5 Issues to Consider Before Deploying Cloud-Based Email for Law Enforcement

Matt Williams | February 23, 2012

In a typical U.S. city, the police department and other criminal justice agencies account for as much as half of the government work force. When it's time to make a big enterprisewide decision, there's no doubt that law enforcement is — and always has been — a powerful bloc that's capable of swaying a project toward success or failure.

It's not surprising, then, that because more city, county and state CIOs have begun to seriously pursue cloud-based email in search of cost savings and up-to-date applications, there now are examples of law enforcement submarining such a migration, as well as being the driving force in a positive outcome.

What should public CIOs consider when thinking about putting their law enforcement agencies' email into a cloud? Here are five points to ponder that have emerged in the two years since Los Angeles broke new ground by announcing its intent to have a private company manage all city workers' email.

1. It Can Be Politically Charged

You have to wonder if Los Angeles CTO Randi Levin wishes she could have a do-over. From the start, her IT department's plan to save money and improve service by having Google host and manage the email of all 30,000 city employees — including the Los Angeles Police Department (LAPD) — ran into opposition on multiple fronts. The Police

Department was concerned about the security of its data, privacy advocates worried about data leaks, and some City Council members expressed concerns of their own — though the city ultimately decided to go forward with it.

The public attention on the project consequently intensified, so Google put more reps in City Hall to make sure its business interests remained on course. In turn, Google's competitors swooped in to try to block the deal. Before she knew it, Levin was in the middle of a politically heated situation without an escape route. In December 2011, the City Council unanimously decided to cancel the email migration of Los Angeles' 13,000 law enforcement personnel because security requirements for criminal justice data weren't met by Google's product, and Levin essentially was left alone to defend the basic precepts of the project.

Levin said Google Apps is "working fine" for the majority of city employees — 17,000 non-law enforcement users have moved over without much trouble. She blamed the stalled migration of law enforcement users on technology outpacing public policy. "The real issue here is the fact that the policies related to a lot of different areas in government are not matching the technologies that are coming out," Levin said in October, prior to the contract's partial cancellation. "That is the core issue: The criminal justice requirements were never written with cloud computing in mind."

Other city- and state-level CIOs who have since pushed for cloud email for their own governments say that the lobbying battle between Google, Microsoft and other big email providers remains fierce and is the tinder that could inflame similar controversies in their own communities. An element of risk remains, say some CIOs privately, that their project could blow up à la Los Angeles. Putting email in the cloud is not for the timid, they caution.

2. There's an Air of Mystery

It's unclear where exactly Los Angeles ran into trouble, and how other cities and states have successfully moved to Google without incident. In October, Levin said there was only one unresolved issue preventing Google Apps from being fully compliant with the Criminal Justice Information Services (CJIS) security requirements overseen by the FBI. Levin didn't divulge publicly what the unresolved problem was.

Google hasn't gone out of its way to reveal what went wrong either, aside from blaming what it claims were unforeseen contract amendments after the project was under way. "We're disappointed that the city introduced requirements for the LAPD after the contract was signed that are, in its own words, 'currently incompatible with cloud computing,'" a Google statement said in December. Google declined to participate in this story.

When Pittsburgh announced in January that it finished a Google Apps rollout of its own, then-CIO Howard A. Stern said city leaders would continue to watch the situation in Los Angeles. After the new email system was done, Stern promptly left the public sector for a job in academia. He's still waiting for a clear explanation. "Quite frankly, L.A. hasn't been forthcoming about what the issues are," Stern said in February.

Before choosing Google, Stern said Pittsburgh had conversations with the company and other cities that were deploying cloud email. He made Pittsburgh's City Council and mayor aware of the red flags in L.A., and told them that while Google might not be a perfect solution, it was still safer — despite the uncertainties — than what his IT department could provide in-house. Stern sold the Pittsburgh Bureau of Police on the fact that Google's email had won Federal Information Security Management Act certification. Police officials backed Stern's proposal, and they all moved forward together.

3. Security Requirements Are Strict

Don't expect the FBI to make any special accommodations for cloud computing in its rules for using data from the CJIS Division, which gives local police access to the federal government's storehouse of fingerprints and criminal histories. According to a December 2011 paper from the FBI on the subject, cloud computing is compatible with the CJIS policy, but not at the expense of the minimum security standards that govern data sharing among law enforcement agencies. The FBI recognizes that its position could make technology deployments more difficult, and that not all IT contractors will be able or willing to play ball. According to the FBI, vendors are required to identify the IT administrators who can access criminal justice information, perform fingerprint-based background checks of those personnel, and prohibit remote maintenance activities that are done outside the U.S.

