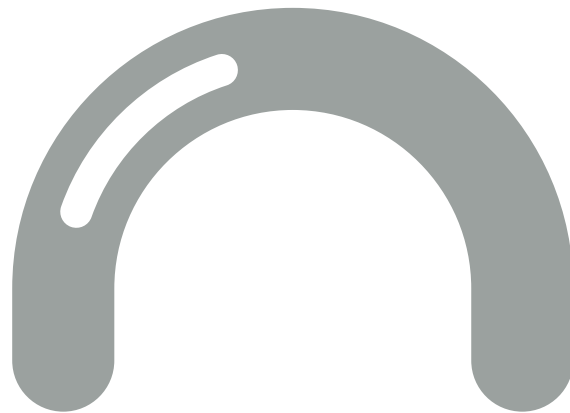


Awareness, Trust and Security to Shape Government Cloud Adoption



Awareness

Trust

Security

A white paper by:



LM CYBER SECURITY™
ALLIANCE



April 2010

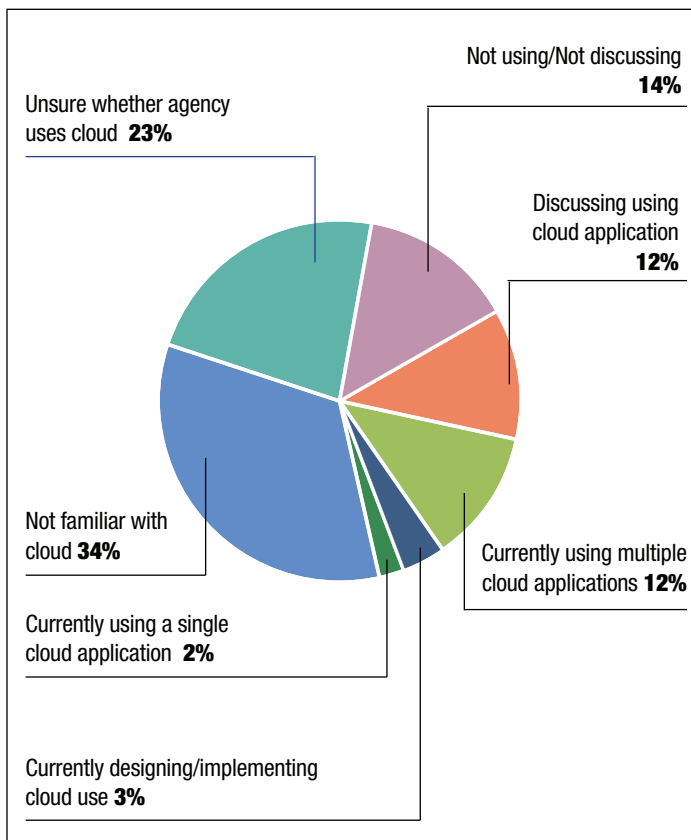


Executive Summary

The awareness, trust and security issues that have limited federal government adoption of cloud computing appear to be more perceptual than prohibitive, according to the Lockheed Martin Cyber Security Alliance survey on cloud computing and cyber security conducted by Market Connections, Inc. Professionals who are most aware of and involved with cloud computing and cyber security generally trust the cloud model, and do not consider it a leading security vulnerability¹. The findings suggest cloud utilization is poised for rapid gains as awareness of cloud computing and the related cyber security implications grow.

Overall, a full 34 percent of federal government, defense/military and intelligence agency respondents are unfamiliar with cloud computing, and only 14 percent said their agencies had adopted it. Three out of five respondents do not expressly trust cloud computing. Twenty-three percent of respondents do not know what their organizations are doing with cloud computing, and there is no consensus on how cloud governance should be handled.

