

Online report sponsored by:

GovConnection®
Gov is all you need™



Cloud Computing

A Work in Progress | S2

Achieving Cloud Greatness | S3

Floating on Clouds | S4

Some Things Are Better Left Private | S5

Lessons-learned from Amazon's Outage? | S6

www.FCW.com/specialreportcloudcomputing



A Work in Progress

Who is responsible for security in the cloud? It depends on whom you're asking, according to Ponemon Institute's Security of Cloud Computing Providers Study.

The April 2011 report found that 69 percent of the 127 cloud providers surveyed said that cloud users are the ones responsible for security. A mere 16 percent said security should be a shared responsibility. With data like that, it's no wonder that CIOs and IT executives wonder if their data and applications are safe in the cloud. The good news is cloud computing really is safer than most people think as long as the right controls are put into place. Most security problems are because of a lack of education, experts say.

"I don't think the market as a whole does a good job at communicating the fact that there are standards and policies in place that help secure the cloud," said Dennis Hurst, founding member of the Cloud Security Alliance (CSA), a nonprofit organization dedicated to cloud security. "Security really depends on the cloud provider and the nature of the business you're going to conduct in the cloud. In reality, there are cloud services out there that are far safer [to use] than someone's own IT infrastructure."

Geoff Weber, a principal at KPMG's federal practice, agreed. "There are plenty of examples of data and security breaches within state and federal enterprises that are not operating in the cloud," he said.

Go by the book

Before assessing a single provider, IT executives should decide exactly what requirements their organizations have when it comes to security, compliance and governance. Everything from how a cloud provider handles disaster recovery to application security and segmentation on a shared server should be discussed. Ownership of data should also be part of any security discussion. Organizations should own their data and have an easy way to pull it out of the cloud if they decide to swap vendors. Another big concern, Weber said, relates to data privacy and multitenancy. "You need to know what happens if there's a breach," he said.

The safest cloud implementations — public or private — use industry standards and matrices that are designed to thwart potential problems and create secure connections. Firewalls, public key infrastructure, virtual private networks and multifactor authentication should be in force from a

technology standpoint, and there should be soft controls in place so employees and users have the appropriate access and rights.

In addition, because the choice of vendor can mean the difference between success and failure, it's important to use the right assessment tools to make sure you're choosing the right cloud provider. For example, in December 2010, the Cloud Security Alliance released Revision 1.1 of the Cloud Controls Matrix (CCM) Security Controls Matrix, as part of the CSA's governance, risk assessment and compliance goals. The CCM security matrix is "specifically designed to provide fundamental security principles to guide cloud vendors and to assist prospective cloud customers in assessing the overall security risk of a cloud provider," according to CSA. IT executives can use the matrix as part of an overall assessment strategy, Hurst said.

Another good source is the National Institute of Standards and Technology, which has a cloud computing working group in its Computing Security Division. NIST's role in cloud computing, according to the organization, is to promote the "effective and secure use of the technology within government and industry by providing technical guidance and promoting standards."

The organization released in February a set of guidelines for managing cloud security and privacy issues. The guidelines contained tips and strategies for those working in the cloud or moving toward it. There's also a NIST Cloud Computing Collaboration website with links to NIST Cloud Computing working groups and events, reference architecture and taxonomy, business use cases, and a standards road map. The Federal Risk and Authorization Management Program is another tool in the arsenal to help organizations assess and authorize cloud computing services and products.

It's this type of collaboration and effort, that's going to help dispel the myth that cloud computing is something that's too dangerous for organizations that have high security requirements, Hurst said.

"There's a common belief that cloud computing is somehow inherently insecure," Hurst said. "However, if people will make themselves aware of the standards and working groups and methodology that's out there for them to use, they can leverage the business value of the cloud today as opposed to waiting until they perceive it to be more secure. Successful — and secure — cloud computing implementations are attainable today." ▲



Achieving Cloud Greatness

The Justice Department will be consolidating the storage systems of 250 offices, which serve 18,000 U.S. attorneys. The destination: the cloud, according to Federal CIO Vivek Kundra, who announced the project in April at the White House Forum on Transforming Federal Information Technology Management. That's no small task, said Mitchell Ummel, director of the Cutter Consortium's Government Public Sector Practice. To succeed, Justice, like other agencies and organizations taking the leap into the cloud, must take several things into consideration.

