Risk Management Intelligence

By Hal Kempfer
Knowledge and Intelligence Program Professionals

In the wake of the attacks of September 11, much has been made of America's vulnerabilities to terrorist strikes. It seems like every day a new Achilles heel is identified, with the solution being massive infusions of money to build yet another Maginot line of defense. The security industry thrives on building defenses against all manner of perceived threats, both real and imagined.

Meanwhile, almost all agree what is needed is better intelligence. A new awareness of intelligence needs arose from the ashes of New York and Washington DC. What virtually no one agrees upon or has come to understand is what that intelligence truly entails. Nonetheless, for lack of a better term, risk management intelligence (RMI) is probably the most important competitive intelligence (CI) challenge facing business today.

Risk Management Exposure

Beyond terrorism is the full array of risks associated with criminal elements, natural disasters, disgruntled or enraged employees or contractors, and other tangential but very real risks to operating a successful enterprise. One of the challenges facing security and risk management services is putting an accurate value on what they are selling. September 11 provided an opportunity to truly gauge the total impact of business risk costs, as whole industries were looking at potential collapse or wholesale bankruptcies. A nation saw the value of its macroeconomic stock dip as all indicators dropped, and as uncertainty gripped the investment community.

In short, a major act of terrorism can literally be an Extinction Level Event, to borrow a disaster movie line, for a major corporation or even an industry. If American and United Airlines had to face the full brunt of liability from the World Trade Center and Pentagon strikes (it was their hijacked planes that were the terrorist weapons), these companies would no longer be in business. Last fall we saw the ripple effect this had across the airline industry and the economy as a whole. It was very clear that the savings enjoyed over the years by not adequately defending against hijacking was far outweighed by the cumulative costs incurred from the risk management failures of that one fateful day.

RMI Defined

RMI is the dedicated research and analysis support for risk management decision-making. It blends concepts found in competitive intelligence, military intelligence, and investigative intelligence. RMI builds upon the precepts found in hazard assessments, vulnerability assessments, and threat assessments. RMI is the cornerstone in any program to mitigate liability and reduce risk.

> A new awareness of intelligence needs arose from the ashes of New York and Washington DC.

The focus of RMI is the decision-making process itself. A natural disaster like an earthquake, or a man-made disaster like a terrorist attack leave no time for mental preparation. There will be little chance to "get smart" or to develop a plan. Good planning and preparation must begin early.

Scenario based planning and wargaming of likely events that could happen are the keys to successfully manage this kind of risk from the outset. Assessing what kind of scenario to wargame, or plan for, is the challenge for the RMI professional.

Apt examples of where this wasn't done, or done adequately, are plentiful from the September 11 attacks. American and

United Airlines had not planned for such a scenario adequately, had not done enough to sufficiently mitigate this kind of risk, and were essentially caught unprepared. Suicide terrorist attacks were not new on September 11, nor were attacks against US targets by Al Qaeda, nor was the World Trade Center unknown as a target. Tom Clancy featured hijacking large commercial aircraft to attack a prominent center of US power in a best-selling novel some years back. Simply waiting for the FBI to call you about a potential terrorist strike is the next best thing to turning on Fox News or reading the morning paper.

Six Production Elements

In terms of functionality, RMI has six distinct 'production' elements. Their separate areas of focus lead to creating the kind of intelligence that drives top management planning and emergency decision-making. These elements are not a fluid process, but rather parts of the puzzle that make up the RMI picture. However, the RMI process has been condensed into a flow chart (Figure 1).

RMI is composed of six production elements:

- Threat assessment
- Vulnerability assessment
- Hazard assessment
- Operational space visualization
- Event modeling
- Situational awareness.

1. Threat Assessment

Threat assessment is a comprehensive, fused intelligence product that looks at all threats whether man-made, natural or *accidental.* It assesses the likelihood of these threats manifesting themselves. It examines criminal and terrorist events, organizations and agendas. It also looks at political, social, economic or other groupings or trends that could impact on the overall threat to the business.

2. Vulnerability Assessment

Vulnerability assessment is exactly what it is sounds like, an expert evaluation of a facility, company, or site. It is both a process of evaluation using determined criteria and primary research of the physical plant. It assesses strengths, weaknesses, and gaps in terms of physical information and personnel security. By definition, vulnerability is essentially the susceptibility of something to various causal elements potentially leading to a disaster. However, without understanding the nature of the *threat,* it is impossible to assess what exactly is a vulnerability.

