THE STAND
Cloud Computing

Q&A with Industry Leaders

Government is moving toward the cloud for at least some of its computing requirements, that's clear, but what's not so obvious is the when, what and how of this transition. Confusion is still the overriding state for most agencies.

THE STAND: Cloud Computing cuts through this fog with the views of three experienced veterans of the field, who explain what planning is needed for a cloud deployment, what's needed in choosing which applications to move to the cloud, and the trade-offs that have to be considered.

Full report available at: www.fcw.com/TheSTANDCloudComputing

THE STAND Cloud Computing

Question 1

How would you describe the state of awareness federal agencies have about computing today?

GiGi Schumm, Vice President and General Manager, Public Sector, Symantec Corp.

GiGi Schumm
Symantec Corp.

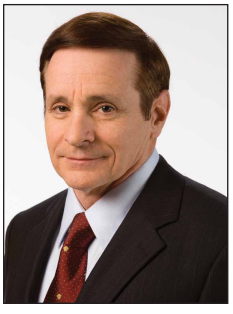
A: Awareness overall is quite high, and a survey we took at a recent government symposium reflected that. Of the more than 1,100 participants, our sample indicates that 15 percent said they had no plans to implement cloud applications, platforms or infrastructure. However, as you drill down into areas below that overall awareness into what's needed to have a successful cloud implementation, or what applications are more appropriate to move to the cloud, at that level of detail I think there's a lot more confusion and uncertainty.

Tom Ruff, Vice President, Public Sector, Akamai Technologies, Inc.

Tom Ruff
Akamai Technologies, Inc.

A: I believe the government has done a remarkable job in creating overall awareness around the cloud, and certainly about the advantages that it can bring to the federal market. Since Federal Chief Information Officer Vivek Kundra's announcement last fall regarding cloud computing, there have been a multitude of initiatives to create awareness about the cloud. Specifically, there has been a strong push to define the cloud, as well as highlighting its advantages and how to maximize ROI for cloud initiatives.

The level of awareness about cloud computing differs from agency to agency, but overall I think federal agencies are further along than the private sector, given the government's proactive stance on the subject.



Richard W. Johnson, Chief Technology Officer and Vice President, Lockheed Martin Information Systems & Global Solutions

Richard W. Johnson
Lockheed Martin Information Systems & Global Solutions

A: While there may be a general understanding of cloud computing in government, a recent survey we conducted with Government IT leaders in collaboration with our Lockheed Martin Cyber Security Alliance partners revealed that awareness, trust and security were lacking. There's certainly a very generalized sense that the cloud is important and that it could reduce costs, but there's not a lot of understanding about the myths associated with cloud computing, risks and avoidance risks, upfront costs in moving to the cloud, and so on.

I think at least part of the reason is that there are many different deployment and service models associated with the cloud, and many different combinations. So, it's very difficult to establish a common baseline within government agencies regarding cloud computing and its deployment.

THE STAND Cloud Computing

Question 2

What are the most significant problems federal agencies must solve today and how can cloud computing be part of the solution?

GiGi Schumm,
Vice President and General Manager, Public Sector,
Symantec Corp.

GiGi Schumm
Symantec Corp.

A: There are three: information risk, information growth, and information trust.

The risk environment has changed so much in the past few years, with nation states, organized crime and malicious attackers targeting organizations in unprecedented ways in order to steal valuable information. It's no longer about someone who just wants to disrupt your systems, or teenage hackers looking for notoriety.

Information is growing anywhere from 40 percent to 80 percent a year, according to what we are hearing. How do you deal with the costs of storing, managing and protecting that information? This is an area where we think the cloud can have a strong impact, because as you move away from a systems centric management model to the cloud you can dramatically reduce the amount of information you have to manage and protect. We've seen data reduction rates of around 90 percent to 95 percent with data de-duplication.

Information trust goes beyond just protecting information from malicious outsiders. It's about whether an IT organization has the trust and confidence to not only secure information but also store, discover and retrieve it in that new cloud computing model.

Of the three, information growth is the problem closest to being adopted for cloud solutions.

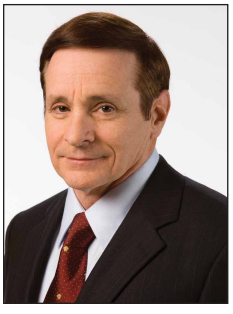
Tom Ruff,
Vice President,
Public Sector,
Akamai Technologies, Inc.

Tom Ruff
Akamai Technologies, Inc.

A: The government has been facing a variety of business challenges, and now they are experiencing significant economic challenges as well. Every agency is faced with cuts, and we'll probably be seeing more. For the first time, agencies are seeing significant cuts, which will impact their current and planned infrastructure expenditures. At the same time, there is an edict for agencies to be more transparent, and to deliver services faster and cheaper. Concurrently, they still have to support both anticipated and unanticipated workloads.

These challenges will make it difficult for agencies to accurately determine the right size of their infrastructures while still meeting security and workload demands.

Based on the right set of applications, cloud computing allows agencies to meet these challenges while at the same time reducing their overall costs.



Richard W. Johnson,
Chief Technology Officer and Vice President,
Lockheed Martin Information Systems & Global Solutions

Richard W. Johnson
Lockheed Martin Information Systems & Global Solutions

A: Agencies must reduce costs, and cloud computing, primarily because of virtualization technology, allows them to provide a more elastic, low cost infrastructure. But agencies also have to be more agile and deliver mission applications to the end user faster. Cloud computing enables a much faster development lifecycle than traditional methods, so they can get those capabilities into the hands of the end user faster, which is where you need them.