Figure A: Government State of Cloud Engagement



Knowledge is not necessarily widespread among agencies involved in cloud computing. Approximately a fifth (21 percent) of respondents who are involved in cyber security at their agencies are not familiar with cloud computing, while nearly half (47 percent) of respondents who are familiar with cloud computing are not involved in cyber security. These findings illustrate awareness gaps among professionals who will be investigating, implementing, using, securing and managing cloud computing. Conversely, this data may also suggest that implementing and managing cloud computing platforms within federal agencies will require cross-functional discussion among both IT policy and IT implementation professionals.

Yet, adoption of cloud-based solutions is growing. Increased awareness and understanding of cloud computing can pave the way for more adoption, as respondents who are familiar with cloud computing tend to pursue its inherent benefits. The adoption rate among respondents familiar with cloud computing (44 percent) is more than triple the overall adoption rate (14 percent). Eighty-five percent of respondents who adopted cloud computing use it for multiple applications, and agencies are increasingly putting mission-critical data management systems into the cloud, which indicates that utilization and trust increase significantly once the cloud-based solutions are adopted. Respondents who are involved with cyber security ranked cloud computing last on their list of security challenges.

The full paper documents and explores these findings, and:

- ▶ Presents a snapshot view of cloud computing adoption in U.S. federal government, defense/military and intelligence agencies;
- ▶ Documents trust levels related to cloud computing, outsourcing and different delivery models;
- ▶ Identifies specific cloud computing and cyber security concerns;
- ▶ Highlights governance issues;
- ▶ Presents recommendations to help government agencies prepare to adopt, secure and manage cloud computing.

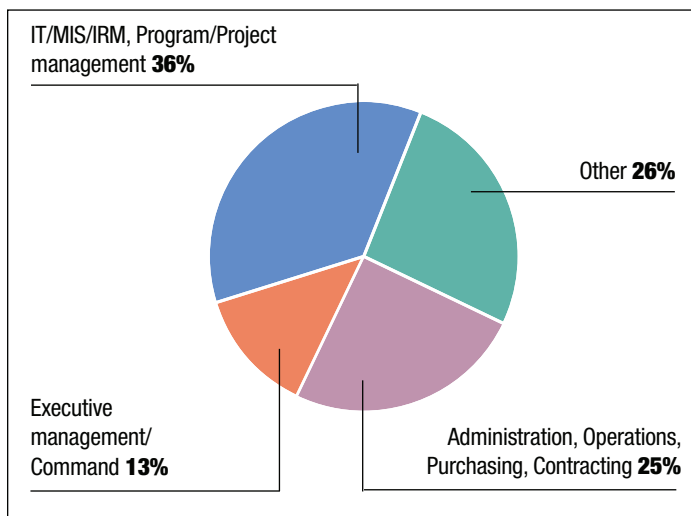
1. Throughout this report, the narrative makes reference to trust and involvement. Participants were asked to rate their involvement, awareness or trust levels about specific aspects of cloud computing and cyber security on a five-point scale, with one representing the lowest level of involvement, awareness or trust and five representing the highest. A response of three is considered neutral. If respondents are said to be "involved" (e.g., Respondents who are involved in cyber security at their organization are more likely to be aware of cloud computing.), the reference is to respondents who rated their involvement as either four or five on the five-point scale, which therefore excludes neutral responses. In discussions of trust, respondents who indicated a trust level of one or two are said to distrust and those who responded four or five are said to trust.



About the Survey

The Lockheed Martin Cyber Security Alliance commissioned Market Connections, Inc. to conduct an online survey of U.S. federal government, defense, military and intelligence agency IT decision makers in February and March 2010. The Alliance consists of the following technology companies: APC by Schneider Electric, CA, Cisco, Dell, EMC Corporation and its RSA Security Division, HP, Intel, Juniper Networks, McAfee, Microsoft, NetApp, Symantec and VMware. The survey measured awareness and attitudes about cloud computing and cyber security topics. The survey produced 198 responses, including respondents from all branches of the military, and representing a wide variety of government agencies. Information technology, operations and management professionals at multiple levels were all represented as shown in Figure B below.