For one, even though it doesn't take very long to provision a cloud-based service or infrastructure, CIOs and IT executives should remember that even cloud-based projects should be viewed as a marathon instead of a sprint. "They should look at the risk and move applications and services to the cloud based on cost and risk," Ummel said. "There's an analysis that needs to be done first."

Ummel suggested creating an enterprise cloud computing road map (ECCR) first and, after you know what you'd like to move, uncover the main drivers for your desire to move to the cloud. "Are the principal drivers cost, agility, flexibility, time to market? What are the long-range business objectives or outcomes to be obtained?" he asked.

After IT executives can answer these questions, they can start looking for viable cloud service providers. This step will become easier as the federal government's Federal Risk and Authorization Management Program (FedRAMP) gets closer to its end goal: providing a security accreditation and authorization program that will vet cloud providers.

FedRAMP is significant because there are very few standards available for assessing potential cloud providers. Even though the program is still in its early stages, it's something to watch and get involved with. Even though there's more work to be done, it will be a far shorter process than waiting for the private sector to develop formal standards for the cloud,

something that may take years, said Deniece Peterson, senior manager of federal industry analysis at research and market intelligence firm Input. "Once FedRAMP is complete, an agency with a need will be able to choose a provider based on consistent data and information," she explained.

Until FedRAMP is rolled out, organizations will still need to do much of their own legwork, asking potential providers about security policies, portability of data, interoperability and procurement. For example, any provider that doesn't use open standards should be immediately ruled out. Even if a provider has all the right answers, it's not a good idea to take a vendor's verbal promise. Requirements should be spelled out explicitly in a contract before a single file is moved from the data center to the cloud, said Dennis Hurst, founding member of the Cloud Security Alliance. The contract should also include a clear description of audit, compliance and security requirements that vendors will be subjected to. "Some audits might ask how data is backed up or how they handle segregation of duties," he said. Uptime guarantees should also be included in the contract, and IT executives should have an understanding of the cloud service's availability and security architecture, Ummel said.

Only when everything is in place should an organizations launch a cloud computing pilot, and even after it goes live, there's still more work to be done.

Organizations must identify and capture metrics including cost and time savings and customer satisfaction so they can extrapolate pilot results for additional cloud implementations in the future, Ummel said. Finally, executives should remember that the old set-it-and-forget-it trajectory is what got most of them into trouble in the past. Even in the cloud, there can be room for improvements and changes. "Continually review and revise your [cloud computing road map] at least once annually," Ummel said. "The enterprise cloud computing market and vendor landscape is rapidly evolving, and new opportunities will continually present themselves." ▲



Floating on Clouds

In December 2010, the General Services Administration announced it was moving 17,000 employees and contractors from a series of 17 fragmented, disparate e-mail systems onto a single cloud-based platform: Google Apps. About the same time, the Agriculture Department moved 120,000 users from its on-premises e-mail and productivity applications to the cloud. In this case, it was Microsoft Online Services including Microsoft Exchange Online and SharePoint Online. The savings were about \$27 million due to consolidation of about 21 different systems.

In May 2010, Recovery.gov, a public website that helps people track spending under the economic stimulus law, moved to Amazon's Elastic Compute Cloud infrastructure-as-a-service platform, saving about \$750,000, all of which was funneled back into the mission to fight fraud. As these examples demonstrate, the government is seeing significant adoption of and benefits from the cloud. And with the February release of the Federal Cloud Computing Strategy, the list is only going to get longer as CIOs and IT executives move toward the goals of consolidating data centers and shifting from an asset ownership mentality to a service provisioning mentality by leveraging cloud computing.

"We have, for the first time, a federal CIO who has cloud at the top of his agenda," said Deniece Peterson, senior manager of federal industry analysis at research and market intelligence firm Input. "Vivek Kundra is putting forth an aggressive timeline, and agencies are going about things slowly looking at low-risk areas and deploying the cloud with care."

