Volume 2, Number 1, Spring 2004

# Journal of Competitive Intelligence and Management

## Introduction



scip

# Journal of Competitive Intelligence and Management

The Journal of Competitive Intelligence and Management (JCIM) is a quarterly, international, blind refereed journal edited under the auspices of the Society of Competitive Intelligence Professionals (SCIP). JCIM is the premier voice of the Competitive Intelligence (CI) profession and the main venue for scholarly material covering all aspects of the CI and management field. Its primary aim is to further the development and professionalization of CI and to encourage greater understanding of the management of competition by publishing original, high quality, scholarly material in an easily readable format with an eye toward practical applications.

**Edited by Craig S. Fleisher (fleisher@uwindsor.ca) and John E. Prescott (prescott@katz.pitt.edu )**

## Editorial Board

# Business Intelligence for Canadian Corporations after September 11 [1]

*François Brouard*
*Eric Sprott School of Business, Carleton University*

## Executive Summary

The crisis provoked by the events of September 11, 2001, has some important implications for corporations in Canada and abroad. These events made it clear that corporations need to learn how to achieve the best performance possible in the face of crises in order to survive through difficult times. Both managers and employees need to think about and understand the consequences of the new environment that exists in the wake of the international terrorism crisis. In their daily and strategic planning activities, corporate management must respond to the risks they face with appropriate business intelligence.

The purpose of this article is to present some reflections on the defensive and offensive dimensions of business intelligence in relation to the September 11 events, to sketch the consequences of these events for Canadian corporations, and to propose some actions that can be taken to improve the preparedness of corporations for future similar events or for other crises.

The introduction briefly presents the September 11 events and some important elements of its associated context. This is followed by a discussion of conceptual frameworks to guide reflection on the crisis within the business intelligence perspective. Next, a presentation of some of the implications of the September 11 events for Canadian corporations is provided. The article concludes with recommendations regarding some business intelligence actions that can be taken to prepare and respond to terrorism.

## Key Words

business intelligence, environmental scanning, September 11, crisis management

## About the Author

**François Brouard** is a faculty member in the Eric Sprott School of Business at Carleton University in Ottawa, Canada. François is also an ABD doctoral candidate in the doctorate in business administration

(DBA) program at Université du Québec à Trois-Rivières. He is in the process of developing a diagnostic tool for environmental scanning practices in small and medium-sized enterprises.

Email: francois_brouard@carleton.ca

## Introduction

The mere mention of "September 11, 2001" brings instant memories to our collective mind. The World Trade Center and Pentagon tragedy of September 11, 2001, is a contemporary historical moment, and one of the most dramatic acts of terrorism ever perpetrated. The televised image of the twin towers hit by the two airplanes and their subsequent collapse will never be forgotten.

But even though the magnitude of the September 11 tragedy has increased its reality, terrorism is not a new phenomenon (Carter, Deutch & Zelikow, 1998; Thompson, 2002). Just a few examples from around the globe include the 1985 explosion off the coast of Ireland of the Air India flight from Toronto, the World Trade Center bombing in 1993, the 1995 nerve agent attack in the Tokyo subway by the Aum Shinrikyo group, the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City, the bomb that exploded at Olympic Park in Atlanta in 1996, the 1996 Paris Metro bombing, the bombing of the U.S. embassies in Kenya and Tanzania in 1998, and the recent suicide bombings in the Middle East (Canadian Security Intelligence Service, 1999; Fleming, 1998; Levitin, 1998).

The Canadian Security Intelligence Service (CSIS) has made several statements regarding terrorism and Canada. "The threat to Canadians and Canadian interests abroad from international terrorism continues to be largely a matter of 'being in the wrong place at the wrong time'" (Canadian Security Intelligence Service, 1999). "The vast majority of terrorist activities in Canada relate to the support of actions elsewhere that are linked to homeland conflicts" (Canadian Security Intelligence Service, 1999). Activities in Canada include providing a safe haven for terrorist or terrorist supporters, fund raising, procuring weapons and material, coercing and manipulating immigrant communities, and facilitating transit to and from other countries. The recent Ahmed Ressam case is a good example of these activities. According to the Canadian Security Intelligence Service (2002b), Canada is also "confronted by domestic terrorism issues related to aboriginal rights, white supremacists, sovereignty, animal-rights, and anti-globalization issues."