Figure B: Respondents by Role



State of Cloud Computing Adoption

Cloud computing has a foothold in the government market, and the survey data suggest adoption is likely to increase. Today just 14 percent of respondents surveyed said their agencies have at least one cloud computing application, and 85 percent of these are using multiple applications in the cloud. Current adoption is virtually the same at federal civilian (13 percent) and defense/military (14 percent) agencies. Figure A (page 1) details the overall level of government cloud adoption.

Several factors suggest the adoption base could grow rapidly. First, the percentage of respondents who are currently discussing migrating to cloud computing or are actively involved in doing so (16 percent) exceeds the percentage who have already adopted. As noted, agencies that adopt cloud computing tend to utilize it for multiple applications, so greater penetration within the current user base could be expected.

Second, the adoption rate among those who are familiar with cloud computing is more than triple the overall adoption rate. Increased awareness of cloud computing is thus expected to result in increased adoption. Since 34 percent of respondents are not familiar with cloud computing, and an additional 23 percent do not know what their agencies are doing

Participants were presented the following definition of cloud computing to use as a guide when answering questions:

CLOUD COMPUTING is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing can take the form of:

- ▶ **SOFTWARE AS A SERVICE (SaaS)** in which the applications are accessible from various client devices through a thin client interface such as a web browser;
- ▶ **PLATFORM AS A SERVICE (PaaS)** in which end users develop or deploy applications on top of cloud infrastructure; or
- ▶ **INFRASTRUCTURE AS A SERVICE (IaaS)** in which the provider manages the hardware, but allows the end user to manage the operating systems, storage, and/or application deployment.

The terminology presented was extracted from National Institute of Standards and Technology (NIST) definitions.

with it, the potential for awareness, and therefore adoption, to grow is very high. Only 5 percent of respondents who are aware of cloud computing do not think it is applicable for their agencies.

Third, the expected growth is consistent with other cloud computing projections. Cloud computing is currently one of the fastest growing trends in all of IT, in both the public and private sectors, and federal CIO Vivek Kundra has been a visible public advocate for cloud computing. The government market for cloud computing will more than triple between 2009 and 2014, but the strong growth rate will actually lag behind the private sector according to 2009 research from INPUT².

Despite these adoption findings and projections, resistance to cloud adoption will remain. There are 14 percent of respondents who are aware of cloud computing, but are not using or discussing it at their agencies. Another 23 percent are unaware of what their agency is doing with cloud computing.

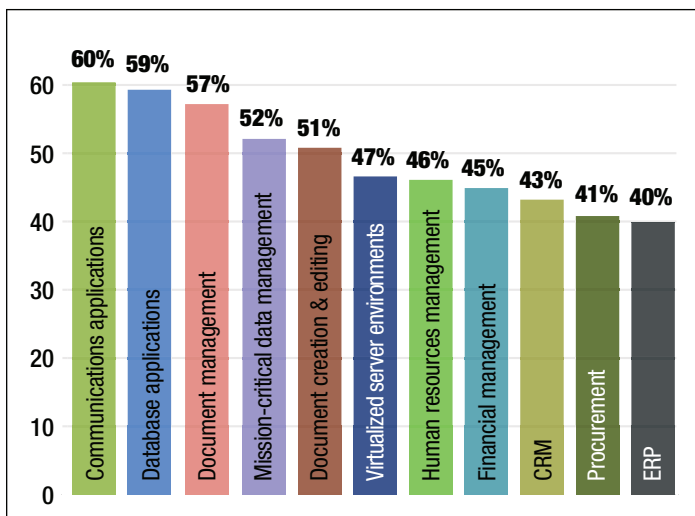
Adoption by Application

Insight from early adopters shows government users are willing to use cloud computing for core functions of their IT infrastructure, which also suggests a strong ongoing role for utility computing. Nearly a quarter of respondents use cloud computing for mission-critical data management, and an even higher percentage are considering doing so, as shown in Figure C (page 3). ERP is the application that agencies are least likely to access from the cloud, but 40 percent of respondents are using or considering the cloud for ERP. CRM is a widely used cloud application outside of government, but ranks second-to-last among applications that government respondents are using or considering.

