

DISPATCHERS IN THE CLOUDS

by

Marc Shaw
California Highway Patrol

April, 2012

COMMAND COLLEGE CLASS 50

The Command College Futures Professional Article is a 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 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 professional article are those of the author, and are not necessarily those of the CA Commission on Peace Officer Standards and Training (POST).

DISPATCHERS IN THE CLOUDS

Visualize a state-of-the-art public safety communications center in the near future. The center is located in northern California, filled with workstations and dispatchers. Suddenly, a major catastrophe occurs in the vacant field next to the building; within minutes, flames and toxic fumes quickly begin to impact the center. Without hesitation, all network traffic, including wireless and hardline 9-1-1 calls, allied agency lines, and radio traffic are all re-routed to a center in San Diego. Minutes later, a call comes in from a frantic mother whose vehicle is disabled in the middle of Interstate 80. Her three kids are with her and they are scared. Her eldest son is having trouble breathing and is in need of medical attention. Unfortunately, the woman is from Ohio and has no idea where she is. The dispatcher quickly obtains the latitude and longitude from the emergency call, which then registers on an interactive Geographic Information Systems (GIS) mapping application. Immediately, the closest paramedic unit is identified through the use of an automated vehicle locator (AVL) system and global positioning satellite (GPS) technology. Seconds later, medical help is on the way along with a tow truck from a local provider and an officer from the Highway Patrol. Once the fire department personnel arrive on scene, they radio for an additional ambulance and provide updated information to the hospital. Remember, the dispatcher is in San Diego – over 500 miles away! Through the use of Radio over Internet Protocol (RoIP) technology, the distance is no longer an issue.

Nearly all of the technologies mentioned above already exist. What is missing is the implementation of some of the ideas and the confluence of a few key trends and events to drive the implementation and adoption of the rest. The future model of law enforcement communications centers is on the verge of a paradigm shift, one which will vastly change the way dispatching services are provided. In the near future, your communications center will

likely integrate cloud-based technology. To take advantage of the cloud for emergency communications, though, we must first understand the long-term benefits of cloud-based communications centers, have clarity regarding options for deployment, and work to obtain the tools necessary for the future.

THE CLOUD

Although less-refined forms of cloud-based computing, such as IBM's "on-demand" computing have existed since 2003, the actual "cloud" came to fruition in 2006 when Amazon and Microsoft afforded companies the opportunity to store data on their underutilized data servers.¹ The mainstream launch of "Google docs"² in January 2010 and Apple's "iCloud"³ in June 2011, though, caused the popularity of the cloud to explode. With more and more people coming in contact with some form of cloud computing, user acceptance is on the rise. While delivering a keynote speech on February 14, 2012, Apple CEO Tim Cook said there were over 100 million people using their iCloud service. Perhaps more intriguing is the fact that Apple gained approximately 15 million new users in just 21 days – an increase of more than 17%.⁴ In its simplest form, cloud computing is "shared services."⁵ End users are able to access applications, services and files from a variety of remote platforms (e.g., the cloud), including desktop and laptop computers, tablets, smartphones and other small form devices.

¹ Walker, Joseph. (2012, January 31). Retrieved March 12, 2012, from <http://www.collegeofcontent.com/Art/20999/32/So-How-Did-Cloud-Computing-Start-Anyway.html>

² Google Docs. (2012, March 6). In *Wikipedia, The Free Encyclopedia*. Retrieved March 11, 2012, from http://en.wikipedia.org/w/index.php?title=Google_Docs&oldid=480508703

³ iCloud. (2012, March 10). In *Wikipedia, The Free Encyclopedia*. Retrieved March 11, 2012, from <http://en.wikipedia.org/w/index.php?title=iCloud&oldid=481230025>

⁴ Panzarion, Matthew. (2012, February 14). Retrieved March 8, 2012, from <http://thenextweb.com/apple/2012/02/14/apples-tim-cook-announces-that-there-are-now-over-100m-icloud-users-marking-15m-user-growth-in-21-days>

⁵ Cloud computing. (2012, February 23). In *Wikipedia, The Free Encyclopedia*. Retrieved February 21, 2012, from http://en.wikipedia.org/w/index.php?title=Cloud_computing&oldid=478497072

Today, concepts like Infrastructure as a Service (IAAS) and Platforms as a Service (PAAS) allow agencies to move the information technology responsibilities outside of the Department to companies that specialize in that line of work. This affords them the ability to focus on their core mission – public safety – rather than on upgrading virus-prone software and procuring the latest hardware. Memory hungry software that was once loaded onto individual machines has become a thing of the past; the need for large server rooms requiring constant attention decreases each day. For example, if an agency wants to launch a new records management system, they have the option to work with a vendor who will design a web-based interface to meet their needs. Agency personnel would then enter the data from any computer with access to the Internet; all information will be stored on an off-site server managed by the vendor.