Terrorism can be defined in many ways (Alexander & Alexander, 2002; Fleming, 1998). For our purposes, a broad definition will be adopted. Terrorism is a premeditated violent act to intimidate or coerce a government, the civilian population or an organization, in furtherance of political, social or economic objectives. This definition encompasses kidnappings, hijackings, shootings, bombings, espionage, cyber attacks, and attacks involving weapons of mass destruction (nuclear, biological or chemical).

Terrorists, like the competitors of an organization, can benefit from information leakage or inappropriate disclosure. They might obtain information through gossip at a trade show, papers presented at a conference, help wanted advertisements, airplane or restaurant discussions, supplier knowledge, sales pitches, company press releases, business friendships, poker games, or off-site relationships (Fuld, 1989).

All organizations, whether public or private, for profit or not-for-profit, are subject to possible dramatic effects from terrorist activities. Some firms' very survival could be endangered by the direct or indirect effects of terrorist acts. Following the September 11 events, travel was disrupted not only in the United States but also in Canada and Europe, and many conferences and festivals were cancelled (Marketing Magic, 2002; Taylor & Enz, 2002).

Organizations are affected by every facet of their external environment. Since the world has changed, our thinking too must change (Grimaldi, 2002). Organizations need to be more aware of their external environment and of how it may affect them (Aguilar, 1967; Garg, Walters, & Priem, 2003; Peteraf, 1993; Raymond, Julien & Ramangalahy, 2001). Managers should adopt the tools that will help them to become aware of their environment and deal with crisis management. One such management tool, business intelligence (BI), is a recognized means of assistance for managers. The informational process by which an organization stays attuned to its environment in order to make decisions and then act in pursuit of its

objectives is called environmental scanning. Business intelligence is the output resulting from that process.

The purpose of this article is to present some reflections on the defensive and offensive dimensions of business intelligence in relation to the September 11 events, to sketch the consequences of such events for Canadian corporations, and to propose some actions that can be taken to improve the preparedness of corporations for future similar events or for other crises.

The article is organized as follows. After this brief description of the context of the September 11 events, a conceptual framework to guide reflection on the crisis within the business intelligence perspective is presented. Next, a discussion of the implications of the September 11 events for Canadian corporations is provided followed by a description of specific actions that can be taken.

## Frameworks to Help Understand the Consequences of Terrorist Acts for Organizations

To help understand and guide reflection on the terrorism crisis, this section will suggest some conceptual frameworks. The literature on crisis management is helpful in providing a framework for crisis analysis in general and terrorism as one specific type of crisis. One of the phases of the crisis management process (signal detection) can be directly linked with environmental scanning and business intelligence activities. A framework is also provided to assess organizational vulnerabilities to acts of terrorism and to orient the business intelligence process.

### Crises, Crisis Management and Early Warning Systems

Various kinds of crises can have an impact on organizations; a terrorist attack is one of the most significant. Other potential crises include extortion, hostile takeover, product tampering, copyright infringement, environmental spills, computer tampering, a security breach, a product/service boycott, malicious rumour, natural disaster, bribery, information sabotage, plant explosion, sexual harassment within the company, the escape of hazardous materials, product recall, counterfeiting and executive kidnapping (Mitroff, Pauchant & Shrivastava, 1989a, 1989b; Pearson & Clair, 1998). Some crises are smaller, with short-term, minor impacts; other crises, like the 9/11 events, are larger, with long-term or permanent impacts.