2. Emerging Technology Markets in the U.S. Federal Government, 2009-2014. INPUT report released December 7, 2009.

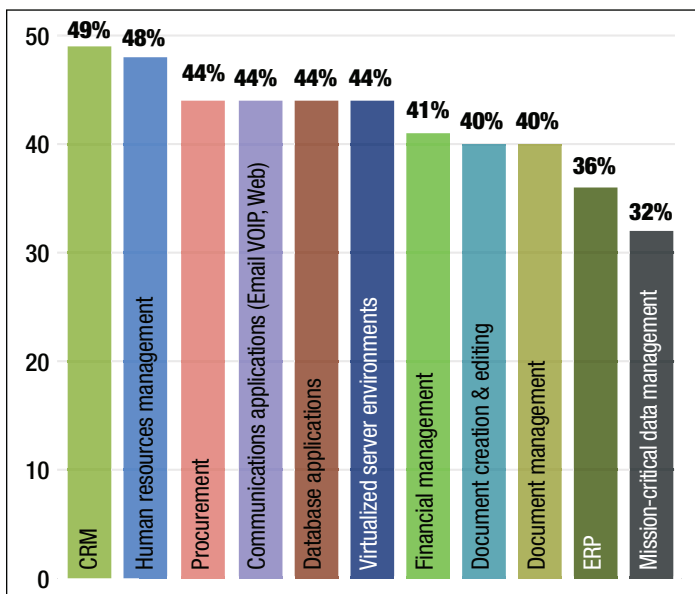


Figure C: What Applications is Cloud Computing Being Used or Considered For



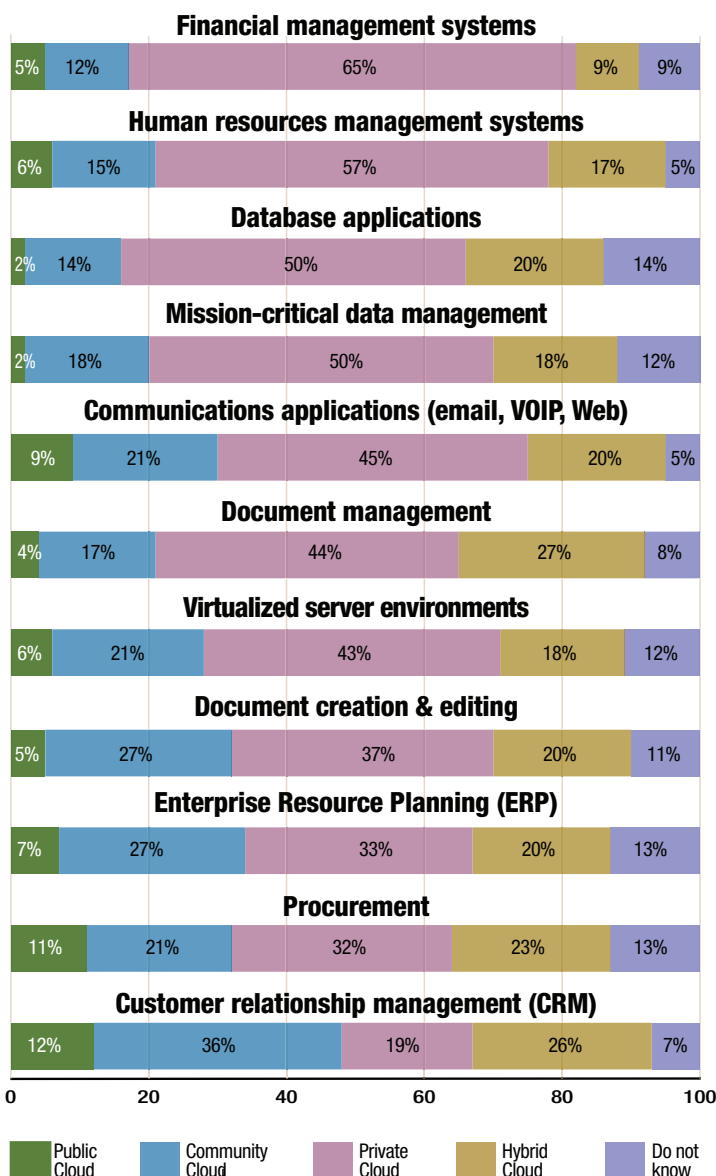
Respondents may be willing to put essential systems in the cloud, but these are among the applications they are least likely to outsource. Figure D shows the likelihood respondents will outsource different cloud applications. They are most likely to outsource CRM, human resources management, procurement, communications, database and virtualized servers. Mission-critical data management applications are least likely to be outsourced, followed by ERP, financial management and database applications. Note that database applications also ranked highly as an application most likely to be outsourced.

