

**Can Law Enforcement Agencies Risk the Move to Cloud Computing
Technology?**

by

**Lt. Matt Morgan
Sacramento County Sheriff's Department**

05/2010

P.O.S.T. COMMAND COLLEGE CLASS #47

The Command College Futures Study Project is a FUTURES study of a particular emerging issue of relevance to law enforcement. Its purpose is NOT to predict the future; rather, to project a variety of possible scenarios useful for strategic planning in anticipation of the emerging landscape facing policing organizations.

This journal article was created using the futures forecasting process of Command College and its outcomes. Defining the future differs from analyzing the past, because it has not yet happened. In this article, methodologies have been used to discern useful alternatives to enhance the success of planners and leaders in their response to a range of possible future environments.

Managing the future means influencing it—creating, constraining and adapting to emerging trends and events in a way that optimizes the opportunities and minimizes the threats of relevance to the profession.

The views and conclusions expressed in the Command College Futures Project and journal article are those of the author, and are not necessarily those of the CA Commission on Peace Officer Standards and Training (POST).

© Copyright 2010
California Commission on Peace Officer Standards and Training

Can Law Enforcement Agencies Risk the Move to Cloud Computing Technology?

It's a simple question with profound consequences, and it is a question you had better be ready to answer. Imagine a technology that will save your department money. Imagine a technology that will increase your efficiency. Cloud Computing technology offers all of that and more. Now imagine a technology with dubious information security. Imagine a technology that could destroy the public's faith in your department. Cloud Computing technology offers that as well. And finally, imagine a roadmap that will assist you on your journey to the clouds. A process to help you achieve the benefits of Cloud Computing while shielding you from the dangers. Find that path and you can succeed; miss that path and it could cost you dearly. So, can law enforcement agencies risk a move to Cloud Computing? Given the nature of the technology and the demands placed on the law enforcement profession, the answer to this question is yes, but success should be measured in public trust, not dollars and cents.

WHAT IS CLOUD COMPUTING

The Cloud referred to in Cloud Computing is the Internet. Typically, IT systems managers would symbolize the part of the network beyond the domain of the internal network as a "cloud". This created an easy-to-understand visual to explain to others the components that made up their IT network. The chart would show all pieces of the organization's system, and would depict the link to the external world as a cloud that represents the Internet (Stevenson 2009). Extending on the concept of the original cloud, in Cloud Computing, the organization would no longer need to maintain their current stand-alone IT systems.

A more technical definition is provided by The National Institute of Standards and Training (NIST), a division of the U. S. Department of Commerce. The definition created by NIST describes Cloud Computing as a model to enable convenient, on-demand network access to a shared pool of configurable computing resources (Mell, Grace 2009). The U. S. Government's definition of Cloud Computing will undoubtedly carry influence over the entire industry; with an annual budget of over \$70 Billion, it is the largest IT consumer on the planet (Cohen 2009).

The organization that contracts for Cloud Computing services would be freed of most of its internal IT systems. There would be no need to house a complex system of servers and networking systems within the contracting organization. The only thing needed would be workstation computers (or portable computers) and a fast internet connection. All other IT equipment would be owned and maintained by the Cloud Service Provider (CSP) at their remote site (Thachappilly 2010).

NIST categorizes Cloud Computing into three separate categories: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). SaaS represents the highest level of dependency on the service provider; the CSP controls the network, servers, operating systems, and storage. In PaaS, the customer would have more control over some of the applications. In IaaS, the consumer would have control over the operating system, storage, deployed applications, possibly some of the network components (Cloud Security Alliance 2009). The consumer will be capable of selecting a service level that will optimize efficiency of their business while maintaining the level of control desired for peace of mind.

Many of the largest High-Tech companies are positioning themselves to be perceived as the leaders of this industry; including IBM, Microsoft, Google, Amazon, Rackspace, and EMC.

These companies are investing tremendous amounts of money to solidify their position in this market. The stakes are very high for the service providers and the need to establish credibility is essential given the expected growth of this technology. By some estimates, Cloud Computing will grow into a \$95 billion dollar market over the next five years (Bruening, Treacy 2009). Cost savings continue to be the main driver behind the interest in moving to Cloud Computing. The cost of transferring data over the Internet is falling, and businesses no longer want to be saddled with the cost and complications of managing hardware and software (Ricadela 2010).

BENEFITS OF CLOUD COMPUTING

The potential for substantial cost savings by using Cloud Computing technology is real. Economy of scale would allow the cloud service provider (CSP) to offer better IT capabilities to each customer while enabling the customer to realize a cost savings. In fact, maintaining multiple stand-alone systems is more expensive than maintaining one massive shared system. As Eric Roch explains in his article “Cloud Computing Economies of Scale”, CSP’s “are building massive data centers close to cheap power, abundant network bandwidth, and efficient cooling”. He further states, “...these huge investments will commoditize many computing problems and make applications unfeasible to competitively maintain them in your own data center.” (Roch 2010).

