

**► SUMMARY**

The Information Sharing Environment (ISE) gives investigators instant access to information obtained from all over the county, state and nation. Command staff must encourage the concept of data sharing via technology to solve and prevent criminal / terrorist activity.

# INVESTIGATOR'S ROUND TABLE GOES **NATIONAL**

Sharing data solves crimes.

By Steve Serrao and Dale Peet

➤ One of the most useful activities in any law enforcement officer's toolkit isn't taught at the police academy, nor is it found in any policy or procedural manual. It's that 6 a.m. breakfast at the local diner—a time when officers gather and chat informally about cases they are working on.

**While much of the talk may amount to idle chatter and amusing anecdotes, sometimes stories about unusual events that weren't significant enough to rate an official report come out as well.** And every now and then, that small piece of shared information becomes the key to solving (or preventing) a much larger crime—something that wouldn't have happened otherwise.

That was the idea behind the establishment of state or regional investigators' Round Tables. Once a month, investigators from a wider area get together, talk about unusual activities, and see if little pieces of information held by different departments might fit together to form a larger picture. It formalized the 6 a.m. chats and gave them a wider scope. But scheduling only allows so many round tables per year. In between meetings, a lot of potentially useful data is being held in individual agencies, often sitting and waiting for the next round table to occur.

Technology has helped us get past both those hurdles: the limited input of the local diner gathering and the delays in obtaining data with the monthly round table gatherings. Government and industry have worked together to create the modern Information Sharing Environment (ISE), giving investigators, analysts and others instant access to all the information obtained from all over the county, the state and even the nation.

Whether it's a beat officer's report of suspected gang activity at a particular street corner, a Computer Aided Dispatch (CAD) report of an unmarked white van sitting outside a government building, a Suspicious Activity Report (SAR) about the unusual comings and goings at a home, or some other seemingly isolated incident, having that information in a central repository can help law enforcement fill in missing pieces or spot patterns that otherwise would not have been apparent.

Yet there's the rub. For all the marvelous things it can do, and the time it can save, the ISE infrastructure is merely a facilitator. The heart of the system isn't the technology; it's the data. Law enforcement agencies or individuals can only act on the data they have. Information that doesn't make it into the system, either because the data owner judges it to be too insignificant or because he chooses not to share it, is essentially lost to the rest of the law enforcement community. And that makes solving or preventing crimes (as well as terrorist activities) that much more difficult for all of us—including the original reporting officer.

Getting this "national round table" to work requires changing some attitudes, particularly among veteran officers who are leery of technology or uncertain about whether the security is in place to protect their sources. Younger officers are more likely to use computers—after all, they've never known a time when computers weren't readily available—but may share the veterans' fears regarding security.

This is where education becomes so important—starting with the command staff. It is critical the command staff get behind the concept of data sharing via technology so the processes gain acceptance throughout the agency. Show your officers and investigators that a search of the NSI (Nationwide SAR Initiative) shared space can give them the same type of

information they're gathering at the early-morning diner.

Only now they're getting results from hundreds of thousands of fellow officers instead of the handful of people they know personally.

Demonstrate how they can search for information regarding an incident that seems insignificant on its own but still has their investigative senses tingling for some reason. Show them how and where to document things of a suspicious nature that may not violate any laws or require filing an official report but still seem important. Helping your agency's personnel get accustomed to data sharing can alert them to persons or activities of interest and help them become better police officers.

A good analogy is what happened with running fingerprints after the Automatic Fingerprint Index System (AFIS) was introduced. We've known for two centuries that the uniqueness of fingerprints makes them ideal for obtaining a positive identification of an individual.

Yet prior to AFIS, matching fingerprints was a manual, extremely painstaking process restricted to the books a department happened to have on-hand. Now, AFIS can compare fingerprints from a crime scene against the millions of records in its database gathered from departments and agencies at

“ One of the keys to data sharing is making sure everyone in the agency understands what resources are available in both technology and functional areas in the agency.

multiple levels all over the country, making finding a match quicker and more reliable.

The ISE does the same with information. An analyst on the East Coast who suspects a murder may be the result of an East Coast/West Coast gang war can go into the ISE and pull up notes and information from brethren on the West Coast that may be useful in solving that crime. Assuming the West Coast did their part by sharing the information in the first place.