Figure D: Likelihood to Outsource Cloud Applications



Respondents who would consider outsourcing want control over their cloud. Private cloud is clearly the favored delivery mode and there is strong resistance to the public cloud model, as shown in Figure E below. Private cloud was the top choice of delivery mode for 10 of the 11 applications surveyed; respondents were most likely to consider a community cloud for CRM outsourcing. The levels of support for community and hybrid clouds were similar to each other, especially for applications that do not involve essential enterprise or employee information. Support for the public cloud model is consistently low. No more than 12 percent of respondents would consider using a public cloud for any application.

Figure E: Cloud Modes Considered for Application Outsourcing





LM CYBER SECURITY™
ALLIANCE



Cloud Awareness Levels

For all the attention and growth cloud computing has achieved, there is still widespread lack of awareness and misunderstanding. The percentage of respondents who are not familiar with cloud computing (34 percent) is two-and-a-half times as high as the percentage whose agencies are using it (14 percent). Respondents at civilian agencies are more aware of cloud computing than their defense/military counterparts (37 percent to 30 percent), but neither population has a high level of awareness. Surprisingly, a fifth (21 percent) of professionals involved in cyber security at their agencies are unaware of cloud computing.

Among respondents who are aware of cloud computing, 23 percent are unsure of what their agency is doing with it. That means more than half (57 percent) of respondents are either unaware of cloud computing in general or their own agency's specific cloud activity. The low level of understanding makes the 14 percent adoption rate more telling, as cloud computing continues to experience the uncertainty associated with emerging technologies.

The survey found that there are significant trust and governance questions regarding cloud computing, and the low level of awareness is certainly a contributing factor. Low awareness appears to extend beyond cloud computing itself, and also to how it should be governed and secured. As noted, nearly a quarter of respondents who are aware of cloud computing do not know what their agencies are doing with it, and 21 percent of respondents who are involved in cyber security are unaware of cloud computing. There were also respondents who are aware of cloud computing who are not involved with cyber security. These differences

Survey participants were given the following definitions for specific cloud models:

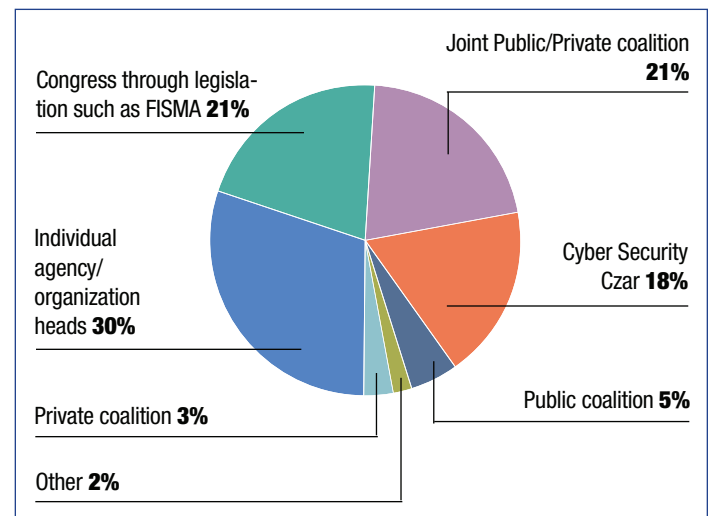
- ▶ **PRIVATE CLOUD** the cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
- ▶ **COMMUNITY CLOUD** the cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
- ▶ **PUBLIC CLOUD** the cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- ▶ **HYBRID CLOUD** the cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting).

