CHAPTER 63

Needs Analysis for Information Sharing

David G. Kamien
President and Founder, Mind-Alliance Systems

Jean-Francois Cloutier
CTO, Mind-Alliance Systems

Denis Ranger
Product Architect, Mind-Alliance Systems

INTRODUCTION

Fundamental to homeland security is the need to share information between international, federal, state, local, and private-sector entities. The critical need to enhance information sharing (IS) in homeland security was expressed in the Intelligence Reform and Terrorism Prevention Act, passed on 17 December 2004. The section headed ''Information Sharing'' requires the president to establish a secure ''information sharing environment'' (ISE) for data related to terrorism. The act also establishes an Information Sharing Council ''to assist the president and the ISE program manager with ISE-related duties.''[1] In essence, this section of the act aims to implement the recommendation of the 9/11 Commission, which called for replacing ''need to know'' with ''need to share'' as the paradigm for IS.[2] We believe that if ISE is to be developed successfully, an analogous paradigm shift is required in Information Sharing Needs Analysis (ISNA) itself. This chapter outlines a new paradigm.

In IT projects, needs assessment has traditionally been a finite phase. To the best of their ability, systems designers develop an analysis of users' current needs and potential future needs. At a certain point, this is translated into a scope of work that is ''frozen'' so that the ''building'' can begin. The quality of the needs analysis is

bounded not only by time but also by the ability to understand the end users' business logic and information needs. Because IS is so fundamental to homeland security, and because IS needs are complex and dynamic,[3] we believe that ISNA must be carefully managed not as a phase in a project but rather as an ongoing—that is, an evolving—process. We also believe that, to a much greater extent than traditional needs analysis, ISNA must involve the sharers of information: the end users of the system.

In homeland security, needs related to IS vary greatly by agency, group, and mission. Disparate agencies will resist a centralized, "one size fits all" approach to IS; and a uniform set of data requirements will satisfy no one. Therefore, ISNA must be decentralized, nonhierarchical, and bottom-up. Groups of sharers should be empowered to determine what their own "private" IS needs are; this empowerment will provide traction against several problems and issues: bureaucratic competition over turf and over the control of information and authority; concerns about legal liability, accountability, and possible accusations of infringement of civil liberties (such as privacy); fear of information overload; inadequacies in the information management system;[4] and concern about strain-limited analytical resources. See Figure 63-1 for a list of impediments to information sharing.

Our concept of distributed ISNA is a key to addressing these significant concerns and achieving the desired outcomes. In short, each sharing group (i.e., an intra- or interagency group of people who have decided to share information among themselves and their systems) crafts its own IS policies, procedures, and collaborative environments.

SCENARIO-BASED ISNA

We use the term *scenario* to refer to a "chronothematic" sequence of events and activities that drive the IS needs of the sharing group. A scenario is a chronology of all the important pre- and postattack factors that are relevant for planning IS and coordinating joint action. The scenario itself is developed collaboratively by the entities involved.

Scenarios strengthen awareness of the interdisciplinary, collaborative nature of regional homeland security. They provide a context and rationale for uncovering and communicating information

FIGURE 63-1

Impediments to information sharing.

- Organizational fragmentation and compartmentalization
- Culture of bureaucratic competition over *turf*—the authority and political power that goes with control of information
- Distrust of other agencies and their use of information
- Accountability and liability exposure concerns
- Parochial traditions, fear of change, and lack of initiative
- Concern about disinformation and leaks or malfeasance that could compromise sources and methods
- Security clearance and classification issues
- Absence of joint concept-of-operations and businesses processes that require sharing
- Legal impediments, such as concern that sharing might taint information for trial
- Civil liberties issues stemming from privacy protection concerns
- Absence of an information sharing needs and gap analysis methodology capable of handling dynamic information resources, needs, and complex requirements
- Federal-centric focus and state and/or local distrust of federal government
- Technology issues, such as the lack of secure communications links, incompatibility of databases and applications, and inadequate budget or staff to remedy system disconnects and incompatibilities
- Ignorance about whether information is important
- Inadequate information interpretation
- Concern about information overload

sharing needs and capabilities. A scenario-based methodology and software environment will help groups of agencies to rapidly "scope out" the following:

- Missions and tasks that drive the need to share information
- What information is shared
- When IS should occur
- How information is to be delivered

This process specifies IS needs at an unprecedented level of detail, laying a basis for improved and better-integrated information.

