IACP 2012

Law Enforcement in the Age of Cloud Computing

How the Cloud is Revolutionizing the Way Agencies Manage their Digital Evidence

IACP 2012

This IACP 2012 program focused on cloud computing and how it relates to law enforcement. Leading visionaries in law enforcement shared their thoughts on the cloud, how they've used it, and their insights about the technology revolution that is on your door step.

This paper provides the basic transcript of the panel presentation in a readable format.

119th Annual International Association of Chiefs of Police Conference
and Law Enforcement Education and Technology Exposition
10/1/2012

Table of Conents

Introduction

This IACP 2012 program focused on cloud computing and how it relates to law enforcement. Leading visionaries in law enforcement taught about the cloud, how they've used it, and their insights about the technology revolution that is on your door step.

Speakers

Richard Beary	Robert Davis	Jeffrey Halstead	Frank Milstead
Hadi Partovi	Rick Smith	Tom Streicher	Keith Trippie

IACP 2012 exposed a trending change in law enforcement technology: Using "the cloud." IACP 2012 brought together thought leaders across all areas of Law Enforcement. This year the event showcased 783 Exhibiting companies. Over 14,000 people attended the 5 day conference. A panel of six law enforcement leaders and two cloud technology leaders examined exactly how the cloud revolutionizes the way agencies manage their digital evidence.

The Old Model is Frustrating. Major city Chiefs told stories about trying to advance their departments' technology. Their results were all frustratingly similar. Their agencies spent millions of dollars and years of resources on the development of tailor-made systems. Most of the time, these systems never even went live. In an age of constrained city budgets and forced labor freezes in many agencies, throwing away millions of dollars on a tech system is more than most can stomach.

If nothing else, take a lesson from Tom Streicher. His agency invested $15M and over a decade of time into a system that never went live. That is a horror story worthy of being told around a campfire. Don't build! Leverage systems already built, and stay within your budget.

The New Model Works for Law Enforcement. These law enforcement leaders point to the same answer. Agencies need to focus on their priorities: protecting the innocent and catching the bad guys. IT should be the last thing agencies worry about. Their solution? The cloud.

Use the Cloud. Stay Focused on Law Enforcement. These thought-leaders and authority figures all came to the same conclusion. The cloud is good for law enforcement. These men know from experience that their agency is much better at policing than at developing IT systems. Keep focusing on protecting your community. Let IT vendors provide systems for you. Don't become a digital storage office. Become a cloud office. You'll be up-and-running faster, your costs will be fixed, and your officers can stay out on patrol, doing what they were trained to do.

Now, the experts tell their stories. Their thoughts on cloud computing are detailed below.

Main Discussion

Keith Trippie
Executive Director for the Enterprise System Development Office (ESDO), within Office of the Chief Information Officer (OCIO) of the Department of Homeland Security (DHS)

I wanted to start off with a few things that I don't know. What's the number of officers that are required to work a multi-jurisdictional drug task force? How do you justify overtime costs to local politicians? How do you manage the media after an officer involved shooting? Those are things I don't know.

The following three things are things that I do know. I know what the change control process is for a zero day security patch. I know how to troubleshoot a system when it goes down. I know the best three tiered architecture for an RMS system with 500 users. If you're spending a lot of time on these last three items, it's taking time away from leading your organization.

I have three primary responsibilities at the department. I oversee the department's cloud strategy, records management function, as well as Enterprise Applications and Services. I'm excited to be here today with leadership from the state and local law enforcement communities from across the country.

Gartner

According to Gartner, which is a leading information technology research and advisory company, cloud services worldwide have grown to $109 billion at the end of this year, up 20% from last year. And by the end of 2014 it could be up as high as $150 billion.

This past year has been a good one for cloud. According to Gartner, which is a leading information technology research and advisory company, **cloud services worldwide have grown to $109 billion at the end of this year, up 20% from last year. And by the end of 2014 it could be up as high as $150 billion.** Your friends and families store pictures in the cloud, you have buddies that store their favorite Rolling Stones songs in the cloud, you have work associates who store email and want to store their RMS in the

cloud. You've seen the commercials on the TV and you've heard the hype.

Disruptive Change of Cloud Computing. Let me explain what cloud is and why it's so important. The legacy IT model that we have as part of our DNA over the past 20 years must evolve to meet the growing needs of the customers within a budget- constrained environment. The traditional model is not well positioned to do that.

You buy assets, you buy some techies, and then hopefully over 12 or 24 months, magic happens. That model has proven not successful for a lot of us in this room, myself included. It also introduces a higher level of risk due to the different security concerns out there. Think of it this way: if you have a bank with 20 different entrances, you've got a guard 20 different entrances. If you can reduce that footprint, maybe you have two doors to guard. You can channel your energy and security around those two points of entry.

Anybody out there work with vendors who have proprietary applications? Any of them share information real well with some of the others? Any of them cheap to migrate away from? These are the same challenges we have at DHS and in the federal space. Fortunately we are experiencing an evolutionary change in the way that we deliver IT. This transformation is replacing the legacy IT model.

The White House issued the 25 point implementation plan, which authorizes a cloud-first policy. That's a memo that I can get onboard with. So we've got to make adjustments to how we deliver IT.

The cloud in and of itself is a consumption-based business model. It's framed around outsourcing. Much like the private sector would outsource their payroll or logistic services, the cloud offers government the ability to outsource traditional IT. We do not advocate the responsibility and oversight of securing the data, but the day to day management of the servers, and how many gerbils it takes to run them. We will retain the oversight for securing the data.

The cloud in and of itself is a consumption-based business model. It's framed around outsourcing. Much like the private sector would outsource their payroll or logistic services, the cloud offers government the ability to outsource traditional IT. We do not advocate the responsibility and oversight of securing the data, but the day to day management of the servers, and how many gerbils it takes to run them. We will retain the oversight for securing the data.

