

# A UNIFYING KNOWLEDGE MANAGEMENT FRAMEWORK FOR HOMELAND SECURITY



Ramon C Barquin, Barquin International

Nothing has stirred more debate in the post-9/11 world than the question of whether the attacks on the World Trade Towers and the Pentagon could have been detected and prevented. Much of that discussion has centered on whether our intelligence and law enforcement communities had the adequate information technology (IT) tools to have identified the terrorist plans early on, located the planners, and taken the necessary preemptive action. Yet the real debate should not be about IT tools, but rather on whether we had the ability to manage all relevant knowledge, share it among the analysts in different agencies, and work collaboratively to accomplish the mission. Clearly we weren't up to the task.

The purpose of this discussion, however, is not to speculate further on the past. Rather, we aim to be forward thinking to prepare ourselves to better manage our collective knowledge and minimize the probabilities of other such similar events occurring.

What then must we do? Former Israeli Prime Minister, Ehud Barak, expressed it succinctly when he stated, "The challenge is to devise the unstoppable to prevent the unthinkable from happening again." And this starts with the ability to know very early, what the 'unthinkable' might be and identify those individuals attempting to move from 'thought' into action. Hence, while "devising the unstoppable..." is a homeland security function, it must depend on a rock-solid intelligence base.

For years, we have defined knowledge management (KM) as the process whereby an enterprise uses its collective intelligence to accomplish its objectives. Ultimately, the homeland security function has to be looked at in the context of a knowledge management framework. What does this entail?

First, when we examine the KM toolkit, it becomes obvious that this discipline relies heavily on IT, but it is not just information technology. In effect, IT is necessary to do knowledge management in any complex environment; but it is not sufficient. Without

understanding the people, the processes and the culture, and incorporating them into the equation, we cannot expect to manage our knowledge satisfactorily.

Decomposing knowledge management, we get the following:

### KNOWLEDGE MANAGEMENT

- A set of tools and processes
- Used by knowledge workers
- In an architected environment
- Created through an enterprise initiative
- To obtain maximum returns
- From its data, information, intelligence and knowledge

The objective of any KM initiative is to endow an enterprise with a robust knowledge management environment. That is, the technological, social and cultural setting and its physical surroundings, that allows knowledge to be shared effectively throughout the enterprise.

There are many ways to construct a KM environment. The framework we use in both the private and public sector is articulated through 12 imperative goals. Each one consists of a cluster of projects addressing an actionable area within the enterprise. Collectively, they catalyze the organization into the creation of a robust knowledge environment where maximum sharing and flow can take place. This is crucial because at the core of KM lies the capacity of the environment to effectively connect someone with a question to a corresponding answer.

### THE BARQUIN FRAMEWORK FOR KNOWLEDGE MANAGEMENT

- Move tacit knowledge to explicit
- Identify and nurture communities of practice
- Find and disseminate best practices
- Develop locators of both experts and expertise
- Have clear taxonomies for major knowledge domains
- Implement enterprise portals as gateways to corporate knowledge
- Build robust data warehousing and business intelligence architectures
- Focus on knowledge about the customer
- Use success stories as a springboard to action
- Assure that corporate culture rewards knowledge sharing
- Focus the enterprise on learning
- Provide the leadership to make KM a priority

It is important that, prior to developing a knowledge management strategy for homeland security, the business strategy itself be clear for alignment to take place. Furthermore, once a KM initiative has been launched it constitutes a KM program, a collection of projects that should be administered using the rigor of project management techniques.



Ultimately, the homeland security function has to be looked at in the context of a knowledge management framework



What does this mean in the context of the homeland security mission? Let's review the framework:

#### Move tacit knowledge to explicit

Most of the knowledge necessary to fulfill the Department of Homeland Security (DHS) mission resides in the heads of individuals who have been doing their jobs for years, whether analysts, firefighters, bio-researchers or demolition experts. Yet we know that within five years, many DHS employees will be eligible to retire. (e.g., approximately 40 percent of FEMA, 31 percent of Customs, and 33 percent of the Coast Guard).<sup>1</sup> It will be necessary to capture that institutional knowledge and transfer it to the new generation of practitioners. KM provides many tools to assist in this process.

#### Identify and nurture communities of practice

Almost all effective knowledge transfer takes place within communities of practice. These are groups of people doing the same type of job, who have a passion for the knowledge implicit in their practice, and who have developed a relationship of trust among themselves. These entities are required for knowledge sharing to take place. The communities of practice involved in homeland security are many but they will certainly cut across the different DHS organizations and go beyond the formal DHS boundary into other enterprises. Furthermore, in many cases they will also cross levels of government, with members from Federal, state or local governments, as well as industry or academia (e.g., ballistics experts). There is much experience in KM on how to work with these communities.