Low-hanging fruit

The success of the cloud in the government sector might be surprising to some because most agencies don't have a great track record when it comes to projects that use new or emerging technologies, with many failing or going over budget before results could be realized. However, the cloud

strategy is different because there's proven technology in place, a mandate to shut down 800 federal data centers by 2015, and a streamlined process to get cloud vendors of all sizes certified as providers. There's also the cloud-first policy that states that every agency looking for new technology must evaluate the cloud first. Finally, there's also a need to have more transparency on spending and a greater awareness of budgets, said Geoff Weber, a principal at KPMG's federal practice. The combination of which, he said, creates a perfect storm for the cloud.

In fact, according to a speech by Kundra in February, agencies across the government have identified at least three systems that can and will move to the cloud during the next 18 months. "These are not just simple systems, but these are going to be systems that are core to the workflow of these agencies. And these are systems that are going to be disruptive in terms of budget savings," he explained.

For example, at the Army, users moved to a Salesforce.com implementation that costs the government \$54,000. Another bid for an on-premises system came in at more than \$1 million. However, the real benefit was that recruiters at the Army Experience Center in Philadelphia are able to track recruits who participate in simulations and connect with them via social networking channels that include Facebook and e-mail.

Government IT executives are also seeing benefits as they shift from traditional infrastructure to infrastructure as a service, Weber said. "Telecom, storage, processing are easy to implement, and take the burden of provisioning, maintenance and training out of the hands of the IT staff and put it in the hands of the cloud provider." This reduces cost of service, but it also helps the government standardize on technology that may have been out of reach in the past, he said. ▲



Some Things Are Better Left Private

Ask even the savviest IT executives to list the differences among public, private and hybrid cloud implementations, and you're bound to get a variety of answers. However, experts say government CIOs and IT executives need to get familiar with the ins and outs of each because their future infrastructure will contain components of all three.

"There will be pieces of the cloud that will have to remain private because of the complexity of the legacy environments in the government sector," said Deniece Peterson, senior manager of federal industry analysis at research and market intelligence firm Input.

The National Institute of Standards and Technology defines a private cloud as "being operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise." To some, the idea of an off-premises cloud solution would automatically put it into the public cloud camp, but it's important to note that even an off-premises cloud implementation can qualify as a private cloud. The difference is ownership. A private cloud is owned by one organization for its exclusive use. In government, this exclusivity means there's less to worry about from a security standpoint.

"A private cloud is no different than a traditional data center," said Dennis Hurst, founding member of the Cloud Security Alliance, a nonprofit organization dedicated to cloud security. "You're going to use a lot of the same technologies to manage it, and from an isolation and audit perspective it's going to be similar, too." In addition, a private cloud can help change the way an organization looks at IT spending, taking it from the peanut butter model – spreading the cost of services and infrastructure across all departments – to a utility billing paradigm. "This is one way where you can identify where your spending is taking place and where you can eliminate computing power and applications," Hurst said.

But that's not to say that a private cloud is automatically more secure. Some large cloud providers might have better security and governance in place than their customers do, and using a public cloud implementation could reduce audit complexity. Banks and financial institutions, which rely on public cloud providers, can attest to that first hand, Hurst said.

It's easier to migrate data and applications to a private cloud. However, private clouds can reduce cost savings unless management is outsourced, Peterson said. This will be specifically pronounced in implementations that have both public and private components.

Equipment is one cost factor. When IT managers need to add capacity, they might need to turn to new equipment to handle the load, necessitating a capital expenditure. In a traditional public cloud, extra capacity can be added incrementally and put into the operating budget bucket. Of course, the same benefits can be achieved by outsourcing a private cloud, Hurst said.