In this model, agencies can go to service providers to require pre-built services. All of us have gone through the scenario where we had to build something from scratch. That's a painful business model to go through. The capital that it takes is going to be very tough for those in this room to try to meet. NIST, which is The National Institute of Standards and Technologies, provides the following definition of cloud computing:

"Cloud computing is a model for enabling convenient on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management, effort, or service provider interaction."

That's a really complicated way of saying "the same way you buy electricity today." Or, "the same way you buy cable." Anybody care how Tony Soprano gets to your television? Probably not. You care that it does, and you want to know exactly how much you're paying per month. This is a proven model in other sectors, and finally it's coming to IT.

On-demand service. This is how consumers in this room can unilaterally envision computing capabilities, whether it's a new server, or licensing a new RMS user automatically without human interaction.

Resource pooling. Resources are pooled so multiple customers are leveraging the same offering. Think buying a condo versus building your own house from scratch. You buy the condo, you're moving in the next day. You go build a house from scratch, 12 months later maybe you move in. Maybe it's what you wanted, but you probably paid a little bit more than what you were budgeting.

Rapid elasticity. Capabilities that can be rapidly provisioned to quickly scale out and then scale back in when you don't need them. That's how Amazon Web Services got started. Twelve months out of the year they had a big infrastructure to support three months out of the year when everybody went to the website and started ordering CDs and books. Nine months out of the year they were getting no value out of that server space. They said, "How do we reuse that?" So they came up with this newer business model. Think about it in your world. You've got a joint task force where you've got to add hundreds of users in a short amount of time. You work that for three or four months. At the end of the three or four months, it would be nice to not have to pay for that anymore. This newer model gives you the flexibility to scale up and scale back down. To me, in a financially austere world, scaling back down is almost as important as being able to scale up.

And finally, **measured service.** You know exactly what you're paying for. You know what it's going to be before you buy it, you know what it's going to be as you're buying it, and then when the bill comes at the end of the month you know exactly what you've paid. That is totally different than the way we've done IT for 20 years, at least in the federal experience. I'm sure that's probably pretty consistent out in the state and local as well.

NIST identifies three different types of cloud services. There's **infrastructure:** think server stuff - network. Then there's the **platform:** think things like databases. Up at the top tier is really where I want to spend some today: **software-as-a-service**. Think about the fun you've had managing your RMS capability, whether you built one, whether you inherited one, or whether you tried to get off of one and go to another one. Just have that in the back of your mind while I'm talking about software-as-a-service.

Software-as-a-Service (SaaS)

Software-as-a-Service. With **software-as-a-service**, the service provider's applications are running on a cloud infrastructure. The consumer does not manage or control any of that infrastructure. Deploying IT is not cheap, it's not easy, it takes time away from your operational focus, and it's not your core responsibility.

IT, when done right, is like referees in a football game. When done right you don't know they're there. But for the first three weeks of this season you felt them. You knew they were there, and it didn't feel right. That's IT done poorly. Cloud can be the new referees coming back.

One of the things that you've got to consider is standardization. It's going to be very hard to get from where you are today to where you want to go in a budget-constrained future if you're not willing to standardize some of your business processes. That's harder than it sounds, but whether you're in the federal space, private sector, or state and local, it's all the same. Are you willing to go with an 80% solution and change your business process to save 10%, 20%, or 30% a year? If you do that you can use the money you were spending on IT to go hire more officers.

NIST identifies three primary deployment models which are generally accepted across government. These range from models that are more secure to those that are more available. Government agencies will employ these models using a risk based decision process.

Private cloud. The private cloud infrastructure is operated solely for an organization, maybe managed by an organization or a third party and may exist on premise or off premise.

Community model. I think this one is going to be really interesting for this community over the next three to four years. This infrastructure is shared by multiple organizations and supports a specific community. This community may share mission data, processes, users, people, or compliance requirements. As security standards mature I would expect that more offerings will be made available to federal, state, and local officials.

Public cloud. While the public cloud may not be a primary focus for many of you in this room, the infrastructure is available and it's where the public would come get services from Fed, state, and local agencies. At DHS we have one primary public cloud provider for our less sensitive data. While this offering is not at the same sensitivity level that most of you may need I would recommend you consider these offerings in the public cloud for any data that isn't as sensitive as typical law enforcement data. Go to www.dhs.gov, www.fema.gov, TSA, or www.ready.gov. Those are websites that are already out there in this thing we call the public cloud.

Currently at the department we're focused on two of these offerings: the **private cloud** and the **public cloud**. We've made those decisions based on the level of sensitivity of our data.

The DHS is moving to cloud for some reasons in addition to complying with the **White House Cloud first Policy** and their recent digital government policy. We look at cloud capabilities to address financial constraints and operational needs to reduce time-to-market for new services. Everybody has probably got an RMS horror story that something was supposed to take six to twelve months, and instead it took two, three, four, maybe ten years to get deployed. A cloud model enables components that are inside the department. Think TSA, CBP, ICE and others. Instead of standing up their own capabilities they can leverage services that are already pre-built. (AKA software-as-a-service)

"Don't spend the capital" is what I'm out communicating with leadership across the different components. Don't go out and spend the capital on IT. Just pay $10 a month or whatever it's going to cost for a particular service offering. Take the saved money and invest it back in the mission. Go buy Jeeps, bullets, and guns, and all of the other things that it takes to help the Department of Security do its mission. Over the past 18 months we've seen savings on average 8%-10%. In some areas it's 30-40%. It depends on your model and your legacy costs.

Email Services

One of the first services is **email**. Today the GSA, The General Services Administration, has awarded a federal contract so state and locals can use 17 different vendors providing records management, email, archiving, and other solutions. It is pre-built. You don't have to go out and spend the capital on developing it. It's a very interesting alternative to the current model of doing IT in the public sector.

Collaboration Services

We've deployed **collaboration services** at the department. We have over 30,000 users collaborating and sharing information across the department. I paid $0.00 to start that service up. Each user pays $3.50 a month. At 10,000 users you're looking at $400,000 a year for 10,000 users to share information in real time, and I paid $0.00 to start it up. That's a powerful change from the old business model.