One of the keys to data sharing is making sure everyone in the agency understands what resources are available in both technology and functional areas in the agency. For example, some years ago one of the authors of this article was unaware of the intelligence unit in his own department until he saw a job posting within the unit. That led to a lifelong interest in intelligence analysis, but more importantly it illustrates that we need to keep everyone in the loop about agency resources and best practices.

You will still hear anecdotes like that today, so don't assume everyone knows. Make sure everyone in the department knows what the fusion center does and emphasize the value of other intelligence units. That alone may increase the amount of sharing that takes place.

Once officers are of a mindset to share data, the next step is

to make it easy to do. A good method is adding a check box to the department's reporting software that allows the same report they're filing locally to be uploaded to a fusion center or other shared database. Using a check box on existing forms keeps from adding to the officers' workload—it takes just a second or two to check the box—and that gives analysts a heads-up on something they may need to know.

It's also important to integrate all the technology available. Many departments, for example, don't realize the value of mining CAD data. There is a lot of specific information, such as names, dates, etc. that may not rate being entered into the official Records Management System (RMS), but it is still valuable.

Some agencies are making their CAD data available and searchable to regional law enforcement. We know crime crosses borders, and this approach will help fill gaps so investigators and analysts can discover previously unseen links that help complete the picture. CAD data might provide something as simple and critical as an address for a suspect.

While the objective is to make it easy to share comprehensive data, we must recognize that without a means of controlling who can see which information, many officers will be hesitant to share all but the most innocuous data. That's why better software systems have multi-tiered permissions that allow officers to determine who can view the record.

For example, general information about an investigation may be viewable by anyone in the system, but data on confidential informants can only be seen by a few specific people as defined by user security rights. Whatever system you use, you'll want to be sure it can support different security roles and rights.

Sometimes data sharing changes the nature of an investigation when new details come to light. For example, in Pennsylvania last year at the PaCIC intelligence center, an analyst was completing a biographical report for a missing person investigation at the request of a municipal police department.

When she did a search on her intelligence platform across all the regional databases from other agencies, she noticed the missing person was also the subject of a fraudulent identification investigation and had two operators' licenses under different names. The analyst contacted both investigators, and they are currently working together to locate the person. Those facts helped investigators change course and look at more hypotheses.

Currently with more than 4,000 users and on its way to 33,000, North Carolina's Criminal Justice Law Enforcement Automated Data Services (CJLEADS) formalizes data sharing from criminal justice organizations—including court, warrant, probation, parole and local jail information—to create a more rounded profile of offenders and provide a single source of information agencies can access securely via the Web.

The NC Department of Insurance Criminal Investigations Division was able to identify, locate, and arrest members of one of the largest staged accident rings operating in the state, saving countless man hours in the process. CJLEADS provided information that helped in arresting 11 of 16 individuals in three counties, and found three more culprits already in prison, where they were served warrants.

In another example, the New Hampshire State Police (NHSP) used data sharing to solve a case involving threatening letters being sent to one of the Governor's offices. As investigators searched for related incidents and reports, a similar case was revealed three states away. Fortunately, NHSP had been scanning regional and national intelligence bulletins into a document repository which was then searched along with many other data sources using a single user interface.

That practice allows the pertinent bulletins to be easily located during future investigations. It turned out that an individual from the Midwest had been sending out similar threatening letters across the country. Only through regional data sharing was the connection made and the case cracked. The case also highlights there are different ways to share data, and different kinds of formats your platform must be able to search.

Encourage officers to enter and share information, no matter how trivial it may seem at the time, and give them the means to do it easily. Train officers on advanced search techniques to help them find relevant clues fast. Together we can create a national-level investigator's round table or version of the 6 a.m. diner meeting—but this time without the cholesterol.

Captain Stephen G. Serrao is a former New Jersey State Police Counterterrorism Bureau Chief. He now serves as Director of Law Enforcement Solutions on the Memex Solutions Team at SAS ([www.memex.com](http://www.memex.com)), the leading worldwide provider of intelligence management and data analytics solutions for law enforcement, military intelligence and commercial organizations. Serrao can be reached at [steve.serrao@sas.com](mailto:steve.serrao@sas.com).

Dale Peet is a 23-year veteran of the Michigan State Police and the retired commander of the Michigan Intelligence Operations Center, Michigan's largest and primary fusion center for homeland security. He now serves as Principal Consultant to the Memex Solutions Team at SAS. Peet can be reached at [dale.peet@sas.com](mailto:dale.peet@sas.com).

LaO

Post your comments on this story by visiting  
[www.lawandordermag.com](http://www.lawandordermag.com)