The terminology presented was extracted from National Institute of Standards and Technology (NIST) definitions.

indicate there is implementation and policy crossover within agencies when it comes to cloud computing, which underscores the importance of keeping multiple stakeholders aware and involved with cloud computing initiatives. These policy considerations may already be surfacing, as 21 percent of respondents said they are concerned about cloud governance within their agency, a figure that rises to 30 percent among respondents who are most involved in cyber security.

The challenge in developing a cloud computing strategy is compounded by the lack of clarity around who should ultimately govern cloud computing, as illustrated in Figure F below. In aggregate, 39 percent of respondents feel cloud computing should be governed at the federal level (either by a cyber security czar or through congressional legislation), 30 percent say it should be governed at the agency level, and 29 percent favor some form of coalition. See figure G next page.

Figure F: Who Should Govern Cloud Computing?

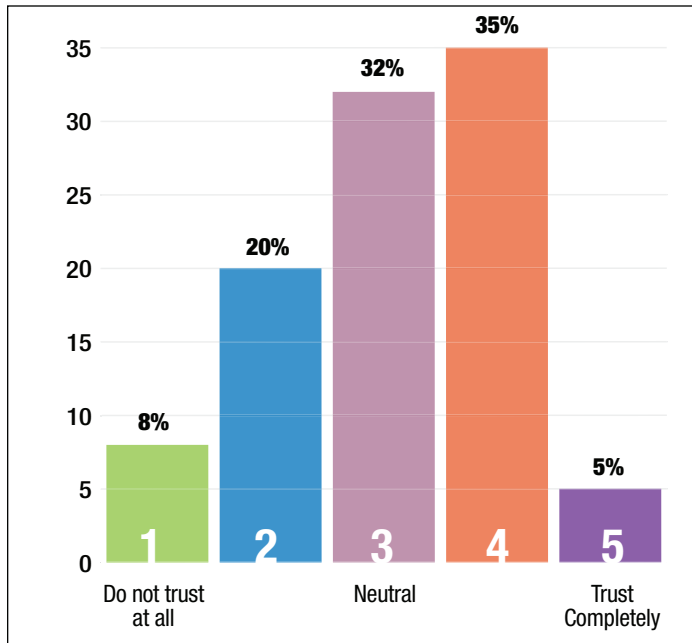


Trust Levels and Considerations

Trust in cloud computing is an unresolved issue among government IT decision makers. While more respondents (40 percent) trust than distrust (28 percent) cloud computing, it would be wrong to conclude the model has attained a solid level of trust. Nearly a third of respondents are neutral or undecided regarding their trust of cloud computing. Therefore while 40 percent of respondents say they trust cloud computing, 60 percent do not. Six percent responded they “do not trust cloud computing at all,” which is twice as many who responded they “trust completely.”