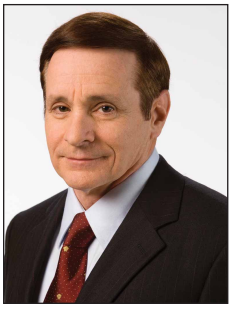
There's also an opportunity for agencies to advance their missions in this. The confluence of virtualization, the ubiquitous capabilities associated with the Internet and the growing use of technology, such as handheld devices, by people in their personal lives, gives the federal government a great chance to provide better services to their constituents. There's a new set of opportunities that didn't exist before these technologies matured.

THE STAND Cloud Computing Question 3

What are the greatest benefits federal agencies can realize by deploying cloud solutions?

GiGi Schumm, Vice President and General Manager, Public Sector, Symantec Corp.

Tom Ruff, Vice President, Public Sector, Akamai Technologies, Inc.



Richard W. Johnson, Chief Technology Officer and Vice President, Lockheed Martin Information Systems & Global Solutions

GiGi Schumm
Symantec Corp.

A: Cost savings, plus improvements in their operational flexibility and transparency are the most obvious right now.

Cost savings is currently the biggest driver for cloud computing, by far. Data center consolidation and the ability to use virtualization, data de-duplication and shared services all represent big opportunities to reduce costs. Flexibility allows agencies to support new initiatives and to scale efforts very quickly, with the recent cash-for-clunkers car buying program a good example of that. And flexibility speaks to government employees and citizens having access to better quality data along with the interoperability of that data, and that's something that the Obama Administration is pushing for.

Tom Ruff
Akamai Technologies, Inc.

A: There are many key benefits for federal agencies to deploy cloud solutions. As one of the hottest concepts in IT today, cloud computing proposes to transform the way IT is consumed and managed, with promises of improved cost efficiencies, accelerated innovation, faster time-to-market, and the ability to scale applications on demand.

With that said, most cloud computing services are accessed over the Internet, and thus fundamentally rely on an inherently unpredictable and insecure medium. Therefore, in order for agencies to realize the full potential of their cloud computing initiatives, they will need to overcome the performance, reliability, and scalability challenges the Internet presents.

Richard W. Johnson
Lockheed Martin Information Systems & Global Solutions

A: Total cost of ownership is obviously the big one. There's also the benefit the cloud provides for green IT, with the reduction in the size of government IT infrastructures. And some of the work we are doing with our partners in the Cloud Security Alliance, and the Lockheed Martin Cyber Security Alliance point to improved data security.

One of the interesting things is that you can only protect what you know you have, and one of the advantages of cloud computing is that you know all of the applications you have, all of the critical systems, and all of the platforms. You know everything that's in your cloud because you are charging for it. And, when you know what you have in your cloud, you have the ability to defend it through a continuous process that's much easier and, at the end of the day, provides for a much more effective security posture.

THE STAND Cloud Computing

Question 4

Can you offer metrics by which an agency can calculate the ROI?

GiGi Schumm, Vice President and General Manager, Public Sector, Symantec Corp.

GiGi Schumm
Symantec Corp.

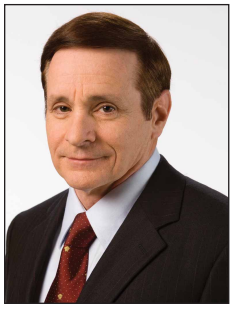
A: There's a certain set of metrics around such things as hardware and software licensing costs, power and energy costs and operations costs that we would expect agencies to consider to see what cost savings they would make by going to the cloud. Then they need to look deeper into the data center to see what the current utilization rates are for servers and storage and how those might be affected.

Soft costs such as flexibility need to be considered also. Because you don't know what the future will bring, you need to look into the future and gauge what requirements will be three to five years out. But if you guess high you'll spend too much money, and if you guess low you won't have the scalability and you'll have to retrofit for that later. The cloud provides elasticity and flexibility that won't necessarily be there if agencies build it themselves.

Tom Ruff, Vice President, Public Sector, Akamai Technologies, Inc.

Tom Ruff
Akamai Technologies, Inc.

A: ROI calculations are easy for measuring such things as IT resource savings, bandwidth consumption and administrative overhead. These are quantifiable costs that can be classified and therefore calculated using various tools currently in the market. However, it's a different matter when you try to calculate for qualitative measurements such as the loss of an agency's brand or citizens' trust when a capability becomes unavailable. For example, when the FBI or Department of Homeland Security websites go down and are unavailable to field agents or citizens during a crisis. It is critical for agencies to evaluate what those subjective costs are, and to ensure services are in place that minimize such risks. With that said, ROI is just one measurement that agencies need to consider. First and foremost agency's must determine if cloud computing can help them complete their mission in a timely and economical fashion. Nothing is going to replace the mission; that is job number one.



Richard W. Johnson, Chief Technology Officer and Vice President, Lockheed Martin Information Systems & Global Solutions

Richard W. Johnson
Lockheed Martin Information Systems & Global Solutions

A: It's largely a matter of the difference between the costs today, and the cost in going to a cloud environment.