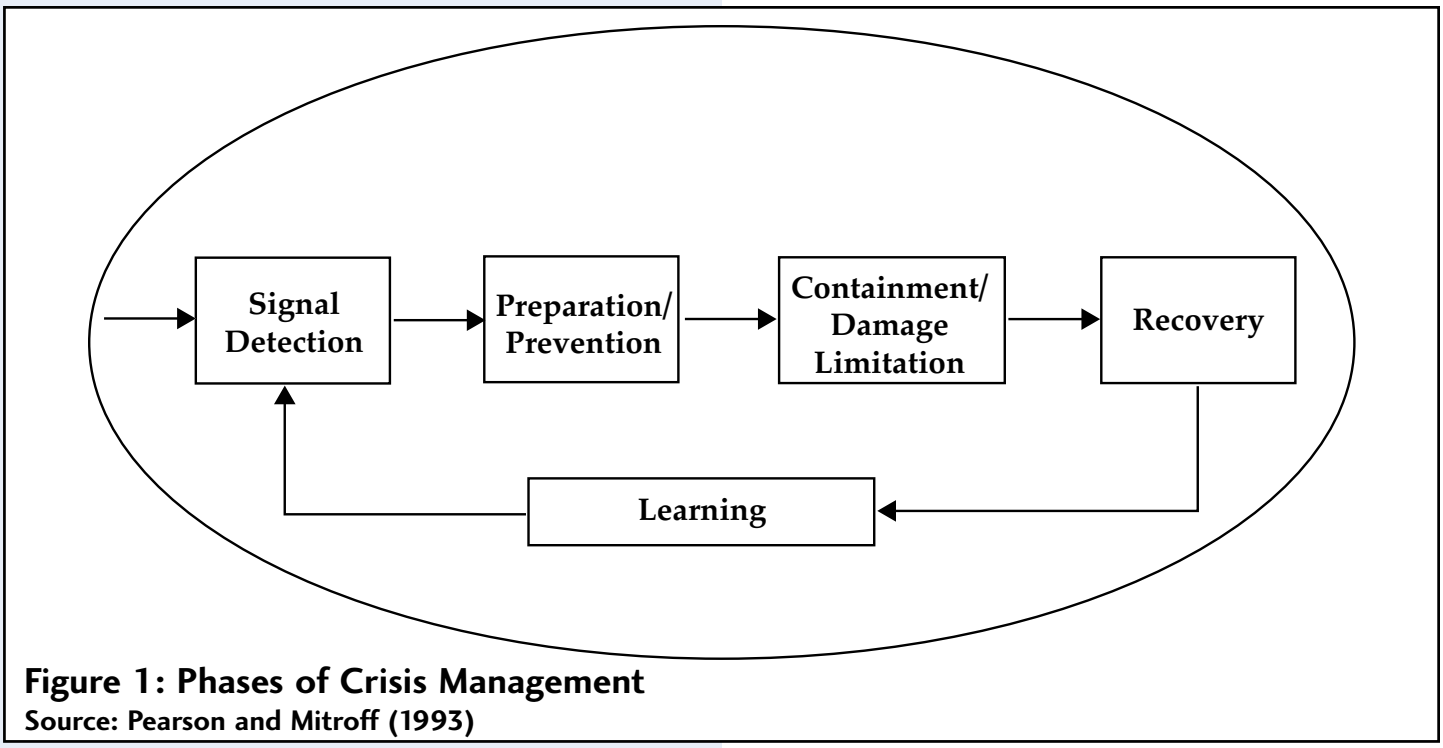


**Figure 1: Phases of Crisis Management**
**Source: Pearson and Mitroff (1993)**

"Crisis management is a systematic approach that engages the whole organization in an effort to avert crises that may affect the firm, and to effectively manage those that do occur" (Pearson, 2002). Based on the works of Mitroff (1988) and Pearson and Mitroff (1993), the crisis management process may be divided into five phases: (1) signal detection, (2) preparation/prevention, (3) containment/damage limitation, (4) recovery, and (5) learning. Figure 1 illustrates these five phases. The crisis management process can be viewed at many levels, such as societal, organizational, or individual.

