web services security standards such as WS-Trust. OASIS also has technical committees in place addressing new security challenges applicable to the cloud, such as cloud identity, identity trust elevation, privacy management and reputation management. Its committees are also working to create profiles which are used to apply existing standards such as XACML directly in support of cloud computing requirements.

Other standards bodies, including the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C), *de jure* bodies such as the International Organization for Standardization/International Electrotechnical Commission Joint Technical Committee 1 (ISO/IEC JTC 1), key industry consortia such as the Open Identity Exchange and the Kantara Initiative and other standards organizations are all key contributors to enabling trust in the cloud. In combination with best practices organizations such as the Cloud Security Alliance, the resources contributed by industry, academia, governments and independent technical experts together represents a huge and ongoing investment to support security risk management in the cloud environment. I would like to note the important role that the National Institute for Standards and Technology (NIST) plays by its active participation in industry standards development and as a convener of industry efforts and focus. NIST recently issued a Special Publication 500-291, the Cloud Computing

Standards Roadmap, which examines the applicability of standards for the cloud and areas where gaps need to be filled.

The NIST publication looks well beyond security alone, and SDOs and consortia have certainly recognized the importance of standards-based cloud interoperability at the data level, and through the development of relevant application, operational management, license management, audit, virtualization, and other standards that are needed to enable interoperability of applications and services across clouds. CA Technologies is a major participant and leader at many levels of the cloud standardization process. And we believe that all of these categories of standardization, and more, are relevant to the development of interoperable clouds and cloud computing trust.

There are several specific efforts I want to highlight as examples of emerging standards in the cloud security arena. The first and perhaps most important in the federal space is the Federal Risk and Authorization Management Program (FedRAMP). While still in its draft form, FedRAMP will provide federal agencies with a baseline, common approach for assessing and authorizing cloud services for use in federal agencies. This will provide federal agencies with a common set of controls against which to evaluate cloud services, and will give cloud providers certainty of federal specifications that must be built into their products. FedRAMP is built on the premise that solutions should be certified once and used many times across federal agencies. Federal agencies, however, have shown a tendency historically to ignore previous certifications and re-certify technologies for use in their own departments based on special requirements. Reciprocity of authorizations will be a critical gauge of the success of FedRAMP.

FedRAMP will also require the transmittal of more frequent operational security information by providers to the government, a process that is most often termed "continuous monitoring." Continuous monitoring offers the potential to dramatically improve the situational security posture of federal information systems that rely on the cloud if implemented correctly.

While we await the final draft of the FedRAMP specifications, several questions about its scope and implementation remain, however. Will agencies be required to honor authorizations made by other agencies and avoid re-evaluating solutions that are implemented similarly at another agency? How often and how will the security data envisioned under continuous monitoring be transmitted? How will the government evaluate this data once received? The answers to these and other questions will be critical to ensuring FedRAMP is both implemented correctly and receives the buy in needed from government and the private sector to ensure its success.

A second area I feel is important is the need to develop common service measurement frameworks to help enable data-driven decisions on the relative effectiveness of cloud solutions based on variables like cost, availability, security, and scalability. Right now, there is no standard mechanism to evaluate common services from different providers against one other. The Cloud Service Measurement Initiative Consortium (CSMIC), under the direction of Carnegie Mellon University and with participation from government agencies like the State of Colorado Office of the CIO, and corporations like CA Technologies and Accenture, has begun developing a service measurement index (SMI), which can be used to measure and compare a business service using a common language and evaluation process. A high level representation of the characteristics and questions the CSMIC seeks to address is included as an attachment to my testimony today. In conjunction with standard

recognition of cloud services authorized under the FedRAMP program, the use of a framework like SMI in government procurements will enhance the analysis of competing cloud services and lead to greater standardization of solutions. As such, CA Technologies encourages the U.S. government to investigate using the SMI to encourage data-driven decision-making on cloud acquisitions.

Thirdly, in the area of identity and access management, the National Strategy for Trusted Identities in Cyberspace (NSTIC) is a critical initiative that will make it easier for citizens and consumers to securely and confidently navigate cyberspace and will enhance trust among different consumers of identity through the sharing and reciprocation of identity credentials. NSTIC is aimed at enhancing online trust by strengthening industry-based identity management practices and minimizing the constant proliferation of username and password combinations that individuals must remember to conduct business on-line. The standards and governance rules that will be developed under NSTIC are a critical component of implementing robust IAM solutions that can enhance trust of and the use of cloud computing services. As the NSTIC program gets up and running at the Department of Commerce, CA Technologies recommends that Congress fully fund this important effort and that federal agencies become active participants in both the development of the NSTIC standards, and ultimately, accept private-sector issued credentials as a means of authentication for citizens who wish to interact with government agencies securely.