And while that seems logical, one of the issues not considered often is the cost associated in transitioning from your current environment to a cloud environment. Even if I put my current email system in a public cloud, I still have to transition the data, and decide how to manage attachments, whether I'm going to have a help desk and so on. What cost impact will that have? And then you must consider security.

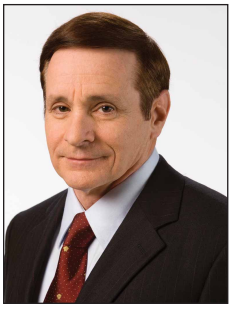
But there's also hidden value when we take a full lifecycle approach, that not only factors in the in the cost of the startup and the cost of the transition, but also takes into account the value of faster development times. With the cloud you can develop applications faster, so you have to determine the ROI if I can deliver a cloud application in six weeks versus six months or six years? What's the value to my end customers in having that improved service?

THE STAND Cloud Computing Question 5

How do you see cloud computing evolving in the federal government over the next year-18 months? Two-to-five years?

GiGi Schumm, Vice President and General Manager, Public Sector, Symantec Corp.

Tom Ruff, Vice President, Public Sector, Akamai Technologies, Inc.



Richard W. Johnson, Chief Technology Officer and Vice President, Lockheed Martin Information Systems & Global Solutions

GiGi Schumm
Symantec Corp.

A: Based on what Symantec is delivering now or will be in the next two to three years, demand for end point security and backup as cloud applications seems to be growing.

End point security is a natural for the cloud since, once it's installed, it has to be continually updated with virus and spam definitions and other preventative security features. That makes it a perfect fit for the cloud. And backup is such a good fit because of the cloud's flexibility. Your backup needs may be very different from what they are today, and you have to be able to scale for that.

Other things further off in the future include data loss protection and identity protection. Those are areas where we'll also see an uptick in the kinds of capabilities offered in the cloud.

Tom Ruff
Akamai Technologies, Inc.

A: Cloud adoption will to continue to grow over the next five years, especially as agencies increasingly explore the broad range of cloud services, technologies, and approaches in today's marketplace. The IT industry is putting significant investment not only into cloud technologies and infrastructure but also into application development. For example, there has been heavy investment in the development of applications that allow users to integrate mobile devices into the cloud environment.

Additionally, technologies and application development will increase the utilization and adoption of the cloud.

Richard W. Johnson
Lockheed Martin Information Systems & Global Solutions

A: For the next year to 18 months agencies will be evaluating, experimenting and investigating cloud computing to see how it can help them meet their affordability goals and improve mission capabilities. From two to five years out, we believe cloud computing will become a core element of the overall portfolio of computing options that the government consider for their entire IT environment. More core mission capabilities will be operationalized by cloud computing, and you'll see increasingly more integration between the enterprise and multiple clouds as domain specific capabilities in the cloud become more prevalent.

THE STAND Cloud Computing Question 6

How does your approach differ from that of other vendors in the space?

GiGi Schumm, Vice President and General Manager, Public Sector, Symantec Corp.

GiGi Schumm
Symantec Corp.

A: Some vendors focus on just a piece of the puzzle, whereas Symantec has a broader view. Symantec is a global leader in backup technologies, for example, and for many years our technologies have been used in outsourced or hosted environments. We have many large partners who use our backup technologies for their customers' data, and we have an online backup service that currently has around 9 million customers. We believe we have the largest cloud-based infrastructure that's been built for that application.

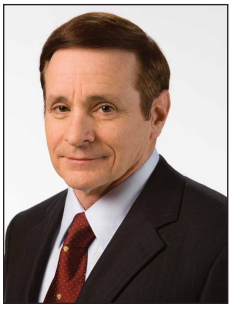
So, we speak from the vantage point of a company who uses cloud services to run its business, that already delivers security and backup services via the cloud. Some 15 percent of our total revenue, or around $1 billion, will be from cloud-based offerings in the next five years. We already have a broad spectrum of cloud-enabling technologies to help agencies to store, manage and backup their data.

Tom Ruff, Vice President, Public Sector, Akamai Technologies, Inc.

Tom Ruff
Akamai Technologies, Inc.

A: Most vendors focus on a specific set of cloud capabilities, such as Software-as-a-Service, (SaaS) Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and X-as-a-Service (XaaS). Akamai provides capabilities in all of these areas, but our true differentiator is that we provide application acceleration services that overlay all of these capabilities which promote end user adoption and drive a better application experience.

We deploy compute power out to the edge of the cloud which eliminates bottlenecks on the Internet. By providing content at the edge closest to the end user's access to the Internet we can offer enormous scale, avoiding common connectivity issues faced by many of our competitors.



Richard W. Johnson, Chief Technology Officer and Vice President, Lockheed Martin Information Systems & Global Solutions

Richard W. Johnson
Lockheed Martin Information Systems & Global Solutions

A: We are an integrator and aggregator, so we don't characterize ourselves as a vendor. We provide technology and create alliances, and in the case of cloud computing we have reached out to some of the top industry vendors and providers of infrastructure and services which allows us to tailor cloud solutions for our customers.

We know our customers need more than a one-size-fits-all solution, and that we have to meet their needs for affordability and security and their mission requirements. And that's what we believe we are the best at, and what separates us from others in the marketplace.

THE STAND Cloud Computing

Question 7

What is your company's unique value proposition in the federal cloud computing space? Why?