That might be why Forrester Research, in an April 21 report, "Sizing the Cloud: Understanding and Quantifying the Future of Cloud Computing," predicts that infrastructure as a service, which can be used for "compute power, storage, database functionality, archive, or other basic resources" will shift from public clouds to virtual private clouds and create a market worth \$1.4 billion by the end of this year. Meanwhile, the total market for private cloud solutions – which includes infrastructure, middleware, business processes and application virtualization tools – will grow from \$7.8 billion this year to \$15.9 billion by 2020. "Infrastructure virtualization tools help enterprises to increase the average utilization of on-premises hardware and thus save hardware costs or improve application performance," according to the report.

"The future of the cloud looks like it's hybrid," Peterson said. "There are going to be a lot of choices being made in the government sector." ▲



Lessons Learned From Amazon's Outage

Every time there's a major cloud-related outage, someone will question whether government agencies should be putting their trust and data in the technology. Those critics got a little louder after an April 21 outage of Amazon Web Services' Elastic Compute Cloud, which brought down the Energy Department's OpenEI.org, a collaboration platform for people who work on clean-energy solutions, among other sites. The site was down for almost two days, along with the popular social networking sites HootSuite.com, Reddit and Quora. The entire outage took about five days to completely resolve.

However, an examination of what happened should help quiet those voices, say experts, who are quick to point out that there's no reason to fear the cloud. In fact, the outage is a perfect way to showcase how most customers could have avoided that fate completely. Amazon's problem started during a routine network upgrade. A configuration error caused a large number of Elastic Block Store (EBS) volumes to become unable to service read and write operations, according to a report released by the company.

"When this network connectivity issue occurred, a large number of EBS nodes in a single EBS cluster lost connection to their replicas," according to the company's report. "When the incorrect traffic shift was rolled back and network connectivity was restored, these nodes rapidly began searching the EBS cluster for available server space where they could remirror data. The free capacity of the EBS cluster was quickly exhausted, leaving many of the nodes 'stuck' in a loop, continuously searching the cluster for free space." That led to what Amazon calls a remirroring storm. A large number of volumes were effectively stuck while the nodes searched the cluster for the storage space they needed for their new replica.

Planning for disaster

Diagnosing the outage is important because users who had planned ahead and constructed their cloud presence so that data resided in multiple regions or different availability zones – presences mapped to different data centers in the same region – were able to avoid an outage or get their services back quickly. "The lessons learned are that cloud – like any other complex system – must also be architected for availability, there is a cost for that high availability, and human error is always a factor," said Mitchell Ummel, director of the Cutter Consortium's Government Public Sector Practice.

Ummel said there's good news that many of media outlets glossed over: the majority of Amazon's customers were unaffected. "We read about big customers such as Netflix that didn't trust one availability zone and were able to fail over to another availability zone or another private or public cloud instance," he said. "Yes, there's an added cost to that, but when a system is crucial, people will pay for it."

Another lesson that everyone should take away from the Amazon outage is the fact that no systems, cloud or otherwise, can guarantee 100 percent uptime. Agencies should only agree to service level agreements when they can be comfortable with the anticipated response to a cloud service failure. Questions about data loss must be asked during any SLA discussion because, as some of Amazon's customers discovered, a widespread outage occasionally leads to data loss. The company reported that 0.07 percent of the data stored in the affected availability zones was not fully recoverable.

Taking all that into perspective, Amazon's outage might go down in history as one of the best things to happen to cloud computing strategies, said Deniece Peterson, senior manager of federal industry analysis at research firm Input. "It raises awareness and gets people thinking about control – who has it, how to share it with a vendor, and how to avoid problems in the future. ▲



**Powerful.
Intelligent.**



Choose the Right IT Partner

» Get the most out of your data center with GovConnection and HP. Our HP enterprise solution specialists are here to serve our federal customers. From servers and storage to networking and beyond, we have the in-house expertise to help you optimize your infrastructure while also cutting costs.

Ask us about the new HP G7 servers, featuring the Intel® Xeon® 5600 processor family. HP G7 servers support your consolidation and virtualization initiatives in the data center by providing higher availability, better adaptability, and faster ROI through advanced power savings.

 We have the product selection, technical expertise, and purchasing contracts you need. Call an Account Manager today to get started.

1-800-800-0019

www.govconnection.com/servervirtualization

Follow us on Twitter!

GovConnection[®]
Gov is all you need™