"Admittedly, these requirements may be difficult for some cloud-computing vendors due to the sheer numbers and the geographic [dispersal] of their personnel. However, these requirements aren't new to vendors serving the criminal justice community and many vendors have successfully met these requirement for years," according to the FBI's CJIS Division.

What does this mean for an email deployment? Expect to work hard on the smallest of details, says Florida CIO David Taylor, who is nearly finished with a new statewide email system that will be managed by a vendor. New legislation in Florida mandated that all executive branch agencies — including law enforcement users — move to a single enterprise email system that would meet all of their business needs. This meant that Florida had no choice but to address the CJIS requirements head-on.

"I don't know what has sunk the boat of other folks out there," Taylor said, referring to Los Angeles, "but I imagine it was one of two things: No. 1, the background checks — they were very challenging." In Florida's case, the state's new Microsoft Outlook Exchange email system will be managed by ACS in a separate data center that Taylor likened to a private cloud. That meant that all 140 of the company's employees working on the implementation had to undergo a stringent background check. Everyone, from the architects to the person who opened cardboard boxes, had to be vetted. Several employees didn't pass and were removed from the project.

The second big issue that could've tripped up a city like Los Angeles was advanced user authentication, Taylor said. More than a user name and password was necessary to meet the CJIS policy. “The interpretation of what the ‘more’ was, as it pertains to all the different ways to connect to a system, was a big point of discussion,” Taylor said. Florida and the vendor had to work together to make a secure architecture and authentication that would fulfill the CJIS requirements for each of the email system’s entry points, such as the Messaging Application Program Interface, BlackBerry and ActiveSync. It was a lot of work to figure all that out, especially since no one had done it before, Taylor said.

There were 32 separate CJIS security requirements that had to be addressed, Taylor said. They covered everything from data encryption to biometric access controls.

4. Skepticism Still Is Common

For every Pittsburgh or Florida, there are at least as many — if not more — doubters of cloud computing. And that may not change anytime soon within police departments, which have been conditioned over the years to protect sensitive information at all costs.

Richy Vaughn, IT director of the Metropolitan Nashville Police Department, is wary of the cloud. In Vaughn’s words, putting his department’s email in a cloud outside of his direct control is an “ insane” notion that isn’t even worth considering. He would worry, he said, about data breaches emanating from a third-party provider and the possibility of officers unwittingly leaking data when using the cloud-based email remotely. Although Vaughn’s IT department is still operating legacy systems itself, he said that’s preferable to moving into a cloud for the sake of modernizing a system. The stakes for security are too great. “If you don’t follow the [CJIS] standards at the minimum, they will shut you down,” he said.

Vaughn’s stance certainly isn’t unusual among police departments across the U.S. The prevailing attitude in law enforcement is that the agency that owns the data is responsible for it. So to ensure security, you must have management control of the data. “That’s a mentality that still permeates, and I’m not sure that’s a bad thing,” said P.J. Doyle, former CJIS director of the Florida Department of Law Enforcement, “because a lot of harm can be done if that information is misused.”

There’s enough ambiguity in the CJIS security policy that a law enforcement agency could, if it wanted to, effectively drag its feet on a cloud email project, said Doyle, who is now president of the CJIS Group, a market research company. Conversely if a criminal justice agency really wanted to put its email in the cloud, it certainly could do that too.

The policy doesn’t prescribe one technology or one solution, so there is room for interpretation. “It’s a misnomer that the [CJIS] standard is so strict that it has to be ‘this way or the highway,’” Doyle said. Taylor added that the CJIS policy itself is fairly clear, but when it’s time to operationalize that policy, honest differences of opinion can arise over what’s acceptable.

5. Absolute Commitment Is Needed

5. Absolute Commitment Is Needed

Without the combined support of the Florida Department of Law Enforcement, the governor, the vendor and the Florida Agency for Enterprise Information Technology, Taylor doubts the state’s email project would be on a successful course. Stern echoed the sentiment, crediting the Pittsburgh Police Department and Mayor Luke Ravenstahl for going along with the plan even though Google hadn’t yet been widely used in the public sector.

Officials in Los Angeles, Pittsburgh, Florida and elsewhere say that you should expect to invest a significant amount of labor to make it work. Constant communication with the FBI’s CJIS auditors is necessary, and CIOs likely will have to consult with their lawyers and CJIS experts. Florida went back and forth dozens of times with the FBI on different versions of security protocols. “ The FBI didn’t have a way to say, ‘If you do it this one way, you’r e good,’” Taylor said. In some respects, it’s ultimately up to the end user to make it happen.

http://www.govtech.com/pcio/5-Issues-to-Consider-Before-Deploying-Cloud-Based-Email-for-Law-Enforcement-.html