Mobile Workforce

DHS is deploying a service that supports a mobile workforce. This will allow our folks across DHS to go anywhere and get online with a laptop or desktop. Then they will connect to DHS back-end services. Can't do that today. This is where we're moving the department in the future.

Case Management

We've recently deployed relationship management, and that's one we're really excited about. It's a Microsoft-based solution, and again, we have paid $0.00 to start that service up. We're using that today. We're partnering with the folks at ICE that will be using it for a Litigation Case Management System to replace their current system. We're also using it to do regulatory tracking. We're using it for FOIA. We're going to be using it for correspondence tracking. Those services are coming online to you in the near future, and obviously Case Management is a big deal.

HSIN | Homeland Security Information Network

〈 NIEM 〉

I'd be remiss if I didn't talk about the **Homeland Security Information Network**, or HSIN. That's our primary information sharing platform at the SBU, or Sensitive but Unclassified level. This platform today supports about 10,000 to 15,000 users on a regular basis across fed, state, and local. This capability is available via the internet and has a strong identify management component that supports the **National Information Exchange Model**. HISN supports the federated approach to information sharing and I think that this is important to those in the room for a couple of reasons.

First, **identity**. An officer sharing sensitive information needs to know you are who you say you are. With a single identity and a trusted federation, a member is provided with cross-mission access to many different information systems. Without having to login 10 different times. No Post-It notes all up and down the side of your computer with different passwords to get into these systems.

And finally **mission support**. This one is kind of cool. Everybody knows what Google does. The concept of having a federated search capability will allow people to go in a nice neat little box, type in a query, and it's able to go out and hit all these discs for data sets and bring back the information. The only way to do that is if we all agree that we're going to standardize and share information across our different boundaries. Proprietary systems don't help us do that.

HISN is in the process of establishing an information exchange criteria within The National Information Exchange Federation to combat multi-jurisdictional criminal activities and support investigations in the Southwest and Southeast regional intelligence centers. Consistently used language will be managed so those end users have repeatable searches and find information more easily.

We have three things going on in the public cloud. They are involved in mitigating cyber threats across the department. There's the group out there called ANON that likes to come in and visit. They're very interested in law enforcement agencies. They visit us multiple times, but we have a cloud service that's in place today that mitigates that risk completely. In 2009, about three years ago, our friends from the Far East hit us with 100 fold DOS attack on www.dhs.gov. The service would have gone offline.

You can think, "Well it's just a public facing app," but when you're talking about public credibility, you do not want that application going offline. There are bad guys that want to take you offline to damage your credibility or cause other cyber risks to your organization. It's important that you consider a content delivery service that will help shield you from those attacks.

And finally another growing capability in this cloud space is **mobile services**. Who would have thought 10 years ago that a plate of glass would bring you the latest information on a B&E? These facts are changing the way your workers work. It's affecting the way college students are being educated, and it's changing the way that we provide real time information during incidents.

Mobile is changing the time gap paradigm for consumers from an "I wish I had that" to "I have that." Netflix, Amazon, iTunes, and others, they figured that out. Mobile is actually out there today and the cloud is going to be deploying more and more mobile services.

Risk management. That is a concern, and it has to be part of the tradeoff discussions when you're considering moving into the cloud. In a network and digital age, the confidentiality of law enforcement data, medical, financial records or others must be

carefully measured. Privacy is one area that the government must continue to monitor closely. We cannot simply forget to protect this type of data in a rush to provide consumer driven services. Rather we must find creative ways to preserve those protections while leveraging the benefits of this new disruptive change in the marketplace.

With a cloud-based service or traditionally hosted IT, first and foremost security and protection of the data is a big deal. Cybercrimes and threats are on the rise, and those threats aren't just centered on high profile organization such as DHS or banks. Every day the bad guys are plotting creative ways to exploit weaknesses in our collective IT network. They do this for financial, criminal, or terrorist gains. The key is for us to make sure that we're protecting our data and making sure that we're delivering services out to our folks out in the field.

Over the past year several standards have emerged that I wanted to make you aware of and to consider including FedRAMP, which is the Federal Risk and Authorization Program. This is chaired by the Department of Homeland Security, my boss, CIO Richard Spires, the DOD CIO, as well as the CIO from GSA. They oversee a program that is establishing a set of federal standards within the federal government that we're hoping state and locals can leverage as well. We are bringing everybody up to a common standard.

While we in government face challenges to successfully implement cloud capabilities to enhance mission performance and realize cost efficiencies, the benefits far outweigh the challenges. Already in the DHS, we're seeing reduced time-to-market for new services. While outsourcing the day-to-day IT capabilities, the cloud may seem like a foreign concept to some of you today.

I don't think of the cloud as simply a technology opportunity. It is a far more interesting discourse and a disruptive change to the fundamental business model for how IT is delivered.

Robert Davis
Senior Vice-President and Managing Director
of West Coast Operations and Senior Leadership Council
Hillard Heintze of Chicago

Rob Davis has served for over 30 years at the San Jose, California Police Department. He served his last seven years as the Chief of Police. During his tenure, Chief Davis was widely recognized as being an innovative law enforcement leader who saw the importance of leveraging technology whenever possible to prevent or reduce crime in real time.

Some of his accomplishments and innovative approaches include deploying mobile fingerprinting devices, allowing for the electronic capture of digital fingerprints in the field. His was one of the first major cities in the nation to issue electronic restraint devices to all field personnel. And finally, as the former President of the Major Cities Chief Association, he helped lead the successful effort to ensure national public safety broadband network.

Rob Davis: Our opportunity here is to speak in language most common to us as cops. We're going to cut to the chase.

In order to do that I'd like to paint a picture from my own background: some of the experiences we had in San Jose. San Jose is the third largest city in the State of California, it's the 10th largest city in the country. Most cities with .5M in population have about 2.6 officers per thousand residents. San Jose had 1.3 officers per thousand just over a year ago. Since I've left, we've dropped to 1.1. We continue to increase the size of our city, and we continue to decrease in the number of officers.

