



Terrorism: A Call for Data Integration

Editor's Note: Please welcome Len Silverston as the newest member to our online columnist staff. Len's column will focus on "National Intelligence and the Integration Gap." This first article is a call to awareness and action by data management professionals in view of recent terrorist attacks and the threat to national security. Future columns will appear bimonthly beginning January 14, 2001, and will address the urgent need to appropriately share the national intelligence of our businesses, government and national alliances to secure our country's safety.

There is no shortage of stories that we, as data management professionals, share about our challenges and struggles in leading the charge to integrate data and share information. I consistently work with data management organizations that have difficulties in gaining complete support for their valiant vision of unifying the enterprise information resource. Now, in a tough economy that has been further impacted by the horrific events of September 11, 2001, enterprises are cutting costs in areas that they perceive are non-core functions such as enterprise architecture, data management and data integration. Ironically, these very same functions are being seen as a core capability that is proving to be essential within our strategy towards countering terrorism.

It is becoming increasingly apparent that having integrated information that is shared between various government agencies could make a huge difference in ongoing detection and prevention of terrorist activity. It might have been able to change the outcome of the September 11th disaster. For example, two of the terrorists involved in the event were on an FBI watch list and, even though they boarded the flight using their real names, they weren't flagged by the airlines, airline security or others.^{1&2} This highlighted the issue that useful FBI watch list information is not shared appropriately with other enterprises such as airlines. The United States is one of the few countries that doesn't coordinate information between the Immigration and Naturalization Service (INS) and the airports; thus, immigration and visa information often goes unnoticed by airlines. Currently, information about dangerous individuals

is stored in some type of watch list in dozens of different databases from the CIA, FBI, National Security Agency, INS, plus local and state agencies.¹

Many of our leaders including President George Bush, Secretary of State Colin Powell, Attorney General John Ashcroft and Homeland Security Secretary Tom Ridge, have all stressed the need for integration, collaboration and cooperation between federal, state and local authorities as well as the public and private sectors. Tom Ridge, the newly appointed cabinet member whose job it is to safeguard our homeland, can only do this with the cooperation and coordination of the federal, state and local agencies. His job is daunting, yet there is now a window of possibility with the recognition of the critical need for integration as an important aspect of securing our country.

On October 29, 2001, speaking on C-Span TV for the House Committee on Terrorism, June Harmon, U. S. Representative from California, stated the case clearly when she said, "We are only as strong as our weakest link. The point made by every witness was that there is a need for increased sharing of information. There are cultural barriers and legal barriers but, being respectful of civil liberties, the sharing has to improve. The importance of intelligence sharing is that it is more advisable to prevent attacks than to respond to them. We must reform intelligence gathering systems so that instead of having 14 disaggregated agencies, we need one with a seamless system to collect, analyze and disseminate information."

The Terrorist Research Center stated, "The most crucial dimension in countering terrorism is current and accurate information. Effective counter- terrorism does not belong with the aegis of the military, law enforcement or intelligence community but requires the unfettered and orchestrated cooperation of the entire national security community."³

What Types of Integrated Information?

The list of types of information that could be integrated is enormous and could

include information from a vast number of databases including terrorist activities, watch-list information, criminal activities, immigration history, airline information, customs information, biochemical involvement and many more.

Which agencies need to be integrated? At a recent enterprise application integration (EAI) conference, the priority for agencies that needed to share information seemed to be law enforcement, intelligence, immigration and customs agencies.² Mark Hurd, president of NCR, told Newsweek recently, "Ideally we can combine the information of the INS, CIA, FBI and other agencies and get answers in real time."⁴ The more agencies that share information, the better position we are in to counter terrorism. However, as time is precious, we must consider what is most reasonable to implement.

As with all enterprises, there are two main types of integration that could occur. Agencies could integrate their operational applications in order to share information across inter-agency systems. This operational integration could be used to detect terrorist activities in real time; for example, the ability to catch anyone on a watch list that is engaged in any type of transaction, such as a flight. The second type of integration involves after-the-fact pooling of information used to analyze patterns that could lead to potential terrorist activity. This involves data warehousing and subsequent data analysis and mining.

