FEATURE

Why The G-Men Aren't I.T. Men

The FBI's new CIO must change the agency's cultural bias against information-sharing and technology before it can become a global intelligence operation truly capable of preventing crime and terrorism.

By Allan Holmes

CIO | Jun 15, 2005 8:00 AM

In the past few months, FBI CIO Zalmai Azmi has been very careful not to say, "I told you so." After the FBI was forced to scrap its $170 million virtual case file (VCF), a case management system, because of numerous delays, cost overruns and incompatible software, Azmi was finally given full authority over the agency's IT budget and encouraged to centralize much of the IT decision making at FBI headquarters in Washington, D.C. He and other top executives at the FBI recognize that they must radically change the agency's culture if the Bureau is ever going to get the high-tech analysis and surveillance tools it needs to effectively fight terrorism. The FBI, they say, must move from a decentralized amalgam of 56 field offices that are deeply distrustful of technology, outsiders and each other to a seamlessly integrated global intelligence operation capable of sharing information and preventing crimes in real-time.

Former IT managers at the FBI say that sharing information has never been standard operating procedure for the nation's top law enforcement agency. In fact, FBI agents intent on solving crime are accustomed to holding information close to their bulletproof vests. Many agents scorn the idea of sharing information within the Bureau—and with other federal, state and local law enforcement agencies. Even when agents are promoted to management positions at headquarters, they bring with them the same secretive modus operandi to the day-to-day management philosophy in Washington, D.C.

FBI CIO Zalmal Azmi is working hard to win buy-in from agents in the field so that the next multimillion-dollar case management system for the FBI doesn't run aground like the last one did.

"They work under the idea that everything needs to be kept secret," says Sherry Higgins, the former project manager for the FBI's $600 million IT modernization project. "But everything doesn't have to be kept secret. To do this right, you have to share information."

In addition, FBI officials have long marginalized the role that IT could play in connecting the dots between seemingly unrelated intelligence, evidence and field notes. (Consider this: Former FBI Director Louis Freeh didn't even have a computer on his desk.) The result is a history of troubled IT projects, including a system to automate 35 million fingerprint files, which ran over budget by $170 million and was delivered years behind schedule. An updated system created to give local police and sheriffs the capability to check for stolen guns, stolen cars and other crime-related data also fell years behind schedule and ran over budget by more than $103 million in the 1990s.

But the VCF's failure caught the public's attention more than any other FBI IT boondoggle, primarily because leaders in the FBI and Congress labeled it as the government's primary weapon to fight terrorism. Without it, the FBI's ability to stop terrorist acts before they happen was seriously jeopardized. "This program has been a train wreck in slow motion, at a cost of $170 million to American taxpayers and an unknown cost to public safety," said Sen. Patrick Leahy (D-Vt.), a ranking member on the appropriations subcommittee for Commerce, Justice, State and the Judiciary, at a February hearing.

Changing the culture at the FBI will be a gargantuan task, Azmi acknowledges. The job has been so frustrating that many top executives left after only short stints. Between 2002 and 2003 alone, four CIOs came and went. And the $170 million VCF system ground through 10 program managers before it was killed. To stop this merry-go-round of failure, top officials say, the FBI not only has to learn to share information, which means communicating more honestly and more frequently with executives and field agents, it needs to establish basic IT management disciplines. As the agency's newly appointed CIO, Azmi is working to win buy-in from agents in the field so that the next case management system does not run aground. His team has almost completed an enterprise architecture that will lay out standards for a Bureauwide information system.

But like other large global organizations that have endured huge IT failures, the FBI must first understand and learn from the failure of the VCF project. The story of what happened with VCF and how an

organization's culture affects the success of IT development has lessons for both private- and public-sector CIOs who strive to make their organizations more competitive and responsive to their constituents.

Azmi likens his work at the FBI to "running a marathon when you are out of shape. Every mile is an uphill battle and an accomplishment at the same time. The race is painful and the 26th-mile marker far away."

A New Mission for the FBI

VCF was the key component in Trilogy, the FBI's effort to modernize its infrastructure. (Trilogy also called for providing agents with 30,000 powerful desktop PCs and a high-bandwidth network to connect FBI locations worldwide; both of those projects have been completed.) VCF was supposed to enable agents to more quickly and easily share information with each other worldwide. As FBI Director Robert Mueller recently explained to Congress, VCF would provide an electronic means for agents to globally send field notes, documents, pieces of intelligence and other evidence so that they could hopefully act faster on leads. A congressional investigation after 9/11 identified poor communication as one of the reasons that the FBI didn't act fast enough on information about Middle Eastern men taking flying lessons. So agency executives hoped VCF would help move the balkanized structure of the FBI, in which agents rarely shared information on cases, to a more unified organization that would trade off leads in a real-time fashion. VCF would be "the first real change in the FBI's workflow and processes since the 1950s," according to a Justice Department Inspector General report.

At its core, VCF was designed to replace a paper-laden process with a Web-based one so that agents could attach to digital reports evidence such as photos, audio files, and possibly news and video surveillance clips. Agents could perform keyword file searches and control access on a need-to-know basis. Currently, agents use WordPerfect to write reports, notes and official documents, print them out, and then fax or send them via overnight mail to supervisors in other locations for approval. Once approved, the documents are faxed or sent back overnight. Clerks then key the reports into the system, a decades-old, Ada-based mainframe called the Automated Case Support System. The process takes days; VCF was designed to cut that time down to hours.