At San Jose we have had to use technology to leverage resources to be successful. Without using our crime data to figure out where to allocate our resources, we'd be sunk. We've tried to be very innovative over the years to accomplish that task. We have budget woes just like anybody else. I think a lot of times people will say, "The larger agencies can find the funds and the resources to fund those big projects. We can't do that if we're a smaller or mid-size agency." That's not necessarily true. The big cities are struggling just like everybody else.

We were able to establish San Jose as one of the safest big cities in the country. We've always been in the top three or four of those safest big cities, and several years running we've been the safest big city based on our crime statistics. But we accomplish that by being very savvy in how we used data.

We realized in San Jose that there was absolutely no way we could take advantage of that technology if we didn't use the cloud.

Let me take you back in the '80's and '90's as we really began ramping up our use of technology. We, like many other agencies, were doing it alone in many of our IT projects. For example, in the '90's we were still doing pen and paper police reports. We are still using paper and pen in several of our units to do our police reports. We knew we needed to automate this. We needed to get access to that crime data, not just for allocation resources, but also for our detectives.

Our department made a decision: we're going to customize a report running software program. The officers wanted the report writing system to let them do what they're currently doing, only in an automated fashion. So in other words, "we want the report on a screen to look like our report now." And every form you can think of that exists within your agency was supposed to be replicated digitally, so they didn't have to change their process. As you can imagine, that became a very clunky process.

That effort to automate report writing at San Jose, went on for years. I had become a captain back in '98. I got back from the National Academy and was tasked with the responsibility of taking over that project. I was trying to see if we couldn't get it back on track, and I will never forget the day I went to the first meeting with our outside vendors, the representatives, and a few other people from around the department who had been pushing this program. I'm a pretty optimistic guy. I see the world as pretty positive, I'm a "glass is ¾'s full" kind of guy.

When I walked into that room, you could cut the tension with a knife. I'd never met any one of these people. These outside vendors gave me looks like, "Here we go with another commander coming in here, trying to run this project that's years behind." It took a lot of effort to get that thing back on track, but I learned one thing from that process: **never ever customize your software again**. And we never did as I was Chief at the PD. We always said, "Where is there an off-the-shelf answer that will allow us to do the things we need to do?"

And here's why. Here are some of the reasons why I believe that to be true. **There are lower start-up costs. You're running almost immediately.** Basically all you're willing to do at some point is just train your people. I know you're going to get some pushback where people say, "but that doesn't look like our form. We have three steps to enter the data into the old system. You're suggesting four! The world is changing, this is horrible."

The bottom line is, at some point, you have to stand up and say, "We're going to change, and I need your help." It will become efficient. You sometimes have to just stand up and say, "We're going to do it this way." We also found that the responsibility for maintaining those products and services lies with the experts. I'm not pulling some tech-savvy Sergeant or Officer, somebody else from around the department to come in and run that program.

We were hired to be cops, not IT techs.

Also, what happens to your maintenance and your programs when all of a sudden those in-house experts transfer, or leave, or retire? All of a sudden, you're scrambling around. We had one officer that did a great job of helping us automate the entry of evidence into our evidence room. We actually created a barcode system. A little barcode on a sticker on a piece of evidence, and scan that into the system. He created that for us. He is no longer with the department. Who takes care of that software program? You get the idea.

Also, cops are more expensive than IT experts, at least they are in California, and that's one of the reasons we've had to make serious changes to our budget in California. You know as well as I do also that technology is ever changing. You invest in something that's your department-owned product, and what you've done is funded research and development for some outside vendor. You'll also have to turn right around and buy some additional technology to upgrade your system.

I've found that when you don't customize your data, that allows you to share your data more easily with more entries. I think we've all learned over the last decade why it's important to be able to share information with each other. Let me just give you one quick example of a successful way that we went about doing this. I had become Chief and we had just turned on a new Computer Aided Dispatch (CAD) system. It had all types of functions in it that were just really great for us. It allowed us to use our GPS devices in our cars to dispatch our officers to crime, based upon their location. We wanted to cut down our response times. **We couldn't turn it on. We didn't have the bandwidth to do that.**

We wanted to put electronic citation devices out in the field and automate that. We

couldn't do it because we didn't have the bandwidth. We wanted to put out the mobile identification units so we could actually take fingerprints in the field. So we said, "How do we do this?" Well, the experts said, "You need to build your own network. You need to get out there and buy some towers and create your system. And you can do it because you're the 10th largest city in the country." Well great, where's the money to do this? We started looking at the cost of doing it. It was millions of dollars. This was my first year as Chief. I thought, "There's no way I'm going to be able to go to my City Development Manager, and the ninth straight year of budget cuts, ask for tens of million dollars to build some network system."

Something else struck me. It seems rather obvious. I'm not a cell phone service. I'm not AT&T. I'm not Verizon. I'm not Sprint. Why in the world would I think that I'm going to be running some network? So instead, we went out and asked our commercial service providers in the area, "is there a way that we can lease or rent some space from you that's secure, and that will allow us to get bandwidth access and turn on these components of our CAD system and our records management system?"

We rent that for approximately $250,000 a year. Huge savings! And I don't worry about it. It's there. So we're starting to talk about how the cloud is kind of scary. You don't know where your data is going etc. Our job is to help you understand why that's not necessarily the case. It is not just the future.

We're looking at cloud computing as the future. We're there. It's the now!

It's just that more and more people are figuring out how to transition to it and learn how to take advantage of those capacities. So the bottom line is this: we live in an information age, and I guarantee you as the Chief in Silicon Valley, my constituents out there expect us to be savvy in terms of how we use technology and data.

Also, the generation is changing. Our new officers expect this type of information. You know there's a difference between the way they operate and the people who operated in the department before us. It's totally different. New officers like to work in groups. They have absolutely no problem sharing information. In fact, they share too much sometimes if you take a look at their Facebook page.