GiGi Schumm,
Vice President and General Manager, Public Sector,
Symantec Corp.

GiGi Schumm
Symantec Corp.

A: We bring an in-depth knowledge to federal agency requirements for privacy and security. Some of the things you see in government are unique and that you don't see in the commercial side, such as Common Criteria and FISMA. There are a lot of government standards for such things as data protection and storage and high availability that need to be interpreted for both physical and virtual computer environments. Symantec has solutions that are cross platform and work in all types of environments.

In the government space you see a lot more heterogeneity, because it contains big computer environments that have been built up over many years. You're going to find a little bit of everything, some virtual and some not, some this platform and some that platform. Having technologies that work across an extremely heterogeneous environment is vital. Symantec has solutions that are road-tested and can scale to whatever size the government needs.

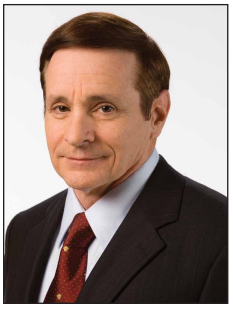
Tom Ruff,
Vice President,
Public Sector,
Akamai Technologies, Inc.

Tom Ruff
Akamai Technologies, Inc.

A: Akamai has the world's largest distributed computing infrastructure platform, and what that does is provide protection to the government's centralized infrastructure from the repercussions of certain anticipated or unanticipated events that drain their existing resources.

In today's rich media, well connected society, it's hard to project workload. In fact it's almost impossible. We can provide agencies with 100 percent availability while also seeing performance improvement worldwide. This is a key differentiator that none of our competitors can legitimately claim.

This worldwide deployment is of importance because agencies are starting to see more and more of their traffic coming from overseas.



Richard W. Johnson,
Chief Technology Officer and Vice President,
Lockheed Martin Information Systems & Global Solutions

Richard W. Johnson
Lockheed Martin Information Systems & Global Solutions

A: We have mission and domain knowledge of our customers across the intelligence, military and civil domains. So we feel we are in a good position to walk in our customers' shoes, and to help them optimize mission and citizen service delivery and performance through the best infrastructure and secure cloud solutions.

We have been for 16 years in a row the number one provider of IT services to the federal government, and we have a deep understanding of technology and how best to integrate technology based upon the needs of the agency to accomplish their mission and deliver citizen services.

Which agencies are the farthest along in the development/deployment of cloud computing and why?

GiGi Schumm,
Vice President and General Manager, Public Sector, Symantec Corp.

GiGi Schumm
Symantec Corp.

A: The Department of Energy has had a project to move some of its applications to the cloud, as has the Department of Health and Human Services around electronic health records. But there will be a lot more. At our symposium, 58 percent of the surveyed agencies attending said they were already making use of the cloud to some extent, though the vast majority were talking about private in-house or outsourced clouds.

That's likely to continue. Over two-thirds of the respondents to our survey said they were looking to implement private in-house clouds versus using public clouds, even when they look at what their longer range plans are.

Which agencies are the farthest along in the development/deployment of cloud computing and why?

Tom Ruff,
Vice President,
Public Sector,
Akamai Technologies, Inc.

Tom Ruff
Akamai Technologies, Inc.

A: I believe the Defense Information Systems Agency (DISA) is one of the most forward leaning agency when it comes to cloud initiatives.

Working with Akamai, DISA has developed a number of cloud computing solutions available to US military, DoD government civilians and DoD contractors.

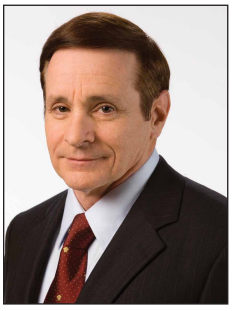
The agency's cloud solutions include: Forge.mil, a system that enables the collaborative development and use of open source and DoD community source software; GIG Content Delivery Service (GCDS), a private cloud deployment of services to over 60 government DOD agencies; and Rapid Access Computing Environment (RACE), a quick-turn solution that uses cloud computing to deliver fast, inexpensive and secure platforms. This service is implemented world wide using Akamai technology behind DISA's firewall.

The General Services Administration (GSA) deploys a secure public cloud offering called USA.gov, which is designed to communicate more effectively with citizens on real-time issues and to foster transparent communications on topics such as benefits, taxes, jobs and healthcare initiatives.

Finally, I'd point to the Census Bureau, which is a classic case for the cloud and how appropriate it is for certain environments. The agency must take on a critical once-in-a-decade mission where it needs to deliver both front end and back end systems to meet the demands of the 2010 Census. The key challenges include the need to deliver on-demand scalability, enhanced Web experience for maximum citizen participation, and 100 percent availability, especially because the bureau has a critical timeframe to conduct the Census and report results to the government and to the public.

The bureau implemented an infrastructure-as-a-service (IaaS) cloud to meet on-demand business challenges. In doing so, the agency was able to offload 85 percent of its infrastructure needs, without putting an additional penny into its infrastructure for the support and execution of the short-term mission.

Which agencies are the farthest along in the development/deployment of cloud computing and why?



Richard W. Johnson, Chief Technology Officer and Vice President, Lockheed Martin Information Systems & Global Solutions

Richard W. Johnson
Lockheed Martin Information Systems & Global Solutions

A: There are some private clouds in the government that started out from a shared services environment and, in many cases, they're using components of cloud computing technologies as opposed to a complete cloud. But you've got Data.gov at the General Services Administration, the National Business Center at the Department of Interior, NASA's Nebula, and DISA with the Rapid Access Computing Environment. I think those are among the best examples of agencies that are further along.