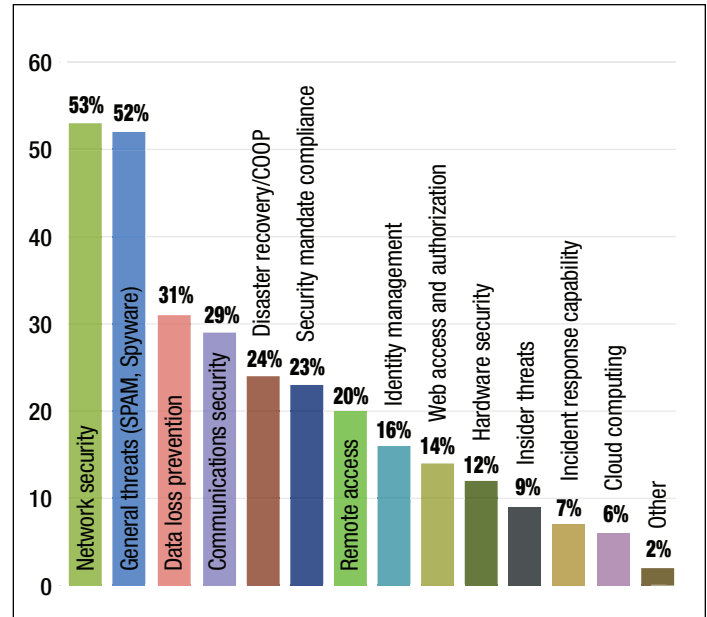
Figure G: Level of Trust in Cloud Computing



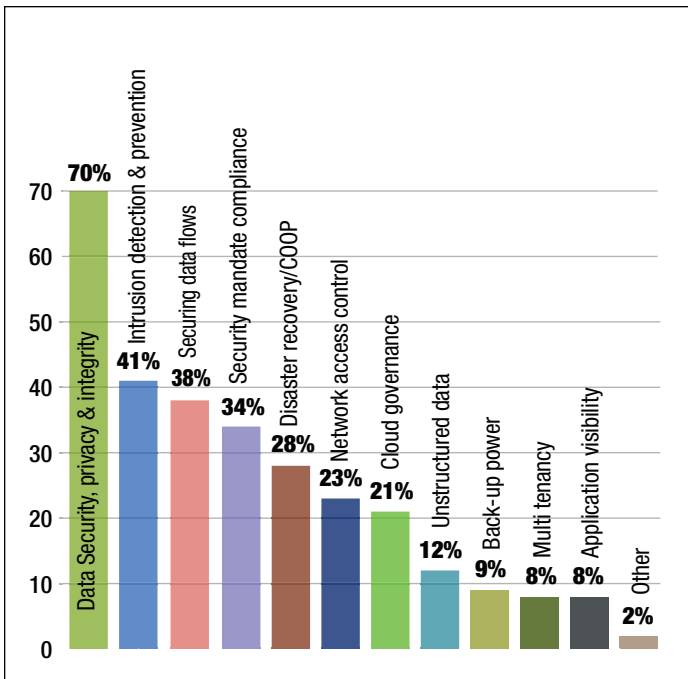
Respondents who are involved in cyber security have more trust in cloud computing. Cloud computing is trusted by 53 percent of respondents who rated their involvement level a four or five on a five-point scale, compared to 40 percent of overall respondents. Twenty percent of those involved in cyber security distrust cloud computing, compared to 28 percent of overall respondents.

Cyber security professionals ranked cloud computing last among their cyber security challenges of note, as Figure H shows. This may indicate an overly narrow view of cyber security, because many of the more highly rated challenges also apply to cloud computing. It could also indicate lack of depth of understanding about cloud computing architectures and under appreciation of what is required to secure cloud computing systems and their users.

Figure H: Cloud Risk Relative to Other Security Concerns



Some of the distrust in cloud computing invariably comes from respondents' inexperience with it. Distrust may also result from uncertainty about how to secure applications and data in the cloud, including how security considerations change based on the specific cloud model (e.g. IaaS, PaaS, SaaS; public, private, community or hybrid cloud). Figure I on page 6 shows respondents' leading security concerns for cloud computing. Data security is by far the top concern of note, and is the only one cited by a majority of respondents. The other leading issues are intrusion detection, securing data flows between data centers, clients, and applications, and security mandate compliance. While these are all legitimate issues, they are not unique to the cloud or inherently impossible to secure in the cloud. Conversely, multi-tenancy, where different, non-related organizations may share infrastructure such as space on a server, is a cloud-specific security consideration, but it ranks near the bottom of respondents' concerns. The specific security concerns of overall respondents are extremely consistent with those of respondents who distrust the cloud, and with those who are involved in cyber security.


