

Information Sharing

Threat Assessment

Author: Stephen G Serrao
Date December 2009

Bridging the Gap Between Federal, Regional Information Sharing

By Captain Stephen G. Serrao (NJSP Retired)

The concept of analytical-driven threat assessment is still very new to law enforcement. In fact, officers on the street harbor disdain for this approach to investigation because they believe it distracts them from doing their jobs – catching criminals and locking them up.

In the wake of 9/11, however, intelligence mandates require analytical-driven policing and greater information sharing among federal, state and local authorities in the battle against crime and terrorism. While these are noteworthy goals, the current state of affairs speaks differently:

- Coordination of intelligence between federal, state and local agencies is still fragmented
- Federal authorities rarely tap state tip-and-lead management systems to investigate suspicious activities and trends
- The FBI has had limited exposure to training on 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 mechanism for exchanging information and intelligence to prevent attacks, are generally not plugged into all local intelligence systems

There are bright spots, though. The Regional Information Sharing System Network (**RISNET**) is composed of six regional centers that facilitate the sharing of intelligence and coordinate efforts against criminal networks that operate in many locations across jurisdictional lines. Additionally, LEO (**Law Enforcement Online**) and Homeland Security Information Network (**HSIN**) are national interactive communications systems and information services primarily for the law enforcement community.

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 intelligence management and analysis systems, which can play a vital role in automating and enforcing the necessary processes that support the collection, management and development of intelligence, and the secure sharing of information between law enforcement partners.

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, and information sharing needs to be facilitated via automation and rules.

Policies can be enforced to alert officials when their searches result in hits pertaining to their cases. Also crucial are secure and scalable platforms that take into account multiple users, access levels and methods of sharing intelligence in today's dynamic intelligence environment.

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 source. 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.

As more and more information-sharing centers become a reality, they need to process the institutional knowledge that exists in law enforcement agencies and leverage powerful 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 analytical technologies, training and expertise that are 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 fight against crime and terrorism.

Captain Stephen G. Serrao is Director of Intelligence Solutions for Memex, Inc. the leading worldwide provider of intelligence management and analysis solutions (www.memex.com). Serrao can be reached at steve.serrao@memex.com.

Contact Us

Memex Technologies Ltd and Memex, Inc

UK and International

Memex Technology Ltd
2 Redwood Court
Peel Park
East Kilbride G74 5PF
Scotland
Telephone: +44 (0)1355 233804
Fax: +44 (0)1355 239676

America

Memex, Inc.
22636 Davis Drive, Suite 130
Sterling, VA 20164, USA
Telephone: +1 703 556 4031
Toll Free: +1 866 MEMEXUS
Fax: +1 703 556 4282

Copyright ©

No part of the contents of this publication may be reproduced or transmitted in any form or by any means without the written permission of Memex.

More Information

For the latest information about our product and services, please visit

<http://www.memex.com>