3. Hazard Assessment

Hazard assessment is an essential element of operational risk management, which is a five-step process of identifying hazards, assessing these hazards, making risk decisions, implementing controls and supervising. For most in the risk management community, this is done with an eye towards hazardous materials (HAZMAT). Often the hazard assessment is focused on toxic industrial chemicals, industrial materials, and radiological materials, along with physical infrastructure problems that could pose some sort of hazard. It also integrates with the threat and vulnerability assessments to evaluate potential disasters such as flood, fire, earthquake, wind or other natural phenomena. A perfect example of a hazard would be a shipping lane wherein barge traffic could potentially impact with an adjacent or crossing railway bridge, causing a derailment accident.

4. Operational Space Visualization

Operational space visualization is an intelligence area least understood in the business world. It often involves close coordination and public-private integration of the emergency response effort. It is the ability for senior decision-makers to *see* and understand the dynamic picture of what is happening, primarily in an emergency situation.

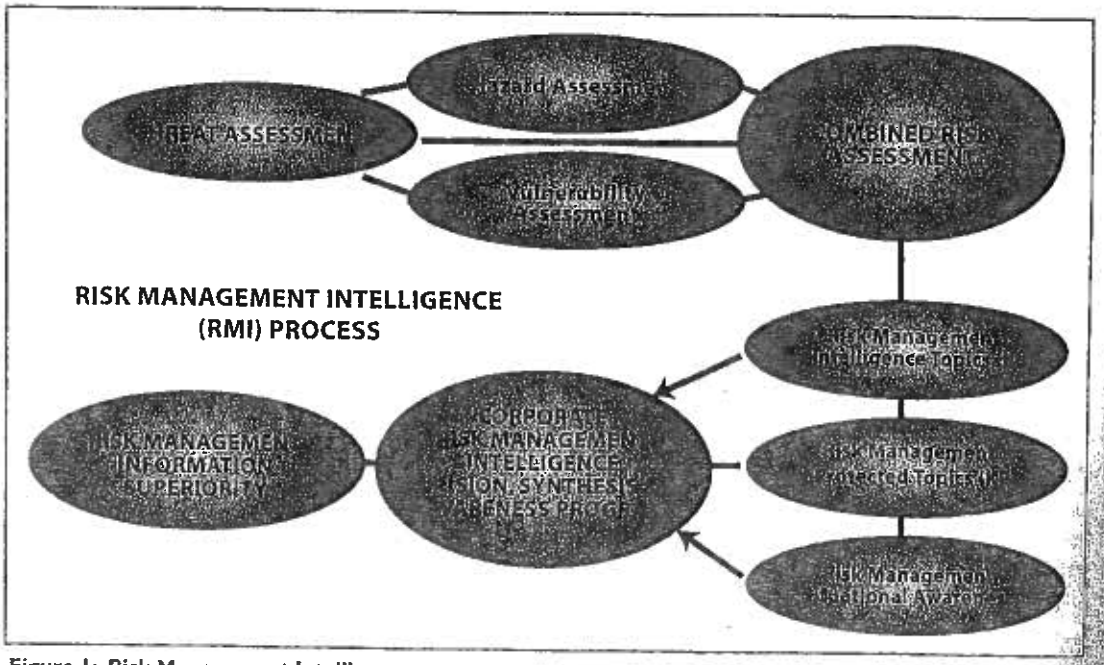

Figure 1: Risk Management Intelligence

This involves physical plant, communications and computers, offices, manpower, finance and accounting, transportation, and a host of other critical business functions. Often it is global in scope, with Gant and Pert chart intricacies to gauge the connected critical paths resulting in a major terrorist event or natural disaster. This all ties into the John Boyd Observation-Orientation-Decision-Action model, or OODA loop, so widely referenced in military management readings.

5. Event Modeling

Event modeling creates a picture and assessment of a chemical, biological, radiological or natural (fire or flood) event. It often focuses on developing a detailed picture of the contamination plume, sometimes in a three-dimensional picture using map-intensive or graphic information system (GIS) software such as Falcon View and a variety of contamination accident depiction software. It provides a *picture* for decision-makers of what the effects on the ground are, where the contamination is and is going, and hopefully where the best places are to establish mitigation infrastructure sites. Most of us probably recall the map of the Persian Gulf during Desert Storm that depicted the intentional oil spills directed by Saddam Hussein. It showed not only where the oil was now, but where the oil spill was going. Similar maps were used during the Exxon Valdez spill in Alaska. Modeling requires highly accurate, detailed and timely weather inputs, which add a facet of planning and support more traditionally found in military vice business intelligence.

6. Situational Awareness

Situational awareness is the art of keeping senior executives informed on what they need to know. It's the ability to understand and track what is happening around us. Most of us had very good situational awareness of the attacks on September 11 due to the extensive media coverage. It all sounds easy in concept, but is daunting in execution. It combines the briefings, reports, emails, phone calls, meetings and all other forms of communication necessary to accurately provide reference and insight into new events, trends, or related subjects. It is not the plan, but much of the foundational understanding that goes into decision-making that drives the planning.

