



Governance of a shared records management system

Written by Don Roskamp

Well-planned governance is essential for the effective operation of police information management. Today's police organizations share boundaries and highways, and criminals that traverse both, spurring a growing demand that has led to the development of law enforcement software that enables data sharing at an unprecedented level of speed and reliability. Police agencies are learning to meet the governance needs generated by this "shared information" in areas such as security, data standards, and administration, using tools such as "memoranda of understanding," or MOUs.

The technology may be new, but the practice of data-sharing among police organizations is well-established. In Ontario, Canada, the Ontario Police Technology Information Cooperative (OPTIC) has shared data on a centralized database system since 1987. Ontario is Canada's second largest province, covering 350,000 square miles with a population of 12 million. About 10,000 officers comprise the OPTIC network, which represents all jurisdictions of the Ontario Provincial Police as well as 42 municipal police services.

The size of OPTIC's network generates enormous potential for cooperation on solving and preventing crime. It also makes effective governance of shared information a necessity.

In 2000, OPTIC selected Niche RMS, a commercial-off-the-shelf (COTS) records management system, to provide a state-of-the-art automated system and data network.

Niche RMS was chosen because of its multi-agency, multi-jurisdictional, full-function capabilities, as well as ease of use and flexibility.

The most important factor for successful governance is a willingness to share data. With motivation, all other issues surrounding governance will fall into place.

Most police agencies within a given area have regular associations of chiefs of police forums to discuss issues of mutual benefit, and the need to share police information has been on the agenda for some time. The first step: form a committee of business and technical personnel from interested police agencies—large and small—to initiate discussions and work out the route to successful cooperation.

Membership in an RMS cooperative should include law enforcement agencies that have full police officer authority, with complete query-sharing capability and access to external systems through available interfaces.

Forming an organization facilitates governance by providing a forum and structure for information exchange between each agency and consolidated input to the technology vendor, as this feedback contributes to the ongoing enhancement of products and services to better serve the police community.

It is essential to establish a mandate or mission statement that identifies its purpose, goals and objectives, and solidifies unity among its members.

All participating police agencies in such a cooperative must be prepared to sign a memorandum of understanding (MOU) that identifies the governance issues identified as important to the organization, and outlines ways of ensuring compliance. The MOU may be referred to as a constitution, by-laws or policies and procedures. There are six key governance issues often addressed in MOUs, described in more detail below:

- 1) Information sharing
 - 2) Data standards
 - 3) Data security
 - 4) Technical issues
 - 5) Election of board of directors
 - 6) Financial operating procedures
- 1) Information sharing: Each agency in the new cooperative has sole control over the degree of information

that it shares with others, and agencies receiving shared information have the responsibility of protecting it to the level requested by the contributing agency. Data that is normally shared includes persons, vehicles, properties, addresses and incidents. Some RMS technology, such as the Niche RMS selected by OPTIC, also has the capability to restrict data access to within an organization and also internally to specific personnel. Data pertaining to the administration and operation of a police agency is not normally shared. (Appendix A is a sample of information sharing policy.)

2) Data standards: Cooperatives must create policy guiding the establishment of a data input base, as well as the standardization of data entry, to ensure they obtain optimal benefits from the system. Standardization allows shared information to be readily accessible and retrievable to all members, and it facilitates audits, public scrutiny, consistency and integrity. Participating agencies should be able to hone in on minimum data standards and may also wish to consult other agencies or states that have established policies that complement their goals, paving the way for expanded data sharing in the future.

3) Data security: This is probably the most complex issue in today's computer environment. Establishing a common set of agency security policies is essential for reliable, credible governance of information management. Cooperatives are advised to produce a manual of security procedures that identifies the threats and risks associated with sharing police data. At minimum, security policies must comply with state legislation and U.S. National Crime Information Center (NCIC) policy. If the agencies have freedom of information practices, these should be included also. Technical security is also essential with any RMS, taking into consideration issues such as malicious software, intrusion, monitoring use, audit trails, and network access control. "Keep it simple," is a good approach. Security policy can be updated on an ongoing basis to cope with emerging trends.

4) Technical issues: Newly-minted cooperatives must hire competent technical personnel who are familiar with the many and complex requirements involved in designing, implementing and maintaining secure networks, such as computer specifications, firewalls, and XML links, to name a few. Specifying standard configurations throughout the cooperative's agencies will save time and money.

5) Election of Board of Directors: It does not need to be cumbersome. Agency heads, those with responsibility for the operation of an approved agency, normally make up the board. Membership can be further based on the number of affiliations of each agency (counties, cities, etc.). The board meets as required (for example, four times a year) to provide direction on the overall operation of the police information system; formulate policies, methods and procedures to ensure the efficient operation of the technology; and resolve any issues that may arise. The board may want to establish a board designate composed of two people—one from the counties and one from the cities—who work together to fulfill its goals and objectives. Good governance requires that issues of contention be resolved through consensus; issues that cannot be resolved using this route should be decided by a majority vote, or a similar pre-established dispute resolution mechanism.

6) Financial operating procedures: The cooperative should take into account the costs of implementing the technology, and the ongoing annual costs associated with governance and the overall operation. Each police agency may simply absorb the costs of personnel attending meetings, formulating policy and working on behalf of the cooperative. It is worth seeking state or federal seed funding for such an inter-agency RMS, as this kind of initiative is particularly important in light of the heightened focus on homeland security issues. Ideally, grant applications will be submitted to the governing bodies of the state and the federal government by a qualified person with a gift for writing grant applications from within one of the interested agencies. An agreement with the technology vendor should address the costs associated with enhancements, new releases and the level of service.

In conclusion, agencies that wish to form a data-sharing cooperative no longer need to look far—best practices have already established for the governance of data-sharing systems. To reiterate, the biggest hurdle will be to enshrine a willingness to view information sharing as realistic and attainable. Once the affiliation of agencies is established, successful and recognized, others will look on with respect. Future links between police agencies within and across states can then also become a reality. Data-sharing limitations are only restricted by imagination.

Originally Printed in Public Safety IT Magazine, January 2007