Crises, viewed with hindsight, leave a trail of early warning signals. Terrorism crises are no exception, as Quinn (1996) illustrates, using the 1995 attack in Tokyo by the Aum Shinrikyo group. It is important, therefore, to have a signal detection mechanism. Business intelligence represents one important type of early warning signal system. Preparation/prevention mechanisms involve probing for any sign of weakness and testing the responses. Gray (2002) reports that a weakness in the communication system between police and fire departments on September 11 may have contributed to the death of firefighters in New York City. It is not possible to avert all crises; some will inevitably occur. Damage containment mechanisms prevent the damage from spreading and limit its effects.

Recovery mechanisms relate to both short-term and long-term business recovery. One example of a recovery mechanism is establishing an alternative site for computer operations. The learning phase involves reflection and critical examination of the lessons learned after a crisis. All five phases of crisis management will be present for both shorter and more permanent crises. The main difference between temporary and permanent crises is that a change in awareness regarding security usually results from permanent crises.

## Defensive and Offensive Intelligence Frameworks

As the crisis management process emphasizes, an early warning signal system is an important phase. Environmental scanning could be defined as an informational process by which an organization stays attuned to its environment in order to make decisions and then acts in pursuit of its objectives. Through environmental scanning, an organization monitors information from its external environment that is relevant to its internal environment (Aguilar, 1967; Bourgeois, 1980; Daft, Sormunen & Parks, 1988; Elenkov, 1997; Fleming, 1998; Thomas, Clark & Gioia, 1993). Business intelligence is the result of that process. Other terms used to describe concepts similar to environmental scanning are Competitive Intelligence (CI) and Strategic Scanning. As the terminology is still in flux, this article will use environmental scanning and business intelligence interchangeably as comprehensive terms that include both process and results (Brouard, 2000).

Before environmental scanning can take place, an organization needs to know where to look and what to scan for. If the company is a software development firm, for example, scanning is directed towards other technology that could affect the product or its creation. Environmental scanning may be viewed as a global process, which can be divided into four different types of more specific processes (Brouard, 2000; Daft & Weick, 1984; Jennings & Lumpkin, 1992; Martinet & Ribault, 1989):

1. Technological scanning is concerned with the technological dimension of an organization's product, service or production process.
2. Competitive scanning is related to actual and potential competitors. In the case of terrorism, the focus is not on the competitors but on a more imprecise set of actors. This type of scanning affects all the other scanning processes.
3. Commercial scanning involves the clientele dimension and the supplier dimension.
4. Socio scanning is concerned with all other elements, such as demography, economic, socio-cultural, political, and others.

The process of scanning itself is termed the intelligence cycle. Usually the intelligence cycle is represented as a four-phase cycle: planning, collection, analysis, dissemination (Kahaner, 1996; Ghoshal & Westney, 1991; Hambrick, 1982; Miller, 2000; Peyrot, Childs, Van Doren & Allen, 2002). In the planning

phase, the organization identifies the intelligence needs of its management team. Collection is the acquisition of relevant data. Analysis creates information by linking data together and by identifying patterns and trends. During the dissemination phase, results of the completed work are transmitted to decision makers.

In addition to the usual presentation of the intelligence-gathering cycle, with the four phases just described, an important component of the intelligence process is protection (Nolan & Quinn, 2000; Pattakos, 1997). During the planning phase of this component, organizations, knowing that it is impossible and costly to protect everything, identify critical assets and determine the protection requirements for them. Vulnerability analysis assesses the weaknesses that may exist in relation to protection needs. Risk and threat assessments provide an estimation of the potential effects of vulnerabilities on organizational activities, which will serve as a basis in designing the measures required for protection and security. Protection measures include a counterintelligence role and a security role, counterintelligence to safeguard information from collection by others, including terrorists, and security to enforce the laws and protect against criminal attacks (Francq, 2001).

In Figure 2 , the gathering cycle is shown on the right side and the protection cycle is presented on the left side. As in the crisis management process, a final loop is the learning phase in which past actions are evaluated and appropriate future actions are undertaken.

One more concept needs to be underscored about this global intelligence process: it can act offensively or defensively. The offensive dimension is present when collection is oriented towards the identification of opportunities or when protection consists of disinformation as a protective means. The defensive dimension is present when collection is oriented towards the identification of existing threats, and this dimension applies in most protection and safeguarding measures.