Sharing is not an issue for these people. They're expecting the ability and capacity to share information quickly and in real time. Also, our budgets are not going to allow us to go at it alone. We have got to figure out how to take advantage of the cloud and other such technologies to leverage our resources and our data at a lower cost. Learn how

cloud computing can be so very helpful to a law enforcement agency. Accessing and sharing critical information inside your department, as well as to those external partners at the local, state, and federal level, can be so very important.

We really don't have a choice. Our budgets are demanding that we share the information, that we get savvier. Cloud is one way to do it.

Chief Frank Milstead
Mesa Arizona Police Department

Chief Milstead was selected to lead the Mesa Police Department on March 22, 2010, after 25 years of service with the Phoenix Police Department. He currently leads a department of more than 1200 men and women, sworn and civilian, dedicated to providing exceptional service to the third largest city in Arizona.

He is leveraging his talents and resources within the department and its partners to make Mesa a safer city. And in December 2011 Forbes Magazine named Mesa Arizona the 7th safest city in the United States.

During his tenure with the Phoenix Police Department, Chief Milstead demonstrated highly successful leadership and management skills, and served in several high profile positions. This included command positions in the Homeland Defense Bureau, Major Offender Bureau, and the Traffic Bureau. Chief Milstead was also involved in several multi-agency high status cases, served in the unified command structure for Super Bowl 42, the 2009 NBA All-Star Games, and also maintains an All-Hazards-incident- Commander status.

Chief Milstead: You have to look at what's going on in the world and what's happening with cloud technology. Where are we seeing it start to proliferate in policing? **Are we seeing a migration of law enforcement information into the cloud computing environment today? I would tell you the answer to that is yes.** The moderator talked about our Homeland Security Information Network, HISN, that comprehensive, nationally secure, entrusted, web-based platform handles all types of Sensitive but Unclassified information for the law enforcement community.

The second thing you look at is The National Crime Information Resource Center. That's operated by the Bureau of Justice Administration for the purpose of providing a secure, web-based development to serve as a one-stop-shop for local, state, tribal, and federal law enforcement to keep us up-to-date on the latest developments in the field of criminal intelligence. Additional materials are there for law enforcement personnel through that National Crime Intelligent Resource Center.

www.opensource.gov is the United States Government's premier provider for foreign open source intelligence. It provides information on foreign, political, military, economic and technical issues beyond the usual media events or outlets that we see. It's an ever expanding universe for open source information. It actually contains information from 160 different countries.

And then what's kind of near and dear to us in the West, in Arizona, California, and Nevada, is COPLINK. COPLINK is our service provider for information sharing. It's an IBM sourced component. It's something that you subscribe to. We are now able to connect COPLINK to NavyLink. NavyLink is another very large system primarily used in the east, around the capital region, to provide information-sharing opportunities for law enforcement. But in proof of concept, we've connected COPLINK and NavyLink together to show that those two systems, albeit disparate, can work in harmony in a cloud based operation.

COPLINK providers are starting to provide information into N-DEx, which is the National Data Exchange, run by the FBI. As we continue to put information into N-DEx, which is nothing more than a data warehouse system for information sharing, that too will be based in the cloud.

We can't do the things we need to do at Mesa PD without leveraging cloud capabilities. We don't have the money. It's a pay-as-you-go system.

Even with our latest body-worn camera system. We provided those cameras to the officers, and to back that digital evidence up we use a cloud-based service where we pay by the gigabyte. We could have never done it on our own. Actually inside I'm laughing. I'm thinking of the City of Mesa internal politics. Our City IT is very difficult to work with, and our PD IT is so understaffed and overworked that there's no way we could have put the body-borne devices on our officers without leveraging the cloud.

Chief Jeffery Halstead
Fort Worth Police Department

As the former President of the Mesa Chiefs Association I had a chance to work with Chief Halstead, had several conversations with him and the thing I've appreciated about him is he's not afraid to speak up when he knows something is right and also to be thought leader within that Mesa City organization in terms of where we're going or where we need to be going.

He's the 24th Chief of Police for the Fort Worth Police Department, he was sworn into office on December 8th 2008 and he leads over 2,000 people within that community of 736,000 residents.

Chief Halstead: Let me just first make it very clear that I am not an "IT person" whatsoever. However, I am a Chief who is very frustrated with the lack of service and vision from my own internal IT service providers. So just a general question to all of you. Big city, small city, it does not really make a difference.

What is that you build? How many of you build your own cars? Your own guns? Your own uniforms? We do none of that, and the reason we don't do any of that is because there are experts that can do it and provide that product for us.

We have eight-year-old children in our school systems that are far more at ease working within the cloud than our organizations are, and that is the frustration that leaves me with some tense discussions with our IT service providers. If you have an internal IT department that actually serves for the Chief of Police within the administration - I found that to be a little better for my mission, but in conflict with the overall city mission. And then I found out in 2009, in our second round of budget cuts, that I lost my IT person within seconds of a city managers decision. I lost 100% of my IT services.

So then I had to get on a waiting list if I wanted any IT service or securities-type infrastructure systems delivered to me. That was through the external IT service

department within our city. I was competing with another city department. The police department is 1/3 of this city's budget. IT is a very small part of the city budget.

And then I thought to myself when I was dealing with the external IT department within our own city, "Who is it that they really hire?" Let's be honest with ourselves. The for-profit industry is going to attract your talent and your vision. We're going to get people who want the security of a job, and I don't know if they're going to have the same vision that we need to provide service to our citizens and keep our city safe. Lastly, in some of the projects that I had been dealing with, I was very concerned. We are advancing into on-officer camera systems. I'm telling you right now, your external IT department that's in the city is going to beg you not to use an external provider.

But I'm telling you, the product they deliver will be crap, and I'm just going to be very honest with you.

It is not going to be secure. Your district attorney is going to be frustrated that there is an external civilian with access who doesn't have a clearance and/or the trust. **Then there will be a day when you will be terminated from your employment because someone viewed your intelligence based product within your own host system, and they compromised evidence.**

My caution to you is from scars on my back, and without a doubt we are already behind in this wave. Let's not fall further behind. Let's convince our administrators and our decision makers, we don't build stuff. We provide a service. Therefore, we should think of this as a service-based opportunity and not an infrastructure that we need to build.

