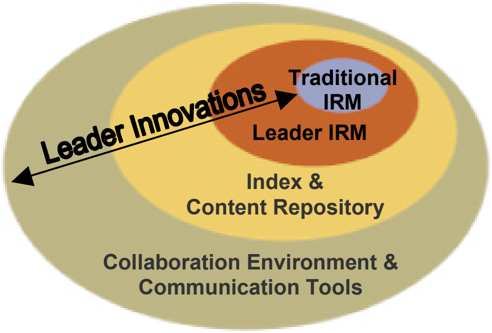
Leader. The Intellectual Capital Company.

Executive Briefing

Leader2Leader® Homeland Security Information Rights Management Platform

Information Rights Management (IRM) organizes access permissions to the data and the network. An IRM Platform enables authorized individuals to actually collaborate as well.

Traditional "rights management" involves network access, permissions, authentication, and encryption. IRM extends this concept to the information being shared among stakeholders — in other words, who should be granted access to a given piece of information and under what conditions. At its most basic level IRM defines who gets access to the information on a given topic. However, real life circumstances are never this simple. Stakeholder groups come in all sizes. Members of stakeholder groups change frequently thus requiring constant directory updating. Stakeholders use a myriad of communication media. Leaders need the flexibility to open up or lock down information sharing granularly as the circumstances dictate. Further, Leaders need to organize that information so that it becomes "intellectual capital" for later benefit. The Leader2Leader® Information Rights Management Platform is designed to extend IRM with embedded browser-based communication features that actually facilitate information sharing and collaboration across information silos.


Traditional IRM
Leader Innovations
Leader IRM
Index & Content Repository
Collaboration Environment & Communication Tools

> **"I was first on the scene at Ground Zero. I didn't even know for eight days that the Pentagon had been attacked… We need to greatly improve our alert communications. What we have now failed us on 9/11."** — Russ Keat, Security Consultant. Found the United States Flag at Ground Zero

Homeland Security Information Network

The Department of Homeland Security (DHS) announced the launch of the Homeland Security Information Network (HSIN) in February 2004 as the umbrella under which DHS organizations will work together. The new system will be based upon the Joint Regional Information Exchange System (JRIES) and currently uses widely available commercial products like Microsoft SharePoint, SQL Server, Groove Networks and K2 Enterprise web crawlers.

HSIN has currently adopted the U.S. Army's "swarming" approach to information sharing. The concept is solid: quickly get the information to the person who needs it. However, information security is jeopardized in the process. Swarming works best within a trusted network. By nature swarming cannot adequately address issues involving need-to-know, organizational culture, statutory requirements, civil liberties and user acceptance as information is shared across jurisdictional boundaries.

DHS-sponsored Terrorex 2004, Las Vegas, January 7-11, 2004

Several information-sharing models were put to the test in January 2004 at The Department of Homeland Security-sponsored "Terrorex 2004 Threat Simulation" in Las Vegas. Leader's collaboration technology was used alongside Groove. Lessons learned from Terrorex included the realization that Groove offered a tactical, "fat client" approach while Leader offered a dual tactical-strategic solution using secure "thin client" web access. Leader's technology provided the ability to maintain a strategic "big picture" of unfolding events while simultaneously providing tactical voice alerts to select groups on a need-to-know basis.

Leader's technology employs commercially available, scalable web technology and provides a viable alternative to DHS for how to solve the problems of cross-jurisdictional information sharing. Leader's technology is offered in a "platform-independent" language (Java) that can be run on any computer operating system supplied by IBM, Sun, HP, Dell, Apple, Linux, UNIX or Microsoft. By contrast, Groove and SharePoint can only run on Microsoft Windows. The swarming approach can be accommodated within the Leader environment, but unlike swarming, Leader's approach also empowers policy makers to decide and control the what's, who's, how's and when's based upon their individual responsibilities and authority levels. Leader's belief is that requiring data owners to open up their networks to "crawlers" makes networks too susceptible to security breaches. Leader believes that the better approach is to empower the data owners with the ability to manage the access rights, and then let the system accommodate individual views of that information dynamically, all without releasing a myriad of crawlers into the wild.

9/11 Commission Report

Quoting several relevant portions of the *9/11 Commission Report* (p. 418, soft cover):

> "The current system is structured on an old mainframe, or hub-and-spoke, concept. In this older approach, each agency has its own database. Agency users send information to the database and then can retrieve it from the database."
>
> "A decentralized network model, the concept behind much of the information revolution, shares data horizontally too. Agencies would still have their own databases, but those databases would be searchable across agency lines. In this system, secrets are protected through the design of the network and an 'information rights management' approach that controls access to the data, not access to the whole network."

Leader's Team Tackled The Most Elusive Problems in Information Rights Management

Leader Technologies formed a technology "dream team" starting in 1997 to address the most elusive problems in large-scale collaborative environments. This effort yielded numerous patentable inventions that are now commercially available and designed to aid in protecting our nation from threats both foreign and domestic.

U.S. Department of Energy, Lawrence Livermore National Laboratory CRADA

During these efforts Leader Technologies teamed with the U.S. Department of Energy – Lawrence Livermore National Laboratory to build a "security shield" prototype that included video security. To quote from Livermore's project report: "This effort resulted in a wired security shield for communication, storing, retrieving, collaborating and analyzing signals and human intelligence input that can be rapidly deployed." (CRADA No. TC-2030-01) Leader2Leader® provides an industrial-strength communications environment that will facilitate Prevention, Analysis, Coping & Recovery – critical elements of signals and human intelligence continuum required to protect our homeland. The platform can be implemented locally, regionally, nationally and internationally in both subscription and premise-based service arrangements depending upon the functionality required. Further, the system is capable of managing complex "many-to-many" sets of rights and permissions governing access to data on a need-to-know basis.

For more information, contact at:

Michael T. McKibben
Chairman & Founder
Leader Technologies Incorporated
921 Eastwind Drive, Suite 118
Westerville, Ohio 43081
(614) 890-1986 VOICE
(614) 864-7922 FAX
mmckibben@leader.com EMAIL
www.leader.com WWW