SOFTWARE "ARCHITECTURE" FOR ISNA

ISNA is not a onetime effort but a continuous process. It is collaborative and information-intensive, with a potentially large

number of scenarios, involving multiple agencies. The process is also communication-intensive, if only because the participants may be geographically dispersed. Clearly, a software environment is needed to support collaboration and to capture, manage, and communicate a continually growing and changing body of knowledge about agency profiles, scenarios, needs for sharing, capabilities, channels, etc. Participants engage in negotiations to hammer out sharing agreements and specify and plan the implementation of channels over which sharing will take place.

The high-level requirements for this software environment are perhaps surprisingly demanding: what an agency needs to know or is able to share can itself be sensitive information. The environment must support secure and fine-grained access control and enforceable dissemination policies on all sharing-related information.

Structurally, IS will rarely be a simple hierarchy or hub-and-spokes arrangement; most often it will be isomorphic with the complex social networks of the communities that built it. The environment must support the construction, representation, and navigation of arbitrarily complex IS formats.

If (to change the metaphor), we think of IS as a map, or as mapping, then revealing the map or doing the mapping should be a bottom-up, opportunistic, discovery-driven process; it does not lend itself to centralized control. Nevertheless, the environment must allow for oversight in order to evaluate whether an IS map, in its shape and details, conforms to stated policy, and to track the implementation of the prescribed sharing channels.

The environment must also allow for descriptions of a wide variety of information, systems, sources, protocols, etc. Additionally, it must integrate seamlessly with any number of loosely coordinated pilots and projects.

Each scenario represents a consensus among agencies as to the context and rationale for IS. A scenario can be quite complex, with alternative outcomes and sub-scenarios. Each agency may have its own idiosyncratic culture and set of priorities. The environment must support a multicultural, collaborative process of composing and modifying possibly complex scenarios.

Cognitive overload is a persistent concern, given the abundance of information about sharing that must be gathered, analyzed, managed, and tracked. Interfaces between end users must allow participants to move back and forth easily between the ''big picture''

and the many details of scenarios, sharing channels, agreements, and so on.

These difficult requirements are not easily addressed by traditional, centralized software. A centralized design, in which all IS knowledge is stored in and accessed from a central location, is inadequate for a number of reasons:

Agencies are unlikely to cede control over the storage and management of information they consider sensitive.

Centralization limits scalability and creates a single point of failure.

ISNA is itself a form of information sharing (if only about IS itself).

The Intelligence Reform and Terrorism Prevention Act dictates a ''decentralized, distributed'' IS environment.

We believe that a system—whether it is conceptualized as architecture, a map, or something else—should eschew centralization. We envision a peer-to-peer (P2P) system in which peers form ''sharing spaces.'' Each sharing space is under the control of a ''sharing community,'' with its members either within a single agency or spread across several agencies. The community collaboratively constructs within its sharing space a local segment of the global IS arrangement. A community may elect to give other communities access to some content of its sharing space, subject to dissemination policies set by community members.

The sharing spaces are allowed to grow, discover each other, and interconnect securely and as needed, all with no need for centralized control. Some sharing spaces will be created by communities for the purpose of developing or specifying sharing needs and capabilities; other sharing spaces will be set up by oversight agencies to import this information and evaluate its ''fitness'' to policy.