Tom Streicher
Former Chief of the Cincinnati Police Department

Chief Streicher experience and reputation not just within Cincinnati PD but throughout the US precedes him. As the Former Police Chief of the department, a position he held for over 12 years, Striker earned the CPD both National and Local recognition for his leadership and accomplishments. Most recently he was awarded the 2011 Police Executive Firm Leadership Award, [00:50:00] which is presented annually to individuals who have made outstanding contributions to the field of law enforcement and to exemplify the highest principals and standards of true leaders in policing on a national level.

Tom Streicher: I've got a nightmare of a story, and it goes all the way back to 1997. In 1997 we came up with a wonderful concept. We decided to apply for a grant from the Department of Justice to standardize the use of a reporting system throughout the county so that everyone would fall under the same reporting system. We would be one of the first agencies in the country to get mobile data computers. We would be entering our information real time into a system, and we'd be able to extract that information in real time to make it easier for us to make decisions on deployment of our officers to save time. That time could then be applied to other aspects of policing.

In order to do this, we had to get agreement from agencies all across the county. Each agency was given the same weight, so a three person agency meant the same as the 1,000 person agency. Threw things kind of out of kilter. The things larger agencies needed weren't needed in the smaller agencies, and unfortunately the larger agencies wound up being on the bottom of the heap and didn't get some of the things they needed.

Much worse than that, the board to direct this were a bunch of former police executives from the county who had been retired more than 10 years earlier and were approaching 70 years of age. 70 years of age is not a bad thing, as I head toward 60 years of age. I think to myself how little I knew about technology, and that causes me to believe that those

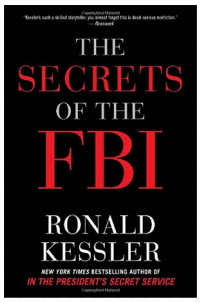
people knew nothing about technology at all. Here's the story. This started in 1997. I was promoted to Chief in 1999.

In 2008, 11 years later still did not have the product we were looking for. We had spent in excess of $15 million trying to build this system.

Many of the agencies had dropped out of the process. Every time I asked about progress on this, I was told "18 months to 2 years out." We had gone through about seven different vendors, and at the end of each one of those contractual agreements with a vendor, the vendor had thrown their hands up and said, "This is an impossible task." Yet we had spent millions of dollars with those vendors.

So in 2008, after 11 years, we had a good relationship with the University of Cincinnati. I contacted the Dean of one the colleges and said, "Is there any chance you can send some of your IT students up there, perhaps even a professor or two, and just take a look at this system and tell me what you think of it. Tell me what you think of what we've been trying to build here." Three days later came back to the office and said, "Okay, we've got an answer for you." I said, "What is it?" he said, "Well, you're about 18 months to 2 years out from having a complete system."

I said, "It's been that way for a decade now!" He said, "But here's the harsh reality of it. If I walked in here and told you today that your system is finished - it's up and ready to go - your system today would be more than 10 years obsolete and was being given away by agencies more than a decade ago." A decade ago was in 2008. And we had invested more than $15 million. That does not count the number of person hours that were invested. That doesn't count salaries. It doesn't count fringe benefits. That's hard real money we had spent.



The book entitled **The Secrets of the FBI**, written by Ronald Kessler, emphasizes that these types of mistakes, these types of missteps. This type of lack of knowledge on behalf of police agencies goes all the way up through the very top of law enforcement at the federal level.

Mr. Louis Free was director of the FBI. The book says, "Free's concept of investigations was limited to what he had done as an agent 10 years earlier knocking on doors and interviewing people. He did not understand the technology that had become essential to law enforcement. He had no use for computers and did not use email. Weldon Kennedy, who Free appointed Associate Deputy Director for Administration, remembered that Free kept a computer on the credenza behind his desk.

"'I never saw him use it and nor did I ever see it turned on.' By the time Free left just before 9/11, the FBI's personal computers were so primitive that no one would take them even as a donation to a church. They were pre-Pentium machines and incapable of using current software, reading a CD-ROM or even working with a mouse. The FBI's internal email was so slow that agents used their personal email addresses instead. The FBI system did not allow email outside the agency often because of funds from the justice department. Local police were far more technologically advanced than the bureau because few of the FBI's computers could handle graphics. Agents would ask local police departments to email photos of suspects to their home computers.

"As their primary computer, agents were expected to use something called an automated case support system developed in the mid 1990's. It used 1980's technology. It could not connect to the internet and did not use a mouse. The system was so slow and useless that for investigations alone the bureau had developed 42 additional separate systems that agents used instead of the main system. Each of these additional systems had to be checked and make sure all references to an individual had been obtained."

Where does this type of failure fall? It falls with us. One of the biggest mistakes is to take our cops and turn them into IT people. What we see them do is specialize. They will cocoon around themselves so they are inseparable from the agency. Nobody else is there that knows how to run what they built. Then there comes time for them to retire. You are without choice but to hire them back as a civilian, and create a "double dipper," which also gets you headlines.

We need to depend on the advice that we've gotten here today from Mr. Trippie, and we also need to pay attention to what the young people who are coming into this profession know and understand. It's something that many of us have been afraid of, me included.

Rick Smith
CEO, Director and Cofounder of TASER International, Inc.

As CEO Rick leads the company with a constant focus on delivering innovative solutions that make communities safer. Rick's quest for technology solutions reduce world violence begin in 1993 when he founded TASER with his brother Tom. Since then TASER ECDs are in now more than 16,000 law enforcement agencies in more than 40 countries.

Rick graduated from Harvard with honors, received his MBA from the University of Chicago with a Master's in International Finance from the University of Leuven in Leuven Belgium. He is the co-winner of the Ernst & Young 2002 Entrepreneur of the Year and named one of the 2010 Most Admired CEO's and Top Level Executives as sponsored by The Business Journal and no pun intended, not shockingly, but he holds 14 patents as well so quite a record of accomplishment. I'd like to introduce Mr. Rick Smith, CEO of TASER.