Standards development, then, is an ongoing and vital area of industry and governmental focus. It is international in scope, and the standards are integral to key government initiatives such as FedRAMP and NSTIC. It is important that the subcommittee recognize that it is only through support for industry-led, internationally supported standards will we have measurable, interoperable security risk management technologies, innovative technical solutions and practices that can ensure trust in cloud-based services, not only in the U.S., but globally.

### **Recommendations for Congress**

I was asked to address some of the security risks and opportunities associated with the transition to cloud computing. I hope that my testimony has highlighted that while there certainly are risks, the opportunities are extremely positive if a number of actions are carried out to ensure that the adoption of cloud technologies does not create new silos in IT security and new, unintended risks. We are in the nascent stage of cloud adoption. To ensure the promises of cloud computing can be delivered in concert with effective security risk management, we recommend that Congress:

- Adopt policies that can accommodate future development and flexibility in the cloud market, specifically, and in IT more generally. Too often, federal policy has imposed static frameworks that must constantly be updated based on new technology developments. We recommend that Congress focus on outcomes and not on specific technologies;
- Avoid policies that create a fragmented, country specific market for cloud services in the United States. As the cloud market continues to evolve, we see great risk for market segmentation based on unique policies designed solely to address US or other countries' market demands. For U.S.-based businesses seeking to compete in markets all over the world, globally harmonized policies will enable industry to build solutions that can be delivered in multiple markets enhances our competitiveness and makes it easier to deliver innovative solutions around the world. Policies that

acknowledge the global nature of cloud markets will enable the US to maintain its leadership position in cloud computing and encourage innovation to support jobs and exports of US developed technologies;

- Support standards developed by recognized standards development organizations in the areas of cloud security, interoperability, and transparency. These standards are vital to the management of cloud security risks and should be embraced by Congressional and Executive Branch policy makers;
- Fund and support the continued development and rollout of FedRAMP and the NSTIC. To enhance operational cybersecurity at the federal level, we recommend that Congress ensure that critical funding to develop and implement these programs be preserved, even in difficult federal budget environments. We further recommend that Congress keep a watchful eye on FedRAMP implementation to ensure that the efficiencies hoped for are achieved;
- Continue support for NIST and its unique role as both an internationally-respected body of security experts developing standards and practices for the Federal government as well as for its important function as a contributor to industry-led standards development and as a convener for addressing emerging security issues; and
- Encourage the federal government to leverage emerging efforts to develop service measurement indexes in government cloud procurements. The CSMIC effort I described in my testimony can provide federal agencies facing budget, performance, and transparency demands with tools that take data-driven approaches to evaluating competing offers of cloud technologies. I believe that frameworks like these can facilitate more robust decision-making about which specific cloud services and providers are right for federal agencies.

\* \* \* \*

Mr. Chairman, Ranking Member Clarke and members of the subcommittee, this concludes my written statement. I appreciate the opportunity to appear before you to share some of our thoughts on cloud security. CA Technologies shares the subcommittee's goal of increasing awareness of the cloud and the particular goal of enhancing cybersecurity, and we would be happy to work with you towards this goal however we can.

I would be happy to answer any questions you may have for me.

Thank you.



## **Timothy Brown Biography**

**Timothy G. Brown** is the Senior Vice President, Distinguished Engineer, and Chief Security Architect for CA Technologies. He has overall technical direction and oversight responsibilities for the CA security products. This includes solutions to control users, their access and how they use information across physical, virtual and cloud environments. With more than 20 years of information security expertise, Brown has been involved in many areas of security including identity and access management, security compliance, threat research, vulnerability management, encryption and managed security services.

Brown has worked with many companies and government agencies to implement sound and practical security policies and solutions. He is on the board of the [Open Identity Exchange](#), and has provided expert testimony at a U.S. Congressional hearing entitled "Cyber Security R&D." He also is a frequent speaker on the evolution of security and cloud computing.

Prior to joining CA Technologies, he spent 12 years at Symantec where in the CTO office he was responsible for companywide technical architecture, integration, gap analysis and technical strategy.

Brown also works with a number of universities and governments doing advanced research in security and insider threat. He is an avid inventor with over 20 filed patents. He is active in promoting cross-industry initiatives and has participated on a number of standards boards.