As an example of potential savings, the City of Los Angeles went to a CSP to administer the employee e-mail system. That limited move to Cloud Computing will save the City more than \$5 million dollars over five years and reduce the need for nine full-time city employees (Williams 2009). To further highlight the potential cost savings, Continuity Central published a survey conducted by Mimecast of 565 IT managers from the United States and Canada. Fifty-

four percent of the respondents listed cost savings as the primary motivation behind the adoption of Cloud Computing (Continuity Central 2010).

Cost savings are not the only potential benefit of Cloud Computing for law enforcement. Cloud Computing has the potential to maximize information sharing amongst regional law enforcement agencies. An agency could join a Community Cloud designed exclusively for policing agencies. Members of that dedicated cloud would have instant access to a shared database of information, thus enhancing the prospects of solving crime, distributing necessary intelligence and safety information, and improving the coordination of scarce field resources.

Crime series that generally affect large regional areas (e.g. burglaries, robberies, vehicle thefts, etc.) would be easier to identify and solve with the comprehensive database. This type of information sharing among a specialized field of interest is just getting established. The National Cancer Institute has set up the Cancer Biomedical Informatics Grid (caBIG) to allow researchers and doctors to instantly share and learn from data entered by any of the participating partners. “caBIG shows us a glimpse of the future in cloud computing, where the computing resources are a given and power is harnessed by having a powerful data-sharing framework” (Kirkwood 2010). Law enforcement agencies could likewise harness Cloud Computing. For instance, information gathered by a participating agency would be instantly available to all member agencies as just one example of the potential of this technology.

CONCERNS ABOUT CLOUD COMPUTING

The major concern with Cloud Computing is information security. In the Mimecast survey of IT managers, forty-six percent listed security concerns as the reason they have not yet moved part or all their operations to Cloud Computing (Continuity Central 2010). There may,

though, be some self-serving concerns amongst this group: The participants of this survey represent the IT staffs of their individual operations, and would be subject to reductions and or elimination if their organization were to migrate to Cloud Computing.

In a separate survey of 1,809 business and IT professionals conducted by the Information Systems Audit and Control Association (ISACA), forty-five percent of the respondents felt the risk of Cloud Computing outweighed the benefits (ISACA 2010). Their primary concern was a loss of direct control of individual IT networks when functions and data storage was moved to the Cloud. Instead, an organization would rely on a CSP to store its data, maintain its software, and perform systems upgrades and data back-up procedures. Again, this survey was conducted amongst those most likely to be negatively affected by their organizations decision to move to Cloud Computing. Surveys of end-users with regard to customer use and satisfaction, though, have yet to be done. So far, the most comprehensive surveys have targeted security concerns amongst IT managers. So are the concerns about Cloud Computing real, or is it just a new technology that threatens one that is established? It is probably a little of both.

One of the concerns about Cloud Computing is how the information is stored. An individual customer would have their data stored on a large computer which could also be hosting data and operating systems from many other entities. The data would only be separated by virtual barriers. These barriers are controlled by the virtualization-manager that is commonly called the hypervisor. There are concerns that a virus or other form of malware uploaded to the server from one user could compromise the hypervisor and affect the data of all entities sharing the same computer (NC State 2010).

Another concern with Cloud Computing is not knowing where the information is stored. Your data will no longer be in the IT closet at the station house, or at the City/County IT

manager's facility. As Robert Gellman of the World Privacy Forum illustrated in his paper titled Privacy in the Clouds, it is possible data could end up in another state or possibly another country. Knowing that information will be important should a dispute arise: Laws related to contracts vary widely based which court has jurisdiction (Gellman 2009).

To address these and other concerns, CSP's are scrambling to ensure their systems and security measures are reliable. To this end, a consortium of 24 service providers, vendors, and government entities are working together to establish a Common Assurance Metric (CAM) for the industry (Dubash 2010). According to Dubash, they hope to establish measurable and quantifiable security standards, which will make it easier for organizations to compare security standards amongst the various providers.

There are several groups working to identify best practices for organizations considering the move to Cloud Computing. One of the most reputable is the Cloud Security Alliance. In Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, editors Glenn Brunette and Rich Mogul point out that Cloud Computing is not more or less secure than the current environment. It is just a new technology that creates new risks and rewards (CSA Brunette, Mogul 2009).

So has the security of Cloud Computing reached an acceptable level? Can a law enforcement agency risk migrating to Cloud Computing? It is critical for Law enforcement agencies to maintain public trust. This is not a new concept; Sir Robert Peel included the importance for public trust in his nine principles of policing in 1829. He recognized then that the power of the police to fulfill their functions and duties was dependent upon public approval and support (Reith 1948). However, Cloud Computing technology is alluring. It offers cost savings at a time when many government agencies are struggling with budget reductions. It offers

increased efficiencies and the ability to access shared law enforcement databases. So the challenge is to find a way to achieve the benefits of Cloud Computing while mitigating the potential risks.