Rick Smith: I didn't invent the TASER, by the way. A lot of people ask me about that. The TASER was invented before I was born back in the 1960's. I got involved in this after a couple of friends of mine were shot and killed and I got very interested in public safety and technology. I ended up finding the right people to bring together and breathed some new life into the TASER, and now we have the great fortune of dealing with most of the agencies in North America, and many around the world.

We have expanded into more of a technology provider, not just providing electronic weapons. All of our weapons are actually computers that generate information we have to manage. Now we've got cameras on 60,000 of those TASERs, and we're focusing on wearable cameras. We've seen the explosion of data that's coming, and that's what attracted me to this cloud business model.

The way I could encourage you, as a Chief, to think about this cloud: it's not as a technology. It's just a different business model.

Historically technology was delivered to your agency through discs purchased from a vendor who would mail them to you with a bunch of manuals. Then you've got to staff-up, build, and run this stuff on site. Frequently you're using consultants, or your own people running these evermore complex systems. As you start moving into things like video data, where the size of your files grows by orders of thousands to millions of times larger, there's an explosion of data that's headed your way.

I'll give you one example, I talked with one major police department, and the complexity of running all of these systems onsite is such that they want 134 different major systems within that agency. And I asked them, "Well geez, how often do you guys update your technology?" Any guesses how often they update their technology? **They said every five years.**

Now you think about how fast technology is moving. The difference with a cloud business model is, instead of building it and running it onsite, you push the technical challenges back to the vendor. You're not even responsible for discs and manuals. The vendor is responsible for delivering a functional service. So the same people that are building that technology are responsible for running it, maintaining it, and delivering it to the agencies.

That gives you a clear line of accountability, whereas right now the system blows up, you get one of these: "It's the IT department's fault." "It's not us, it's the vendor." Well, which vendor is it? Which part is breaking? Then you have this incredibly complex technical problem to solve. As a Chief or as a Manager, you don't know who to go choke, right? Who owns this problem? **So really, the cloud is simply about not trying to build and run everything locally onsite. It's about being able to test fully functional capabilities and procure those capabilities instead of spending years building something that may never actually get functional.** With a cloud business model you can actually have a bake-off between vendors on live systems. The same ones you would deploy. And in many cases, cloud providers are providing free use of that service for an extended period of time before you ever even have to even make a purchase decision.

You've seen it on the consumer space. How many of you have an email system that you use from a cloud provider: Apple, Yahoo, or Gmail? Those are all free services where the cost of delivery is so low that they can pay for it simply with advertising. That's a great example of the economies of scale that happen when you get this clarity that comes from the vendor being able to support and deliver one functional service, rather than a technology bundle that's got to be built and operated onsite by people that don't have the expertise nor the time. When you've got to manage 134 systems you can't

become an expert in any one of them. That's where you get that "deer-in-the-headlights" look where people are overstaffed, the systems get too complicated, and then that introduces cost risks and huge security risks.

The more complex something gets the harder it is to keep it live and keep it secure.

Richard Beary
Former Chief of the Lake Mary Police Department

In 1992, Richard Beary was appointed chief of police for the city of Lake Mary, Florida. Beary served during a time of unprecedented growth. Utilizing a strong community-policing philosophy, the city and department prospered, and, in 2007, Lake Mary was named the fourth best place to live in America by CNN and Money Magazine. The city leadership encouraged the development of strong partnerships, which allowed Beary to devote time to IACP committees and issues. As a member of the IACP Narcotics and Dangerous Drug Committee, one of his proudest achievements was convincing Congress not to eliminate the civil forfeiture of drug traffickers' illegal profits and property. Retired Drug Enforcement Administration Administrator Thomas Constantine and every committee member will confirm this was a highly contentious issue. Had they failed, police agencies would have lost millions of dollars, and criminals would have reaped profit from their criminal acts. In June 2007, Chief Beary announced my retirement after 30 years of municipal police service.

Richard Beary: We've virtualized our Com Center. Here is one of your big savings. You know those big computer rooms you used to have to build to hold all those servers because everyone had to have a server for their own app? Those are gone. **The electricity we're saving alone was worth the investment of pushing some of those servers is in the cloud.**

We have issues with trying to organize our employee data, particularly as it comes to payroll. Well when you've got people spread all over, do you really want them coming back and submitting timesheets? Because when I got there, we were doing manual physical timesheets, and the employees would drive in some cases 70 miles once a week to turn in their pay sheet so that somebody could put an initial on it. Well instead of building this whole system, we went out to the web. We got a vendor, the officer logs in, and we get their data. But guess where they have to log in from? One of our domains, so we know where they are. So we do some checks and balances.

Another way that cloud is going to affect every single one of you: the rebanding of all

your radios. Everybody is going through this national rebanding. If you're finished, good. If you're not, I feel sorry for you. You know, we had this model. If we needed to reprogram a radio, or we needed to do upgrades on our radio, what did we do? We collected all the hundreds and hundreds of radios, and we sent somebody across town, we drove all those radios, they sat there for four or five days, and we had people on the streets without radios waiting for the radios to come back.

And in Orange County, Florida, we're part of the countywide radio system. There are over 10,000 subscribers units in that county. You think about what it's going to take to physically touch every single subscriber unit to do that upgrade. So what have we done with our new system? **We've pushed that out on the web.** If there's an upgrade that comes out or a new reprogram that happens, when that officer turns the radio back on what happens? **Boom. Total upload of all that software. We're not transporting radios all over town. We don't have cops out there without the radios.**

What I'm saying to you is there are a lot of simple applications that don't take a lot of rocket science. Those of you who are law enforcement executives: how many of you have been screwed by a software company? Come on, let's be honest.

Using the cloud means you're not held hostage. Those old companies screwed you, and then they kept giving it to you because you couldn't walk away.

The cloud allows you to not be held hostage.