And that's primarily because these agencies were already further along than other agencies with respect to their shared services model, and they were already provisioning a series of core missions with that model. To go from a shared services model to a cloud computing model was a natural step for them.

A good example of one that's fairly mature along those lines would be DISA, which had a service oriented architecture infrastructure from which they built services, so it's natural to take that infrastructure and transition that into a cloud on which they could then host applications, and also provide a platform for others to build applications that they could use across the Department of Defense.

How big of a challenge is the development of common security requirements for the federal government?

GiGi Schumm, Vice President and General Manager, Public Sector, Symantec Corp.

GiGi Schumm
Symantec Corp.

A: Fully 90 percent of those who answered our survey said they needed clear guidance about government cloud security standards. Efforts such as FedRAMP that federal chief information officer Vivek Kundra is launching with the National Institute of Standards and Technology will help to flesh out a lot of those issues and provide answers, but we're in the very early stages and there'll be a learning curve that everyone will have to go through.

We think the questions that need to be answered are, first, what kind of information will be in the cloud and what kind and size of datasets are involved? That will drive decisions about what kind of applications make the most sense to put in the cloud. And then how are you going to define trust relationships in the cloud and handle authentication, validation and the understanding of what security controls to put around the data?

A third question where we believe government customers need more guidance is how to extend compliance around some of the key regulations such as FISMA to information in the cloud. And, lastly, how will a cloud strategy affect an agency's continuity of operations. What level of high availability, disaster recovery and storage management will the cloud vendor provide?

How big of a challenge is the development of common security requirements for the federal government?

Tom Ruff,
Vice President,
Public Sector,
Akamai Technologies, Inc.

Tom Ruff
Akamai Technologies, Inc.

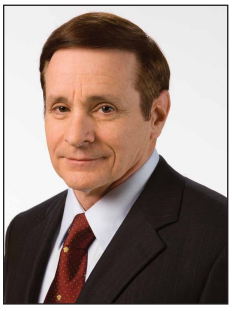
A: The government, and in many respects, the public sector overall, has an advantage over the commercial marketplace when it comes to the development of common security requirements.

The government took a big step towards this development with the enactment of the Federal Information Security Management Act (FISMA), which requires each federal agency to develop, document, and implement an agency-wide program to provide information security.

While some agencies might interpret the guidelines slightly differently given their security posture, FISMA ensures there is a minimum baseline set of recommended guidelines.

When it comes to security in government FISMA is table stakes; agencies should not work with providers that do not meet FISMA guidelines. Moreover, agencies should work with providers that not only meet FISMA requirements but that also offer an enhanced array of offerings that meet their security strategy around cloud computing.

How big of a challenge is the development of common security requirements for the federal government?



Richard W. Johnson, Chief Technology Officer and Vice President, Lockheed Martin Information Systems & Global Solutions

Richard W. Johnson
Lockheed Martin Information Systems & Global Solutions

A: I think probably the biggest challenge they have in cloud computing, besides identity and access management, is data. How do you secure the data, because it's all about the data. And you really need to take a lifecycle management approach to the security of the data, from its actual creation to storage to maintenance to its backup to recovery, and then to its eventual destruction. And then how do you know if your data is completely protected so it can't be accessed by those who don't have the right permissions and that it's secure through its total lifecycle.

That's one of the biggest challenges, and it's one of the areas that the Cloud Security Alliance is focused on. The same risk management process and responsibilities that federal agencies have today for their enterprise is extended to the cloud. We currently wrestle with risk management associated with data in the enterprise, but that becomes compounded when you put it into the public cloud. Because he who has control of data can set the terms and conditions.

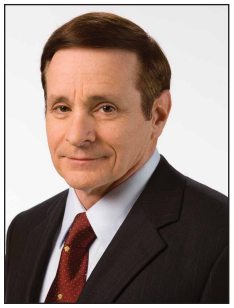
So that is a focus for consideration in placing data in the public cloud or in a private cloud where you can control your own data. And that's one of the issues you've got to wrestle with when you're deciding whether to go to a cloud.

THE STAND Cloud Computing Question 10

How powerful can cloud-enabled collaboration be for federal agencies?

GiGi Schumm, Vice President and General Manager, Public Sector, Symantec Corp.

Tom Ruff, Vice President, Public Sector, Akamai Technologies, Inc.



Richard W. Johnson, Chief Technology Officer and Vice President, Lockheed Martin Information Systems & Global Solutions

GiGi Schumm
Symantec Corp.

A: It provides tremendous opportunity for the public sector to deliver services for the people, reduce the cost of government operations and make more effective use of taxpayer dollars. It's really a very nascent area and still at the very early stage, but it's one where we do see promise. There's just not a ton of examples yet.

Cash-for-clunkers was one early example. That was a collaboration between the public and private sectors, it was cloud-based and consumers could get online and find information about the program and what cars were available and what dealerships had them.

Tom Ruff
Akamai Technologies, Inc.

A: When government agencies collaborate with each other or with citizens they can accomplish things that they couldn't otherwise do individually. The cloud really fosters a unique environment that allows individuals and teams to solve problems faster and with a greater degree of accuracy. Whether it's a team of subject matter experts addressing the Gulf oil spill or a group of citizens providing feedback on a government initiative, government is key.