Technologies

There are many technology alternatives available that provide integration solutions. Larry Ellison, CEO of Oracle Corporation, has offered to provide free software for a national ID smart card system with biometric identifiers to capture profiles of people and all their activities. Face recognition technology, eye scanners and X-ray scanning devices provide consistent means of identifying people. Once information is integrated, powerful data mining techniques can be used to discover clues leading to terrorist activity. Neural net technologies exist from companies such as HNC that

provide software that learns how to spot suspicious activities by analyzing otherwise imperceptible patterns.⁴

People and Culture are at the Core

While there are great challenges in implementing technological integration solutions, the root issue lies with people and organizations' commitment and ability to integrate. This involves willingness to give up individual (agency) recognition, having inter-agency trust and working as a consolidated team to fight terrorism. Tom Ridge is charged with integrating roughly 50 federal agencies such as the CIA, FBI, INS, NSA and many other agencies that traditionally do not share information. Within these federal authorities there are many branches and sub-agencies where information is held very confidentially, which is one reason that information is not shared. Samuel Berger, the former national security advisor to President Clinton, and R. James Woolsey, former director of the Central Intelligence Agency, suggested at an EAI conference last month that the most serious issues blocking rapid integration involve policy and politics, rather than technology. Berger further pointed out, "Databases equal budgets. If an agency gives up control of their database, they give up their budget. There is nothing people in government will fight harder for."² The budget line-item system where agencies are granted monies for their organization needs to include incentives for teamwork and cooperation, thus providing ongoing reasons for agencies to share information and work together.

Although information sharing is a key to counter terrorism; historically, there has not been much cooperation between agencies. The following insider joke highlights the FBI's notorious reputation for not sharing information and taking the credit. "Dogs from the FBI, the DEA, Customs and the Department of Agriculture are sent to sniff a mysterious package. The DEA dog finds drugs, the Customs dog finds money and the Agriculture Department dog finds diseased meat. The FBI dog snorts the drugs, buries the money, eats the meat – and issues a

press release."⁵

Even if we are able to provide integrated terrorist information, there are huge risks. Pooled information represents a jackpot of gold for information thieves. The information becomes more valuable once it is integrated; therefore, additional security provisions need to be established to protect this information. Privacy-minded individuals may object to integrated information strategies such as national profiling of people's information. However, under the current wartime circumstances, the safety of all citizens as a primary goal must be strongly considered and weighed against privacy considerations.


Where Do We Go from Here?

With this daunting need to integrate information and the tremendous barriers in accomplishing this task, where does one start? Clearly there are many areas where integration can make a big difference and one starting point would be to prioritize the needs and define incremental steps towards more integration information systems. For example, one priority could be to initially identify a few strategic agencies that will integrate profiles of potential terrorists. The overall plan needs to encompass a method of enlisting the cooperation from all levels of each of the various agencies, a consolidated information requirements definition with priorities and funding, overall information models showing integration points, systems and data architecture, and a comprehensive analysis of various technology alternatives.

I have personally worked on a data integration effort across all the state agencies within Colorado and am somewhat aware of the extraordinary difficulty in integrating data. Our team used the concept "communities of interest," which identifies the agencies that would reap the highest rewards if their data were consolidated. Instead of trying to integrate all information, strategic communities were formed between a few agencies to move incrementally closer toward data integration.

Sadly, our culture is more reactive than proactive. The 1997 "Organizing for Information Warfare: The Truth Is Out There" article by the Terrorist Research

Center asked the question, "Is it necessary to wait for this watershed event to critically affect us within our borders before we organize?"³ This is similar to the Y2K situation where we always knew there was a problem and talked about it but acted only when we had to do something. We need to learn that the age-old issue of data integration should ideally be a priority that is set up before we are in crisis mode as opposed something we do when we are forced into it.

It is my hope that this tragedy will open up a window of opportunity that will initiate an integrated effort such as we have never seen before and with results that have far greater impact beyond effectively fighting terrorism. With everything that we have to lose as a result of terrorism, perhaps the September 11 event and this ongoing war on terrorism will be enough of a wake up call to move towards interorganization sharing, collaboration and cooperation. 

References

1. Schwartz, Ephram. Sullivan, Tom. "U.S attack: Data integration needed to track terrorists." Info World. September 13, 2001.
2. Ferguson, Renee Boucher. Berger, Woolsey. "Call For Inter-Agency Sharing", eWeek. October 17, 2001.
3. Devost, Matthew G., Houghton, Brian, K., Pollard, Neal A. "Organizing for Information Warfare: The Truth Is Out There." The Terrorist Research Center. 1997.
4. Levy, Steven. "A High Tech Home-Front." Newsweek. October 8, 2001.
5. Thomas, Evan. "Handbook for the New War." Newsweek. October 8, 2001.
6. Perez, Jeanette. "Data in a Time of Terrorism." Intelligent Enterprise. October 22, 2001.

Len Silverston is a data management consultant with more than 20 years of experience in helping enterprises integrate data. Silverston is the author of the best-selling "The Data Model Resource Book" series (Wiley, 2001, <http://silverston.wiley.com>), which describes more than 230 integrated, reusable generic and industry-specific data models. He has developed extensive software versions of these data models, some of which are now licensed worldwide by Microsoft and some that are available for licensing directly. Silverston's company, Universal Data Models, www.universaldatamodels.com, provides consulting, training and software to jump start data modeling and data warehouse design efforts while increasing design quality and facilitating data integration. He can be reached at lsilverston@univdata.com.