The VCF contract was awarded to Science Applications International Corp. (SAIC) in June 2001. The contract called for a Web-based front end that would link to legacy systems. Even when the contract was awarded, the FBI had yet to identify all of the requirements, Mueller told a Senate appropriations subcommittee in February.

But three months later, terrorists flew jets into the World Trade Center and the Pentagon, and the FBI was given a new mission: Stop terrorist attacks before they happen. The FBI scrapped the original VCF contract and determined that the new case management system must involve a complete replacement of its legacy systems to give the agency a more robust technology solution that would analyze clues, evidence and leads. In February 2002, the FBI asked SAIC to develop a much more ambitious VCF system that could manage millions of case files in a variety of formats, absorb hundreds of thousands of new case files every year and provide agents with a three-second response time to specific queries. Under pressure to respond to the terrorist attacks, the FBI asked SAIC to deliver the system in 22 months in a "flash cutover" strategy, which called for ditching the decades-old system for VCF overnight.

Yet even by then, the FBI had established few requirements for VCF. "Here is where SAIC made honest mistakes," said Arnold Punaro, executive vice president of SAIC, in testimony submitted Feb. 3 to a Senate appropriations subcommittee. "We should have known that this approach was too ambitious.... It was here that SAIC should have made its concerns known to the director," particularly concerning the flash cutover approach.

Mark Hughes, president of SAIC's system and networks solutions group, which oversaw VCF development, says his team did express concerns about the drastically changing scope of the project to program managers at the FBI. But he suspects those concerns never reached Mueller. "We took for granted the message was being moved up the management chain," Hughes said.

They shouldn't have.

An Atmosphere of Secrecy

In late spring 2002, just three months into her new job as Trilogy program manager, Sherry Higgins wanted to know the answer to a simple question: Why did the Bureau's top executives and the project's

contractor, SAIC, insist on using IBM mainframes as the platform for the VCF project, rather than cheaper and more efficient thin clients or Web-based technology?

Higgins couldn't get a straight answer, so she called a meeting with executives from SAIC. She recalls that the answers she got to her questions were vague and evasive. At another meeting a few months later, Higgins asked point-blank why SAIC was dead set on mainframe technology. Finally, "they said that that was what the FBI directed them to do," Higgins recalls.

Higgins then tried to find out why the Bureau wanted to pursue mainframe technology. She called another meeting with about 15 FBI IT experts and asked each attendee why the FBI had directed SAIC to use a mainframe platform. No one offered a reason, until Higgins called on Fred Dexter, then deputy assistant director for information resources management. As Higgins recalls, Dexter said, "It's that way because the leadership just spent $10 million on a mainframe, and they don't want it to go to waste." (Dexter, who has since left the FBI, could not be reached for comment.)

To Higgins, his answer illustrates one reason why the FBI had so much trouble equipping its agents with high-tech systems and software to fight crime and terrorism. "They'll throw good money after bad to cover up a bad decision," says Higgins, who is now a senior consultant for the International Institute for Learning.

Higgins, a seasoned program manager who has handled major projects for AT&T, Lucent and the Olympics, quickly learned that the culture of the FBI was dominated by a secretive G-Man mentality. Secrecy may be useful in investigating crimes, but it created an atmosphere of distrust among field agents and managers in headquarters, Higgins says. The secrecy also bred a culture of intimidation, say former FBI and U.S. Justice Department managers. Many current FBI and DoJ IT employees, former FBI executives and Washington IT experts familiar with the FBI either declined to be interviewed for this article or requested anonymity. "There always has been a culture of intimidation at the FBI," says one former IT manager. "It doesn't surprise me one bit that people don't want to talk."

Underlying the machismo was an even deeper problem: VCF, if it ever worked as envisioned, would shake up the agency's work processes and collide with the widely held perception among FBI agents that technology wasn't a central part of helping them do their jobs. Agents

view gathering human intelligence as one of the primary means of working cases, with computers providing a supporting role, says Frederick Bragg, a special agent in Syracuse, N.Y., and president of the FBI Agents Association. "You can sit at your computer all day and look at what other people already know," he says. "Most agents would rather go out in the field."

Bragg acknowledged some resistance to technology; however, he said agents are not opposed to anything that can help them in their job. Agents do not fear technology, he adds. But having seen the VCF failure, and experiencing unfulfilled promises of other technology advances to help solve crimes, agents have become wary. "They are now more circumspect. They have an attitude: We'll believe it when we see it," Bragg says.

Ken Orr, head of the Ken Orr Institute and a former member of the National Research Council (NRC) committee, which advised the FBI on the VCF project, agrees. "The problem at the FBI appears to be mostly cultural," Orr says. "And that's orders of magnitude harder to correct than a project management problem."

The FBI's dismissive attitude toward IT was embodied by former FBI Director Freeh, who ran the Bureau from 1993 to just before 9/11. "[Freeh] was not an IT person," says a former DoJ IT manager familiar with the FBI IT culture. He and the businesspeople around him were uncomfortable within technology. "They only see IT as a back-office support function," adds the manager, who asked not to be identified. (Freeh did not return phone calls to his office at MBNA America, where he is in charge of government affairs for the bank.)