Organizations can get a real-time response through a distributed collaboration solution which will be more effective than putting people on planes or having conference calls. This allows experts around the world to participate in the session, provide their expert and to collaborate together. I don't know how else you could achieve a more powerful problem-solving capability than cloud collaboration.

Richard W. Johnson
Lockheed Martin Information Systems & Global Solutions

A: I think that collaboration is really a cultural challenge, not a technical challenge. The agencies have to be motivated to collaborate and that has been a challenge across federal government. But I do think cloud-enabled collaboration can be focused on some very specific key missions, such as better command and control, better support for the DOD and warfighters, and perhaps better intelligence gathering and dissemination.

The cloud is an enabler. It will help you plan and improve your collaboration with activities such as applications development. When you put the changes in place to overcome those cultural challenges you can generate and deliver applications faster using the cloud.

However, there are some technical challenges with cloud-to-cloud coordination. If you're going to have multiple clouds, there is a technical issue with cloud-to-cloud interoperability. Standards organizations such as the Cloud Security Alliance, are working to address this challenge.

THE STAND Cloud Computing Question 11

How important is it for agencies to integrate their existing workflow, business and security processes into Cloud Computing plans?

GiGi Schumm, Vice President and General Manager, Public Sector, Symantec Corp.

GiGi Schumm
Symantec Corp.

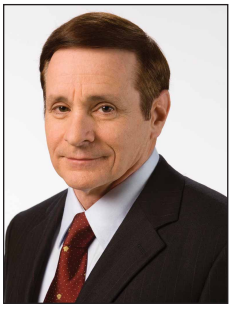
A: It's important to understand them when agencies are creating or contemplating cloud computing plans, but they don't necessarily want to pick them up and move them en masse to the cloud, because that way they could end up paving the cow pass. They'll be moving over business processes and workflows that were created for older technologies and an older computing paradigm, when they might be better served by redesigning them to accommodate the cloud.

Tom Ruff, Vice President, Public Sector, Akamai Technologies, Inc.

Tom Ruff
Akamai Technologies, Inc.

A: Cloud capabilities will become as ubiquitous as email and chat is today, it's just a matter of time. This is a fundamental change and very similar to what we saw with the Internet 15 years ago. We're just at the beginning of this shift, and it's going to be imperative that agencies accommodate this change from enterprise computing (big data centers) to cloud computing. Agencies must convert that understanding into their existing management practices. Agencies will not be able to fully leverage the cloud or mitigate risk unless they introduce management and security practices that support this new paradigm of delivery.

The good news is that agencies have already been modifying their workflow and business processes to accommodate the Internet. Cloud based services will just be an extension of that, making the extension of current processes for cloud computing more evolutionary than revolutionary.



Richard W. Johnson, Chief Technology Officer and Vice President, Lockheed Martin Information Systems & Global Solutions

Richard W. Johnson
Lockheed Martin Information Systems & Global Solutions

A: One thing that's absolutely clear is that cloud computing is not going to be part of a rip-and-replace implementation plan in the federal government. Instead, cloud computing is being integrated into core enterprise environments, which means that integration into existing workflow, business and security processes is an extremely important aspect for agencies and their adoption of cloud computing.

And that's what we are seeing. The key here is that our customers are asking three basic questions that we are trying to help them answer. The first is, what makes sense to move to the cloud? The second is, if it makes sense then what's the best way to achieve this migration to the cloud? Thirdly, if I don't buy anything new from a hardware or software perspective, what is the best way for me to take advantage of the cloud for innovation and mission capability?

Integrating the cloud into their existing enterprise environment means answering those three questions, and making sure they have the ability to do exactly the things they want to in a more flexible, agile, affordable, and secure way. And planning for that happens right at stage one, when they start thinking about what makes sense for them to start moving to the cloud.

Pick one core product you believe is most critical to successful deployment of a federal cloud. Detail the product and explain why it's important?

GiGi Schumm, Vice President and General Manager, Public Sector, Symantec Corp.

GiGi Schumm
Symantec Corp.

A: Well, we cheated a little on this one and chose a product area rather than a single product, focused on data identity and data loss prevention. We have a number of products that all attack this issue of knowing where your data is, who owns it and then making sure it stays where it's supposed to.

We have our Data Insight product, which is all about understanding the ownership and use of data. Then there's our Data Loss Prevention product. And then, more recently, our encryption technologies have become important as a part of the entire spectrum of the data protection and data loss prevention program. And finally, once our acquisition of VeriSign closes, we'll have the final piece in place, which is identity protection.

These aren't cloud technologies in themselves, but we believe they are the most important in enabling agencies to move their current or new applications to the cloud. In the old days of securing the infrastructure people first built a strong perimeter, then made sure the networks were secure, then focused on making sure specific systems were locked down tight. That all turned out to be not enough. With things like virtualization and the cloud the emphasis has to be on where the information is, who should have access to it and ensuring that only those who do can access it.

Pick one core product you believe is most critical to successful deployment of a federal cloud. Detail the product and explain why it's important?

Tom Ruff,
Vice President,
Public Sector,
Akamai Technologies, Inc.