The vendor is ultimately responsible to secure and maintain the data, ensuring the servers are constantly updated with the latest virus protection and software updates, and making any design modifications or output changes requested by the agency. If the agency selects a records management system that already exists, it can quickly implement it by utilizing the cloud infrastructure without having to acquire significant hardware. This substantially lowers both time and cost barriers to deployment.⁶ Ultimately, cloud computing offers the government an opportunity to be more efficient, agile, and innovative through more effective use of IT investments.

A COMMON PLATFORM

⁶ Kundra, Vivek. (2010, December). *25 Point Implementation Plan to Reform Federal IT Management*. Washington, DC: U.S. Government Printing Office.

While many of the cutting-edge technologies needed to create cloud-based consolidated communications centers exist (or are on the cusp of existing) it is imperative that a common standard for radio and voice protocols be developed to create a level playing field for agencies seeking to transition to a cloud-based model. As an example, in 1989, Project 25 (P25) was initiated by public safety agencies and manufacturers in the United States. The purpose of P25 was to address the inability of first responders to communicate with one another, which negatively impacted coordinated response efforts, increased response times, and compromised officer safety. P25 addressed the need for common digital public safety radio communications standards for First Responders and Homeland Security/Emergency Response professionals. New initiatives, similar to Project 25, should be drafted to ensure all manufacturers develop products along a common platform, which will allow them to be integrated into a variety of applications.

As the dispatch center business process is re-engineered to coincide with cloud-based options, it should also provide commonalities that will allow for implementation of P25 protocols on a variety of scales based on the size and scope of the organization. Using the California Highway Patrol as an example, 25 communications centers are scattered across the State. Some are housed in undersized patrol stations, while others are modern standalone facilities responsible for large geographic regions. Many of the smaller centers are grossly inadequate and due for replacement. Given the current economic climate, however, funding replacements for the 20 outdated centers is certainly unlikely. Integrating a cloud-based model opens a number of possibilities.

Using the cloud, the CHP could establish a few large communications centers to manage communications for sizeable geographic regions, aligned with the eight field divisions that

currently exist within the CHP structure. Another possibility would be to construct two or three “mega-centers” and position them throughout the state. In essence, these facilities could be large call centers, with several hundred calltakers, each responsible for the various dispatch functions. Of course, during the initial design phase, thought should be given to whether other state agencies would be interested in participating in the consolidation. The economy of scale for such mega-projects could once again enhance the fiscal savings across State departments. In fact, as these projects are deployed, they could either contract for services to local agencies, or serve as a model for local county or regional government entities to replicate for their service populations.

IS IT SECURE

Public and private clouds exist, and clearly, for law enforcement purposes, agency directors must ensure the clouds they utilize will maintain the integrity of the data stored there. In 2002, the Federal Government established the Federal Information Security Management Act (FISMA), which established strict information security protocols.⁷ Initially, many public safety agency directors felt physical control of their data was a necessity, meaning data servers must be at a secure location, such as their police station. The public sector, though, has embraced the need for secure cloud space and created specific segments that meet the FISMA standards, such as, Google Apps for Government, which provides segregated systems for US government customers and the data is stored exclusively in the United States.⁸

⁷ Federal Information Security Management Act of 2002. (2012, March 6). In *Wikipedia, The Free Encyclopedia*. Retrieved 19:03, March 11, 2012, from http://en.wikipedia.org/w/index.php?title=Federal_Information_Security_Management_Act_of_2002&oldid=480447665

⁸ Google. Retrieved March 10, 2012, from <http://www.google.com/apps/intl/en/government/trust.html>

In conjunction with FISMA, the development of appropriate security protocols must be developed to ensure that sensitive data cannot be compromised. In response, Federal Chief Information Officer Steven VanRoekel said in 2011 that the White House's Office of Management and Budget (OMB) would launch the Federal Risk and Authorization Management Program (FedRAMP), a unified government-wide risk management initiative focused on providing security for cloud-based systems. The program offers a standard approach to conduct security assessments of cloud systems based on an accepted set of baseline controls and consistent processes vetted and agreed upon by agencies across the federal government. He added that "as the government migrates to the cloud, we are committed to doing so in a way that is cost effective and ensures the safety, security and reliability of our data. To date, each federal agency has gone through multiple steps that take anywhere from six to 18 months and countless man hours to properly assess and authorize the security of a system before it grants authority to transition to the cloud."⁹