To enable the rapid growth of a P2P network, the installation of a peer and attendant software must be a very simple and trustworthy process. We believe it can be made no more complicated than opening a Web page on a software distribution server, clicking on a button to download and install the software, and then following a guided configuration script. To instill confidence, the software would be delivered with source code and would log all activities as well as enable security audits.

The creation and configuration of sharing spaces must be simple to support agile information sharing; new information sharing communities must be able to form easily and quickly and disband as soon as the need for them disappears.The information (about IS) held in each sharing space would be encoded in ''atomic'' form, not as files. A uniform knowledge representation format, such as W3C's Resource Description Framework, would be used to enable open-ended querying of all information and provide the opportunity for rule-based analysis, such as determination of fitness to policy.

The peers in a sharing space collaborate and share their computing and storage resources while carrying out ISNA functions such as managing scenarios, recording sharing needs and capabilities, and discovering information sharing opportunities and gaps.

Peers expose service interfaces for remote access by Web applications or stand-alone tools through which end users collaborate in composing scenarios, analyzing needs and capabilities, and negotiating information sharing agreements.

CONCLUSION

The end result is a networked environment for ISNA that does not depend on a central controlling entity, gives each participant complete control over security and privacy, imposes minimal initial IT costs, and grows opportunistically to fit the demands of IS communities. We advocate a comprehensive approach to defining IS needs and to designing supporting IS policies and mechanisms to ensure that practices comply with policy.

Finally, we should note that much of this is very similar to ''results management'' as a framework for homeland security. The elements of results management are management system standards, scenario-based planning, risk management, and development of capabilities, with the goal of devising strategies for homeland security and assessing progress. As applied to homeland security, both results management and IS must be flexible, so as to respond effectively to changes—sometimes very dramatic changes—in threats or in operations. Goals, priorities, activities, partnerships, and allocations of resources may need to be reviewed or reconsidered very quickly; and the system must immediately take into account any new terrorist weapon or capability that threatens domestic targets, or any significant change in counterterrorist technology.

See also Chapter 16 **Homeland Security's National Strategic Position: Goals, Objectives, Measures Assessment.**

NOTES

1. Intelligence Reform and Terrorism Prevention Act, P.L. 108-458, 2004, Section 1016.
2. Final Report of the 9/11 Commission, p. 417.
3. IS needs evolve over time, as do various factors in homeland security, such as threats, personnel, initiatives, geopolitics, standards, and technologies.
4. For example, construction of the FBI's Virtual Case Management System has been delayed despite available funding. See Curt Anderson, ''FBI Computer Overhaul Hits Another Snag,'' Associated Press (13 January 2004).

SECTION TWELVE

Domestic Security and Civil Liberties

CHAPTER 64

Introduction to Section 12

K. A. Taipale
Executive Director, Center for Advanced Studies in Science and Technology Policy, World Policy Institute

Within the public discourse, concerns about domestic security and civil liberties are often asserted as competing and potentially incompatible policy interests requiring the achievement of some tolerable state of balance. Implicit in this notion of balance is the smuggled assumption of a dichotomous rivalry in which security and liberty are traded one for another in a zero-sum political game. But the notion is misleading, for there is no fulcrum—as is implicit in the metaphor of a balance—at which point the correct amount of security and liberty can be achieved. Rather, security and liberty are dual obligations of civil society, and each must be maximized within the constraints imposed by the other. ''In a liberal republic, liberty presupposes security; [and] the point of security is liberty.''[1]

Because metaphor affects not just how we communicate but also how we structure our understanding and perception from the outset, challenging the prevailing metaphor of balance is not simply a semantic game. Metaphor has suasive power, particularly in policy debates, because it sets the expectations that can presuppose the outcome. The notion of balance pits security against liberty in a presumed Jacobin antagonism: those seeking to maintain civil liberties can then be said to be against collective security, and those seeking security can be accused of being too easily willing to forgo individual liberty. Often invoked—but rarely parsed—is a comment attributed to Benjamin Franklin: ''Those who would give up Essential