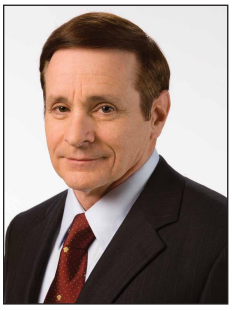
Tom Ruff
Akamai Technologies, Inc.

A: The internet is becoming a critical part of an agency's IT delivery infrastructure. However, the internet historically provided very little QOS (Quality of Service) and controls to ensure a customer could use the internet to deliver mission critical applications and content. Akamai's Dynamic Site Accelerator (DSA) service, built on our cloud platform, gives agencies the performance, reliability, availability and controls they need to leverage the internet for business

How do you get closer to your constituents, partners, and sister agencies? How do you deliver new capabilities quickly, in a transparent, accessible, and secure manner? How do you deploy for scale and availability fast, while only paying for what you actually need, without fielding excess infrastructure? These are problems that the cloud is working to solve for Federal agencies, and this is why Akamai built, deployed, and operates our DSA service. Akamai's DSA cloud service allows agencies to extend their reach across the globe in order to serve end users anywhere in the world, regardless of internet conditions.

Delivering the control they need to manage and distribute information rich content and applications anytime, anyplace. Akamai's DSA Secure service provides federal agencies with an architectural cloud foundation built on solid and proven cloud delivery experience.

Pick one core product you believe is most critical to successful deployment of a federal cloud. Detail the product and explain why it's important?



Richard W. Johnson, Chief Technology Officer and Vice President, Lockheed Martin Information Systems & Global Solutions

Richard W. Johnson
Lockheed Martin Information Systems & Global Solutions

A: If you're able to find one magical product that provides a complete end-to-end secure mission cloud we'll certainly look at it.

Seriously, there are certain technologies that are vital to cloud computing service delivery. The two most important are virtualization and Internet-based communications. Those are the two that really have spurred the cloud. But the reality is that no one product foundationally provides an end-to-end cloud solution. It's an integration of multiple technologies. The core is virtualization and communications.

What are the top 10 things a federal agency needs to do to ensure that a cloud computing project is successful?

GiGi Schumm, Vice President and General Manager, Public Sector, Symantec Corp.

GiGi Schumm
Symantec Corp.

A: Everything involved with cloud centers around trust. Gartner Research says the transformation that's fueling the cloud computing movement is about a shift in the way that IT services are acquired and consumed, and it goes on to say that trust is one of the key enablers. So, what goes into making up that trust? How are federal government customers going to have the trust they need to move applications to the cloud? Underlying all of that is availability and security. So, ensuring things like data privacy, data portability, data ownership and interoperability are all important considerations.

There are some important, non-obvious things that agencies have to be aware of. Data portability is an example. They may have a situation where they want something in the cloud now, but later want it in-house. Or they've got it with one cloud provider now, and down the road they may want to move it to another cloud provider which has a different infrastructure. So data portability is pretty important. I'm not sure agencies are as focused on that. They're thinking about how they get things to the cloud, not necessarily that they're not going to stay there forever.

What are the top 10 things a federal agency needs to do to ensure that a cloud computing project is successful?

Tom Ruff,
Vice President,
Public Sector,
Akamai Technologies, Inc.

Tom Ruff
Akamai Technologies, Inc.

A: Know the difference between public, private and hybrid clouds and the various X-as-a-service delivery models that are associated with them. And perform an application and business impact analysis so you understand which of your applications are more suited to the cloud.

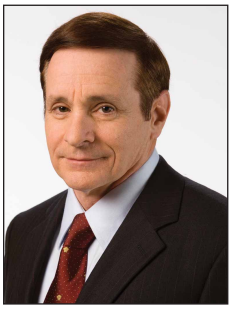
Invest the time to document the current environment to determine realistic cloud ROIs. You can reduce your risk of deploying clouds by understanding and closely adhering to the National Institute of Standards and Technology (NIST) standards for the cloud.

Never compromise on security. That's critical. Hold your cloud providers accountable and make them demonstrate that they have the correct security safeguards in place. Also, ensure the provider's offering is reliable and that it scales, and has the ability to handle peak load capabilities that the cloud requires. Demand references.

Ensure that there are minimal switchover costs in the event that you, the agency, need to change your cloud approach.

And don't overlook the importance of the network. A secure, reliable and highly available network is the key to a successful cloud deployment and implementation. Even with the best cloud service in the world, if people can't get to the service it's of little value.

What are the top 10 things a federal agency needs to do to ensure that a cloud computing project is successful?



Richard W. Johnson, Chief Technology Officer and Vice President, Lockheed Martin Information Systems & Global Solutions

Richard W. Johnson
Lockheed Martin Information Systems & Global Solutions

A: Look at the full lifecycle and total cost of ownership to determine true affordability. Maintain a focus on culture, processes, standards and experience, because they are still critical to success. Leverage cloud computing fully to enhance agility, security and for greenness, not only to cut costs.

Realize that the use of both public and private clouds will provide the most flexibility, but that one solution will not fit every environment. Think standards. And don't forget you'll need to train software developers, systems engineers, system architects and O&M teams as you shift to this new development environment and architecture.

Have a transition strategy to get into the cloud, but don't forget you'll also need one for exiting the cloud or shifting from one cloud to another. You'll also need a good foundation of strong risk management and expertise in managing service level agreements. And remember, going to the cloud is a partnership. As an integrator we can recommend, but we can only execute your vision for the cloud if we work together.