In what is perhaps the most compelling evidence of confidence in the security of the cloud, in December 2010, the Office of Management and Budget in Washington DC declared that government now operates under a cloud-first policy. This means that agencies must first try to incorporate some type of cloud computing into each IT project under consideration.¹⁰ With that in mind, it is apparent that the level of support is increasing and should continue to expand, provided appropriate levels of security are incorporated. In an interview with Nicholas Popp, vice president of product management and development at Symantec, he acknowledged the cloud is not quite up to par with on-premise installations when it comes to security. He predicted

⁹ Higgins, John. (2011, December 13). Feds Aim to Lock Down the Cloud. *Technology News World*, Retrieved March 1, 2012, from <http://www.technewsworld.com/story/73956.html>

¹⁰ Unknown. (2011). When the Cloud Makes Sense. *Federal Computer Week*, Retrieved March 3, 2011, from <http://fcw.com/DownloadingCloudComputing>

within three to five years, though, the cloud will be the more secure environment for small and mid-sized businesses.¹¹ Additionally, according to David McClure, associate administrator for the Office of Citizen Services and Innovative Technologies at the General Services Administration said, "FedRAMP will evolve as a program to reflect the changing nature of cloud computing and incorporate lessons learned. As cloud computing, standards and capabilities evolve, so will FedRAMP." McClure also noted that a joint authorization board (JAB) would be established to define and update FedRAMP security standards.¹² Cloud computing has the potential to play a major part in addressing inefficiencies in government, improving government service delivery, and saving money.

WHY NOW?

Investing capital during the current economic downturn, to provide a funding mechanism for upgraded communications infrastructure in the future, will position agencies to transition to the communications needs of the future. According to the Federal Cloud Computing Strategy¹³, an estimated \$20 billion of the federal government's \$80 billion in IT spending is a potential target for migration to cloud computing solutions. Funding sources should be identified immediately, and planning models must ensure that infrastructure improvements are aligned with a model of consolidated, cloud-based communications centers. Some states may be able to utilize 9-1-1 funding streams for this purpose, particularly with the incorporation of Next Generation 9-1-1 technology. Others may find the ability to implement local taxes or surcharges as more direct means of obtaining one-time funding to cover initial construction costs.

¹¹ Olavsrud, Thor. (2012, February 17). Security in the Cloud Is All About Visibility and Control. *Network World*, Retrieved February 18, 2012, from <http://www.networkworld.com/research/2012/021812-security-in-the-cloud-is-256332.html?page=3>

¹² Higgins, John. (2011, December 13). Feds Aim to Lock Down the Cloud. *Technology News World*, Retrieved March 1, 2012, from <http://www.technewsworld.com/story/73956.html>

¹³ Kundra, Vivek. (2011, February). *Federal Cloud Computing Strategy*. Washington, DC: U.S. Government Printing Office.

In California, the State government allows departments to buy directly from suppliers through pre-existing contracts and agreements known as Leveraged Procurement Agreements (<http://www.dgs.ca.gov/pd/Programs/Leveraged.aspx>). Shared acquisition or leveraged procurement with other public safety entities within the region will help ensure system compatibilities and competitive pricing and may shorten the procurement cycle. Finally, by making the transition to a virtual communications environment, centers that experience spikes in call volume or workload due to significant emergency incidents, lengthy large-scale events, or even long-term staffing shortages, would have the ability to distribute their workload among other dispatch centers. In turn, the public would not see a decline in the level of customer service and the operating costs for the public safety agency would likely remain unchanged.

CONCLUSION

Ask yourself the question “Is it time to move our dispatch operations to the cloud and consolidate within our own agency, or possibly with other public safety providers?” Most of the technological capabilities either exist, or will exist in the very near future. The security concerns have been addressed and solutions identified. What remains is the cultural mindset of “this is how we have always done it.” With the emergence of a secure, reliable Cloud, you are presented with the opportunity to radically alter and improve the system, save a considerable amount of money in the long-run, have a positive impact on the environment and increase the overall efficiency of your dispatch operations. Are you ready? No matter the size or type of your agency, implementation of a cloud-based system, on some scale, should be an option for you. Understand it. Accept it. Embrace it. The cloud is here and it is going to change the way we do business.