PATH TO SUCCESS

There are some essential steps an organization should take to mitigate the risks associated with Cloud Computing. Amongst the most critical are:

- The creation of a comprehensive Service Level Agreement (SLA) with the CSP. The SLA is the contract that will describe the services to be provided and the cost of those services. It will identify what is to be provided, who is to do it, where it will take place, what security assurances exist, and how disagreements are to be resolved. Some of the most significant risk of migrating to Cloud Computing can be controlled by a well-crafted SLA.
- Follow the recommendations of the Cloud Security Alliance, the World Privacy Forum, and other groups dedicated to identify best practices in the field of Cloud Computing and information security. The Cloud Computing industry is evolving. Standards and definitions are still fluid, so do not rely solely on the promises from individual CSP's. Research the technology and compare identified best practices with the services offered by prospective CSP's.
- Take gradual steps into the world of Cloud Computing. Identify less critical segments of your IT needs and consider moving those into the Cloud before committing all your IT needs. Los Angeles is an excellent example of this method. The move of e-mail to a CSP was done specifically because it was a low risk system as compared to other City-

wide computing and data-base needs. The City enjoyed some immediate cost reductions from this move while protecting other more critical systems from the associated risks of Cloud Computing.

- Monitor the transition to Cloud Computing. Demand that the CSP comply with the conditions set forth in the SLA. Make sure you have verification as to where your data and computing are being stored. It is critical to use a third party auditor to help monitor the service being provided by the CSP. The Cloud Security Alliance recommends using a “cloud aware” auditor to ensure they are familiar with cloud and virtualization challenges (Cloud Security Alliance 2009).
- Include the public in the transition process. Public discussions should be held prior to this transition. It is the public’s personal information that will be at risk while stored on the cloud. They have a right to understand the transition and offer input to the process. The World Privacy Forum recommends that citizens be made third party beneficiaries of the contract. This would allow harmed citizens to sue the CSP for security violations, lessening the exposure of the contracting law enforcement agency (Gellman 2009).

CONCLUSION

Cloud Computing technology is with us. Maybe you have not heard of it yet. Maybe you have not given it any consideration. Never the less, it is here and you had better be prepared to answer a few questions about the technology and its relationship with your organization. What will Cloud Computing mean to your organization? Will it mean cost savings and greater efficiency? Or will it mean a breach in data security that damages your organization’s reputation? They are simple questions with profound implications. Fortunately, there is a path

you can navigate that will avail your organization of the benefits of Cloud Computing while mitigating your exposure to potential risks. Follow it into the Cloud; that is where the future is.

Bibliography

- Cloud Computing Adoption: Survey Results (02/05/2010). Retrieved 03/27/2010, from: <http://www.continuitycentral.com/news04991.html>
- Cloud Security Guidance for Critical Areas of Focus in Cloud Computing V2.1. 2009. Cloud Security Alliance. www.cloudsecurityalliance.org/guidance/csaguide.v2.pdf
- Cohen, R. (04-20-2009). “The U.S. Federal Government Defines Cloud Computing”. www.sys-con.com. <http://cloudcomputing.sys-con.com/node/954002/print>
- Dubash, M. (02-09-2010). “Group Aims to Set Standard for Cloud Security”. ZDNet.co.uk <http://www.zdnet.co.uk/>.
<http://news.zdnet.co.uk/itmanagement/0,1000000308,40032011,00.htm>
- Gellman, R. (02/23/2009). “Privacy in the Clouds: Risk to privacy and confidentiality from Cloud Computing”. Retrieved 03/25/2009, from: <http://www.worldprivacyforum.org>
- Kirkwood, M. (01/27/2010). “Extraordinary Measures: Computing in the Cloud for Cancer.” Retrieved 05/11/2010, from: <http://www.readriteweb.com/cloud/2010/01/cloudcancer.php>
- Mell, P. and Grance, T. (06-01-2009) Draft NIST Working Definition of Cloud Computing. National Institute of Standards and Technology. <http://www.csrc.nist.gov>
- North Carolina State University (05/03/2010). New research offers security for virtualization, cloud computing. *ScienceDaily*. Retrieved May 12, 2010, from: <http://www.sciencedaily.com/releases/2010/04/100427111259.htm>
- Ricadela, A. (04/29/2010). “Amazon Looks to Widen Lead in Cloud Computing”. Retrieved 05/19/2010, from: <http://www.msnbc.msn.com/id/36849177/ns/businessbusinessweekcom/>
- Roch, E. (02/16/2010) “Cloud Computing Economies of Scale”. Retrieved 05/19/2010, from: <http://it.toolbox.com/blogs/the-soa-blog/cloud-computing-economies-of-scale-36954>
- Stevenson, D. (03-20-2009). “What is Cloud Computing?” Message posted to <http://it.toolbox.com/blogs/original-thinking/what-is-cloud-computing-a-simple-definition-30648>

Strickland, J. (04/08/2008). "How Cloud Computing Works". Retrieved 05/05/2010, from:
<http://communication.howstuffworks.com/cloud-computing.htm>

Thachappilly, G. (05/07/2010). "Cloud Computing has Significance for Management and Environment". Retrieved 05/19/2010, from:
<http://businessmanagement.suite101.com/article.cfm/cloud-computing-has-significance-for-management-and-environment>

Williams, M. (10/27/2009). Los Angeles City Council Approves Google E-Mail Plan.
Retrieved 03/12/2010, from: <http://www.govtech.com/gt/732223>