

Analysts Address Information-Sharing Gaps

By Captain Stephen G. Serrao, New Jersey State Police (retired)

Memex

www.memex.com

Information sharing between the numerous and various levels of federal, state, and local law enforcement agencies has historically been problematic. Both human and technological shortcomings have been blamed for the lack of meaningful sharing. The slow and disjointed improvement that we have seen over the years has largely come about as a result of significant natural and historic events.

Without doubt, the tragic events of 9/11 have had a positive effect “jump starting” the law enforcement community’s efforts to resolve long standing information sharing and communications issues. The scrutiny and investigation into “who knew what and when,” and more importantly, “who told whom” has dramatically revealed the gaps and “holes” in the flow of information.

The public’s perception of law enforcement’s ability to protect life and property, and prevent future heinous acts has undoubtedly been negatively affected. And the recent, tragic events in Mumbai, India, no doubt, raise concerns for when or how a similar terrorist, hostage or murder spree might take place in America.

Pertinent Questions

As we see great strides being taken all across the country to improve sharing, remove barriers and integrate data at all levels, several questions arise:

- What’s the next step?
- What is being done with the information?
- What analysis is being conducted?
- What type of threat assessment is being conducted?

The concept of “Intelligence Led Policing” is widely accepted as an effective policing strategy. An underlying principal of this strategy is analytical-driven threat assessment. Although this type of assessment is not new, its broad application is relatively new to most in the law enforcement community. In fact, many officers on the street harbor disdain for this approach to policing and criminal investigation because they believe it distracts them from doing their jobs – catching criminals and locking them up.

Best practice models and intelligence mandates require analytical-driven policing and greater information sharing among federal, state and local authorities in the battle against crime and terrorism.

Some law enforcement executives believe these noteworthy goals have been accomplished. An examination of the current state of affairs speaks differently:

- Coordination of intelligence between federal, state and local agencies is still inconsistent from jurisdiction to jurisdiction
- Federal authorities rarely, and then only manually, tap state tips-and-lead management systems to investigate suspicious activities and trends. Additionally, all feeds of local suspicious activity information are manually fed to the FBI Guardian System
- The FBI has had limited exposure to training and access to state and local information systems and, consequently, cannot access the information they need in real time
- Fusion Centers, which are the intra- and inter-state mechanisms for exchanging information and intelligence to prevent attacks, are just realizing the value of integrating multiple data sources, including local intelligence systems

There are bright spots, though:

- The FBI has begun to place Field Intelligence Group personnel at state and local Fusion Centers in an effort to make the state-federal connection more seamless
- The DHS (Department of Homeland Security) also has begun to co-locate analytical personnel at state and local Fusion Centers
- The Regional Information Sharing System Network (RISSNET) continues to act as a facilitator in the sharing of intelligence and helps coordinate efforts against criminal networks that operate across jurisdictional lines in many locations
- LEO (Law Enforcement Online) and Homeland Security Information Network (HSIN), two national interactive communications systems and information services, are more routinely used by the state/local law enforcement community
- The National Data Exchange System has gone live. This system will provide unprecedented national access to local law enforcement records management systems

However, the challenge of successfully managing the significant protocol and procedures related to criminal intelligence information still remains.

Part of the strategy to overcome this obstacle is the use of automated and computerized intelligence management and analysis systems. These systems can play a vital role in supporting and enforcing the necessary processes that support the collection, management and development of intelligence. They also provide for the efficient and secure sharing of information between law enforcement partners at all levels.

The Trust Factor

Technology also can play a leading role in building trust among the different entities managing the data. While collecting information is important, disseminating it is paramount. Information sharing needs to be facilitated via automation and a rules-based model, limiting the need for human intervention. Policies can be enforced to alert officials when their searches result in hits pertaining to issues that are pertinent and important to them. Secure and scalable platforms that take into account multiple users, access levels and methods of sharing intelligence in today's dynamic intelligence environment are crucial to the successful sharing of raw information, and unfinished and finished intelligence products.

During the critical development stage of any intelligence-led operation, an intelligence system should support the evaluation of information and the development of structured intelligence records, using tools that automate the creation and the linking of those records to their sources, as mandated by federal regulation. Of necessity, it should support security to its lowest level, locking not only entire records but also parts of those records through a flexible security definition system.

In addition, powerful visualization tools are necessary to help investigators and analysts connect seemingly disparate data, understand complex scenarios, and identify hidden relationships and links between data. Workflow management tools should be flexible enough to suit all staffing levels and experience. The input and retrieval of data should not be restricted to one specialist unit, since all information is potentially valuable to an agency.

Since real-time information is critical in the fight against crime and terrorism, the system's information-sharing tools must reduce barriers so information is available to those who need it most.

Information that Bears Analysis

As more and more information-sharing centers become a reality, we need to insure that they leverage the institutional knowledge that exists in law enforcement agencies and take full advantage of existing and developing technology. The daily examination of the influx of data is important so analysts can make judgments about the severity of threats. While a common activity for the military, the law enforcement community has yet to fully embrace the absolute need for employing predictive analytical processes, utilizing cutting edge technologies, training personnel, and developing true expertise. This can be best demonstrated by the painfully slow pace at which formally trained analysts are hired and deployed.

Furthermore, the fact that many large police agencies have yet to purchase, develop, or deploy new information sharing and analysis technology is alarming. Lack of funding and bureaucratically long procurement cycles have contributed to this problem in acquiring resources that are all absolutely necessary in a post-9/11 policing environment.

Good technology with properly trained investigators and analysts behind it can begin to bridge the information-sharing gap, and aid the continuing fight against crime and terrorism.

Captain Stephen G. Serrao is Director of Product Management, Americas Region, for Memex, Inc., the leading worldwide provider of intelligence management, data integration, and analysis solutions (www.memex.com). Serrao can be reached at steve.serrrao@memex.com.

www.memex.com

North America

Memex, Inc.
1595 Spring Hill Road
Suite 200
Vienna, VA 22182 USA

T: +1 703 556 4031
Toll Free: +1 866 MEMEXUS
F: +1 703 556 4282

UK & International

Memex Technology Ltd
2 Redwood Court
Peel Park
East Kilbride G74 5PF
Scotland

T: +44 (0)1355 233804
F: +44 (0)1355 239676

Registered in:
Scotland

Company number:
SC108095

Registered Office:
2 Redwood Court, Peel Park,
East Kilbride, G74 5PF

VAT No:
481 0520 74

Memex