Figure 1: Cloud Computing Security Concerns


Other studies have found that while security is considered the top challenge associated with cloud computing³, federal government professionals think cloud computing itself raises an organization's risk less than most other IT megatrends, including mobility, Web 2.0, and virtualization⁴, which have all been widely adopted.

Previously presented cloud computing adoption data suggest cloud computing security and trust issues can be overcome. Recall that respondents who are involved with cyber security ranked cloud computing last on their list of notable security challenges, and that 85 percent of adopters use cloud computing for multiple applications. These results suggest that as professionals gain understanding and experience with cloud computing, they gain confidence in their ability to implement effective, secure systems.

Conclusions and Recommendations

Cloud computing has low levels of awareness, trust and adoption among IT decision makers in the U.S. defense/military and federal government. Despite all the attention cloud computing receives as one of the leading IT trends, a third of government IT decision makers surveyed were not familiar with cloud computing, and a similar percentage do not trust it. Awareness and trust are lacking even among professionals who are familiar with it and may be responsible for securing enterprise systems and information. While cloud adoption is expected to grow, respondents' inexperience with cloud computing, security concerns (and in some cases, lack of concern) and uncertainty about governance could make it difficult for organizations to effectively implement cloud computing or realize full value from it.

The outlook for cloud computing adoption in government depends on how well cloud computing service providers and potential users raise the levels of awareness and trust in the model. The data reflects barriers to adoption, but adoption rates and user experiences show the barriers can be overcome. Respondents who know cloud computing best trust it most. For example, those who are familiar with cloud computing tend to implement it, those who implement expand their use by accessing multiple applications through the cloud, and professionals who are most involved in cyber security have more trust in cloud computing than IT decision makers at large.

Against this backdrop, we recommend organizations take the following actions to assess the suitability of cloud computing for their agencies and to prepare for implementation:

► DEFINE WHAT THE CLOUD MEANS TO YOUR ORGANIZATION.

Private? Public? SaaS? IaaS? PaaS? Having a common definition of what a cloud means will make it much easier to manage cloud initiatives, including planning, implementation and security.

► **CREATE AWARENESS OF CLOUD INITIATIVES THROUGHOUT THE ORGANIZATION.** Besides the 21 percent of respondents who are involved in cyber security but not familiar with cloud computing, 47 percent of respondents who are familiar with cloud computing are not involved with cyber security. The data suggest that professionals who will be implementing cloud computing are not responsible for managing security, and vice versa. To ensure policies, systems and governance are aligned, stakeholders throughout the organization need to be aware of all cloud computing activity, even if it is only in the discussion stage.

► **TAKE A BROAD VIEW WHEN ASSESSING CLOUD'S IMPACT.** Cloud computing can have security implications that security professionals may not have considered, and overall security policies need to extend to users who access applications through the cloud and via traditional methods. Systems, staff, training and policies should be assessed and adjusted as necessary to effectively support cloud computing.

► **ENGAGE PROFESSIONALS FROM ORGANIZATIONS WITH SPECIFIC CLOUD SECURITY EXPERTISE.** Considering the low level of awareness for cloud computing among government IT decision makers, and its lack of adoption and maturity within the public sector, organizations who are considering cloud initiatives should seek guidance from professionals from organizations with specific experience in secure cloud computing. Only 5 percent of respondents involved in cyber security ranked cloud computing as one of their top security concerns. The lack of concern may come from respondents' confidence in their ability to secure the organization from cloud computing threats. As with any IT initiative, early engagement of security professionals will yield a more cost-effective risk management approach than retroactive ones. Experienced professionals can identify security and other implementation issues and recommend appropriate solutions.

3. IDC Enterprise Panel, August, 2008

4. Ponemon Institute "Cyber Security Mega Trends: U.S. Federal Government." November, 2009.