And finally look at the movement to the cloud as an inflection point for your agency. Take advantage of it as a way of rallying leadership efforts.

THE STAND Cloud Computing Question 14

If you were going to give federal IT project managers one piece of advice about cloud computing, what would it be?

GiGi Schumm,
Vice President and General Manager, Public Sector,
Symantec Corp.

GiGi Schumm
Symantec Corp.

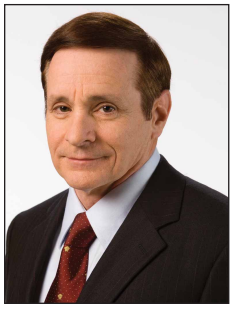
A: It would be around the whole concept of trust and compliance. How can they ensure their data is secure when they move them to the cloud, and not only secure but able to meet all of the data compliance and governance requirements? They could take many applications and just throw them into the cloud, but they shouldn't unless they understand that the applications and the data will be as secure as if they were housed within the agency's own four walls. They need to know how that data will be managed, how they segment them from someone else's information, and so on.

There also has to be a degree of transparency between the agency and the cloud provider. For example, Symantec uses cloud-based services to help run our business and we have applications and important data that are out in the cloud. You can be sure we have many conversations with our cloud provider, that we have service level agreements and audit rights, and that the provider is meeting the same security standards that we would use. We need to make sure that the provider can and is doing what they say are doing.

Tom Ruff,
Vice President,
Public Sector,
Akamai Technologies, Inc.

Tom Ruff
Akamai Technologies, Inc.

A: Agencies really need to fully understand their environment and therefore the applications which are most appropriate for the cloud. And I would add one more suggestion. They've got to have secure computing in order for cloud computing to take off. To do that they must hold their service providers accountable. Don't compromise the mission just to save money. At the end of the day, if they understand the cloud and what their service providers can deliver, they can accomplish their mission and save money.



Richard W. Johnson,
Chief Technology Officer and Vice President,
Lockheed Martin Information Systems & Global Solutions

Richard W. Johnson
Lockheed Martin Information Systems & Global Solutions

A: Don't forget there are transformation considerations, and you need to plan for your transition from your current environment to a cloud environment. Understand that a risk management approach is the best way to handle that, because there are many permutations and combinations in delivering and accessing cloud services. And you really need to be able to look at the different options and decide what's best for your agency.

Remember that best practices that apply to every project also apply to cloud computing. Cloud computing happens to be an inflection point in our industry, and as a leader, this inflection point provides an opportunity to apply your past experience and leverage this new capability to quickly provide value for your agency or mission.

THE STAND Cloud Computing Question 15

Talk about your company's strategic approach to cloud computing in the federal market.

GiGi Schumm, Vice President and General Manager, Public Sector, Symantec Corp.

GiGi Schumm
Symantec Corp.

A: We think that we can help agencies protect their information, whether they're looking to take advantage of public or private clouds. We think we've got the security expertise needed to help federal agencies ensure they maintain the level of risk management needed to meet their mission objectives.

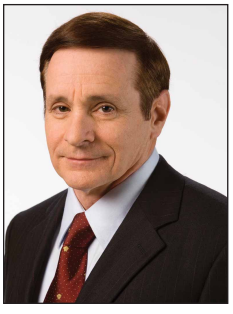
Symantec is in a unique position. We're a consumer of cloud services as a company, we're a provider of cloud services. Our online backup I talked about as well as the Symantec hosted security services that we offer, and we have a lot of technology that's cloud enabling. We believe we have the broadest spectrum of cloud enabling technology out there because it goes beyond traditional security software. We have backup and storage technology, virtualization technology and have more recently introduced encryption and identity management technologies. All of those are really key technologies in enabling agencies to take advantage of the cloud.

Tom Ruff, Vice President, Public Sector, Akamai Technologies, Inc.

Tom Ruff
Akamai Technologies, Inc.

A: Akamai provides a set of discrete cloud based service capabilities. Our strategic approach is not based on any one aspect of cloud software or platform services, but to remain the cloud enabler or optimizer. What I mean by that is our cloud strategy positions Akamai to be an overlay technology that enhances a variety of cloud services in a way that allows those capabilities to remain visible, controlled, highly available, scalable and secured.

We don't play in just one cloud offering, we play across multiple aspects of the cloud. We not only provide discrete capabilities, but more importantly we provide enhanced cloud services in order to overcome the limitations of the cloud and to fully meets the agency's needs.



Richard W. Johnson, Chief Technology Officer and Vice President, Lockheed Martin Information Systems & Global Solutions

Richard W. Johnson
Lockheed Martin Information Systems & Global Solutions

A: It's based on partnership and innovation. By collaborating with partners and Lockheed Martin technologists, together we can provide more innovative capabilities because we realize that no one individual or company can meet all of the technical requirements to deliver cloud computing in government.

These two aspects of our strategy have three major elements associated with them. The first is focusing on development of a suite of secure cloud services, which are operationalized and bring strategic benefits to our customer's core missions. The second is the launch of an online marketplace that allows our customers to go to, test, evaluate and then purchase our secure cloud services.

And the third is the delivery of those capabilities via a trusted cloud service and operating model, which provides the ability to customize the various offerings specific to agency needs, and to the specific business model and buying patterns that are most beneficial to individual agencies.