As long as your platform is right, you can say, "You know what Mr. Vendor? I'm not happy with you, see ya." Next company in, I got a fixed price for what it's going to cost me, and I'm on with the business. I'm not going to be held hostage anymore.

Hadi Partovi
Entrepreneur and Angel Investor

Mr. Hadi Partovi was on the founding teams of "Tellme" and "iLike." As an angel investor and startup advisor, Hadi's portfolio includes Facebook, Zappos, Dropbox, OPOWER,Flixster, Bluekai, and many others. A graduate of Harvard University, Hadi began his career during the browser wars in the 1990s, when he was Microsoft's Group Program Manager forInternet Explorer. After the release of IE 5.0, Hadi co-founded Tellme Networks. Tellme was acquired by Microsoft for a reported $800 million. Hadi was General Manager of MSN.com during MSN's only year of profit, where he delivered 30% annual growth and incubated Start.com (now Live.com). After leaving Microsoft a second time, Hadi co-founded iLike with twin brother Ali Partovi, and together they built the leading music application on the Facebook platform. in 2009, iLike was acquired by MySpace where both Partovis worked as Senior Vice Presidents. Hadi is a strategic advisor to numerous startups including Facebook,Dropbox, OPOWER, and Bluekai. He is also an active angel investor with a wide range of investments.

Mr. Partovi: I graduated out of college and worked at Microsoft, and I had the good fortune of seeing many ways of computing change in the Tech world, the first being in the '90's. I saw Microsoft's vision of computers on every desktop, which back then seemed crazy, and is now something we take for granted. About 10 years later, with the internet, the belief that all these computers should be connected to each other, which again back then seemed a little bit unrealistic, and is now something we all take for granted.

We're now in the process of two different ways of computing that are also changing the world. One is with the proliferations of smart phones, each of which packs more power than an entire desktop computer of ten years ago. We're already at the point that more than half of all phones being purchased are smart phones, which means within ten years everybody is going to take it for granted that a phone is a very powerful computer. The other wave of change that we're currently in is the cloud wave. I actually hate that term, because it really is just a continuation of the internet wave. It just means that now computers are connected. Instead of just getting services like Facebook online, all the

services we use at work should also be online. Anybody who uses Microsoft Word knows it's a pain in the butt to deal with these security updates and patches. Then if you want new features, you need to purchase the new release and personally install that or get your IT department to install that.

Whereas if you use Facebook, it updates itself every week. Every single week they're pushing out a new version. You don't need to worry about it, and you just see a new feature.

The simplicity of that for the user, in the ease of managing it, the ease of updating it, and even the ease of learning how to use it, are what makes the internet easier than desktop applications.

And the word "cloud," the reason I hate it - it just means applying the simplicity of the internet to the applications we use in the workplace.

Security

Rick Smith: We spent a lot of time looking at security issues, and what a lot of people don't realize is that your biggest risk is typically not your technology. It's pretty rare that somebody hacks through a firewall on some technical patch. The risk is your people. That's where you're breached. Hackers will get somebody's user name and password and find some way to hack your people systems. It's the same thing from your legal perspective. For example, look at the OJ trial. Did the defense go after DNA technology to convince the jury they couldn't rely on the technology? No. They went after the people. They said we don't know that the officers didn't tamper with the blood samples in some way.

When you think about chain of custody, one of the most important things is to look at your business process. **How many human fingers are in the process at different stages? That's likely where your biggest weakness is going to be, more than the technology.** So if you have your lawyers look at the business process, where are there manual interventions where somebody could tamper with it? For security, you minimize those. Then actually look at the technology. The technology is actually pretty straightforward. For example, there's a technology called hashing where you take a file and you run it through an algorithm that can then give you a fingerprint of that file. And later if you have to prove it's not been tampered with, you can prove to a statistical relevance of about one in five quintillion that something's been tampered with. That statistic is millions of times stronger than the statistical probabilities of a random DNA match.

So the technology is the easy part. The harder part is the business process. That's where you should put most of your focus. And then once you identify which technologies are being used, those are pretty easy to audit.

Rob Davis: Let's put it in simple terms. You've got a very sensitive Internal Affairs or a sensitive homicide case, maybe an assault case. Depending upon your setup, there could be a lot of people in your agency that just waltz into the area where those file cabinets are held and work their way through that file. They can take a look, take pictures of things, etc…

It's a whole lot better, it's more secure, to have a system recording digital fingerprints for the people who touch that file.

Total Cost of Ownership

Tom Streicher: $15 million had been invested as of 2011 when I left. That does not count salaries. That's just the hard dollars that we had invested.

Rob Davis: I think in general you find that first of all you can stand your system up immediately. You don't have those startup costs. Somebody else has already paid for the R&D to do that. You simply just turn it on. You're not building your DISH network. You buy it, you plug it in, you turn it on, and it's ready to go. So there's just a lot of the cost savings that come with that type of system.

Tom Streicher: This is Heather Whitten and she is one of our IT professionals in the Cincinnati Police Department and did and still does an amazing job of working with our systems. In fact she has pioneered some of the most modern usages of data on license plate recognition throughout the country. She's an amazing technician for us.

Heather Whitten: Just a quick note on the total cost of ownership. We looked at building an in house system – servers. I'm glad you had addressed the electricity. It was originally going to run about $500,000 to build these servers in-house. In our first 17 months, by using a paid service, we only ended up spending about $125,000. So we saved almost $375,000. We're still not even close to that $500,000 and we've been live in the cloud for almost three years now.

Keith Trippie: The other side of it is, let's face it, if you go out and try to deploy something from scratch, has anybody ever hit the schedule? If it's a six to twelve month project, anybody hit the schedule? How about budget? Was it actually $500,000? I bet it would be a million dollars by the time it got done. We all face that.

Conclusion

Rob Davis: You've heard the experience of all of these individuals seated up here. Our message is this: you do not need to fear cloud computing. There are a lot of issues and concerns that people might have. We have been some of the recipients of the problems that come when you're not using such a system like that. You're not leveraging advanced technology, and you're spending millions of dollars that you don't need to spend. Don't fear it.