Situational Awareness, or "SA," is driven by such concepts as Key Intelligence Topics (KITs) or Priority Intelligence Requirements (PIRs), or the still used acronym of Essential Elements of Information (EEIs) to establish lanes in the road and desired vistas for examination for the senior executive. Obviously, these are focused on risk management issues for RMI. SA is not an implicitly finished product though, like a periodic CI (competitive intelligence) report, but instead the broader process that keeps decision-makers attuned to events around them at all times.

Decision-Making Support

These six parts are all integral components of an integrated and holistic process that has one simple goal: provide the decision-makers with the information they need to make knowledgeable, sound decisions addressing strategic risk. It is not restricted to evaluating the threat of terrorism, HAZMAT contamination, floods or fire, but as a methodology can be applied to all manner of corporate risk, even expanded to financial or human resources.

While September 11 placed the airline industry in a precipitous state, underscoring the fundamental risks involved with terrorism to the corporate bottom line, the bankruptcies at Enron and WorldCom represent clearly identifiable risks that could have been much more effectively identified and mitigated using a modified RMI approach. There were hazards, vulnerabilities and threats, sometimes these are very tangible, other times not. In all cases, it is an intelligence process that defines them.

Lessons From RMI

Part of the difficulty is effectively modeling an event. Modeling is an interdisciplinary and software intensive effort that is critical for both planning and managing emergency events. Ask GE and Motorola, and they'll both have ample evidence of just how legally and economically compelling accurate contamination modeling can be for senior executives trying to make strategic decisions. To help key executives visualize what could happen or what is happening requires synthesizing and analyzing large amounts of data to turn it all into an easily understandable, timely and accurate visual representation.

> RMI is an integrated process that ties together security and top management in a synergistic effort to better understand and make decisions regarding risk.

At its essence, RMI is an integrated process that ties together security and top management in a synergistic effort to better understand and make decisions regarding risk. Rather than the Security Manager having to constantly convince senior managers that there is an investment in security that *must be done*, RMI provides a body of empiricism or substantive research and analysis that enables the decision-maker to better judge what actually needs to be done.

Too many Security Managers rely on an experience-driven vice intelligence-driven approach, which puts their senior executives at a disadvantage in having to gauge risks, threats, and vulnerabilities by themselves. Such a legacy approach is often the *trust me* method that has been the subject of so many business failures or MBA program case studies.

RMI provides the tools for sound decisions; it greatly removes the 'risk' associated with blind faith in a single manager or managers in a specialized area. For the risk and security managers, it allows them to articulate their professional opinions without having to ultimately say, *trust me*, but instead being able to confidently say, *this is what the intelligence is showing us*

and my assessment is. . . . For CI practitioners, this is an integral approach towards revalidating the inherent value of a dedicated intelligence operation supporting decision-making. Rather than simply being an adjunct to marketing, finance or business development, the "CI shop" provides multi-disciplinary support to managing risk for the organization or corporation, to include becoming an indispensable piece of the risk manager's tool kit.

Superficially a security or risk manager may see a strong RMI component as a competitive threat to their positions in the firm. Often, security and risk management is only seen as an expense with a very difficult to define return on investment. Adding an intelligence component can be seen as adding garnish to a main course that senior executives don't really enjoy anyway, and would rather not have to partake — except that it keeps their companies healthy.

In The End, Reducing Risk

RMI is the foundation for a sound risk management program. It allows executives to make superior decisions because they have superior information. RMI develops a framework, a deliberate shaping to the decision-space (cognitive parameters in which decisions are made) where a very asymmetric crisis or potential crisis can be planned for or mitigated in a rational and manageable manner. Our current system of haphazard *risk* or *threat* information flow are often quick information dumps on top executives, resulting in poorly conceived decisions.

The general lack of risk management situational awareness at senior levels is a flawed approach that is quickly becoming apparent in the post-September 11 world in which we all live. Managing risk well is the new business discipline, and it is one that will demand the same level of executive knowledge and intensity of effort as marketing, operations or administration to keep a company successful, or to ensure its survival. RMI is the key to unlocking the superior information that will result in superior decisions.

Hal Kempfer is the president and founder of Knowledge and Intelligence Program Professionals (KIPP at www.kipp-intelligence.com*) in Long Beach, California, and has about 15 years in 'intelligence' covering the spectrum of business or competitive, military and law enforcement or investigative intelligence. LtCol Kempfer USMCR recently completed a one-year recall to active duty as the Director(s) of Intelligence (G-2 and J-2) here in the United States and overseas of two different expeditionary organizations, one being the first Combined (coalition) Joint Task Force for Consequence Management.* HalKempfer@KIPP-Intelligence.com