**Find and disseminate best practices**

Within communities, the concept of ‘best practices’ spreads quickly. Finding and vetting them is important, as is their dissemination. So if a chemist, for example, develops a faster way to identify sarin, that innovation must be transmitted quickly to other practitioners. Identifying ‘worst practices’ is also an important concept since sharing the knowledge of what not to do can be extremely valuable.

**Develop locators of both experts and expertise**

Any attempt to systematically connect someone with a question to someone with the answer, should begin with locators of experts and expertise. DHS has a substantial number of experts with a wealth of expertise that can be tapped into by the larger community through tools such as these. Furthermore, there are numerous references in the KM literature to serve as guidance on implementation and operations.

**Have clear taxonomies for major knowledge domains**

Retrieving the right knowledge at the right time presupposes being able to find it. Robust indexing, search and retrieval engines rely on strong taxonomies, or ordered sets of topics, that permit extensive classification of content along different relevant dimensions. DHS needs to build ontology and taxonomies at least for the bio, chemical, nuclear, cyber, and conventional weapons threat areas.

**Implement enterprise portals as gateways to corporate knowledge**

The concept of a portal has provided a simple way to cut through complexity by giving knowledge workers a one-stop capability to easily access the knowledge base they work with day-to-day. Hence, homeland security would benefit from organizing much of the workflow critical to its mission around a powerful and secure portal.

**Build robust data warehousing and business intelligence architectures**

However useful, a portal is not enough. Ultimately, DHS must put its ‘data house’ in order. That means designing and implementing an enterprise architecture featuring strong analytical capabilities that enable the extraction of meaning from data. Identifying patterns and relationships in events, people, places and things are essential to prevention and lay the groundwork for response.

**Focus on knowledge about the customer**

Every enterprise has customers; DHS is no exception. A customer is a person one has to deal with. In the context of homeland security this means that terrorists, as well as victims, first responders and airline operators, for example, are customers. Hence, ‘dealings’ with them can be managed with customer relationship management (CRM) tools. The private sector has proven the value of such tools in harnessing the resources of an organization to address the needs of ‘preferred’ customers by identifying differentiating, interacting and personalizing all transactions.

**Use success stories as a springboard to action**

For knowledge to flow we must first capture attention, and narrative is the key to this. As humans, we are pre-conditioned to hearing stories. It cuts through distrust, provides insights into situations, presents patterns for desirable behavior and ultimately inspires others to action. In homeland security this can be a powerful tool.

**Assure that corporate culture rewards knowledge sharing**

Beyond the needed technology, the issue of corporate culture looms large. A new department composed of multiple agencies, bureaus and pieces thereof, will inherit all the legacy cultures of its parts. From the KM viewpoint, a new corporate culture should provide the right incentives for knowledge to be shared rather than hoarded. This could be accomplished through formal performance plans, rewarding contributions to knowledge repositories, or by providing additional compensation for tutoring and mentoring new employees.

**Focus the enterprise on learning**

Peter Senge<sup>2</sup> introduced us to the ‘fifth discipline’ – systems thinking – and to learning organizations. DHS must become a learning organization since the principal threat terrorists present is asymmetrical. They will be evolving, shifting and probing and the DHS must learn faster than the terrorists. In order for that to happen, the basic principles of learning organizations, enhanced through e-learning, must be adopted.

**Provide the leadership to make KM a priority**

Without leadership, knowledge management initiatives flounder. Leaders who understand the importance of KM and its vision take it under their wings and make it happen. This is arguably the most urgent DHS imperative.

**CONCLUSION**

In conclusion, to accomplish the homeland security mission we must have knowledge superiority over our potential attackers, and thus set the enabling base in people, processes and technology. Knowledge management as a discipline focuses on precisely this objective. Our framework can provide a high-level blueprint to bring it to bear on this crucial challenge facing our nation. ■

1. Katherine McIntyre Peters, “Five Homeland Security Hurdles,” Government Executive, February 2002.  
2. Senge, Peter, *The Fifth Discipline: The Art and Practice of the Learning Organization*, Currency Doubleday, a division of Bantam Doubleday Dell Publishing Group, Inc., 1990, 413 p.

Dr Ramon C Barquin is the President of Barquin International, a consulting firm. He was also the co-founder and first President of The Data Warehousing Institute, and President of the Computer Ethics Institute. He specializes in developing information systems strategies – particularly data warehousing, customer relationship management, business intelligence, and knowledge management – for public and private sector enterprises.