The two sides are linked in their application and represent a continuous, dynamic flow. They may be viewed as two sides of the same coin, or as the yin and yang of the intelligence process. For example, more dissemination activities for employees and management within an organization provide more information for competitors, if protection measures are not in place to control or limit information dissemination.

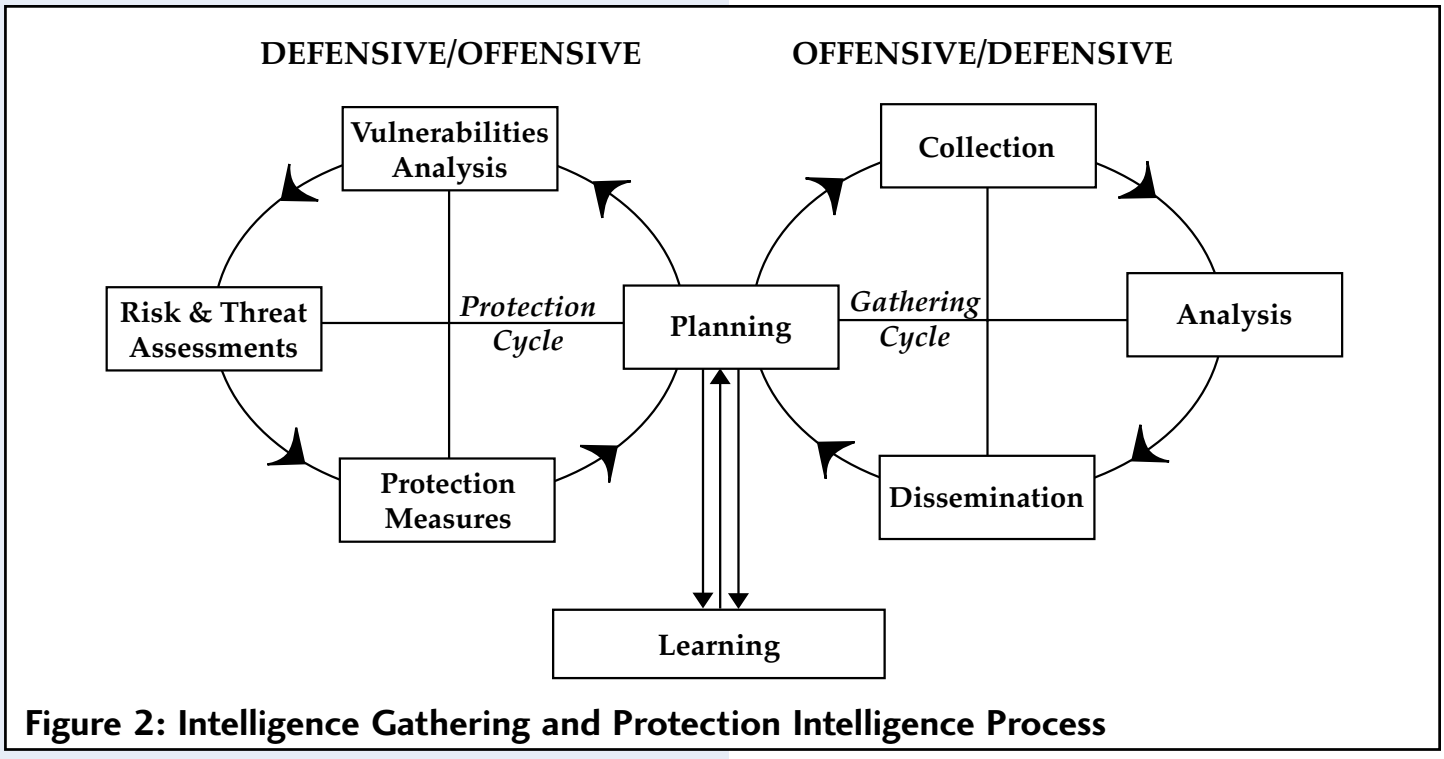


**Figure 2: Intelligence Gathering and Protection Intelligence Process**

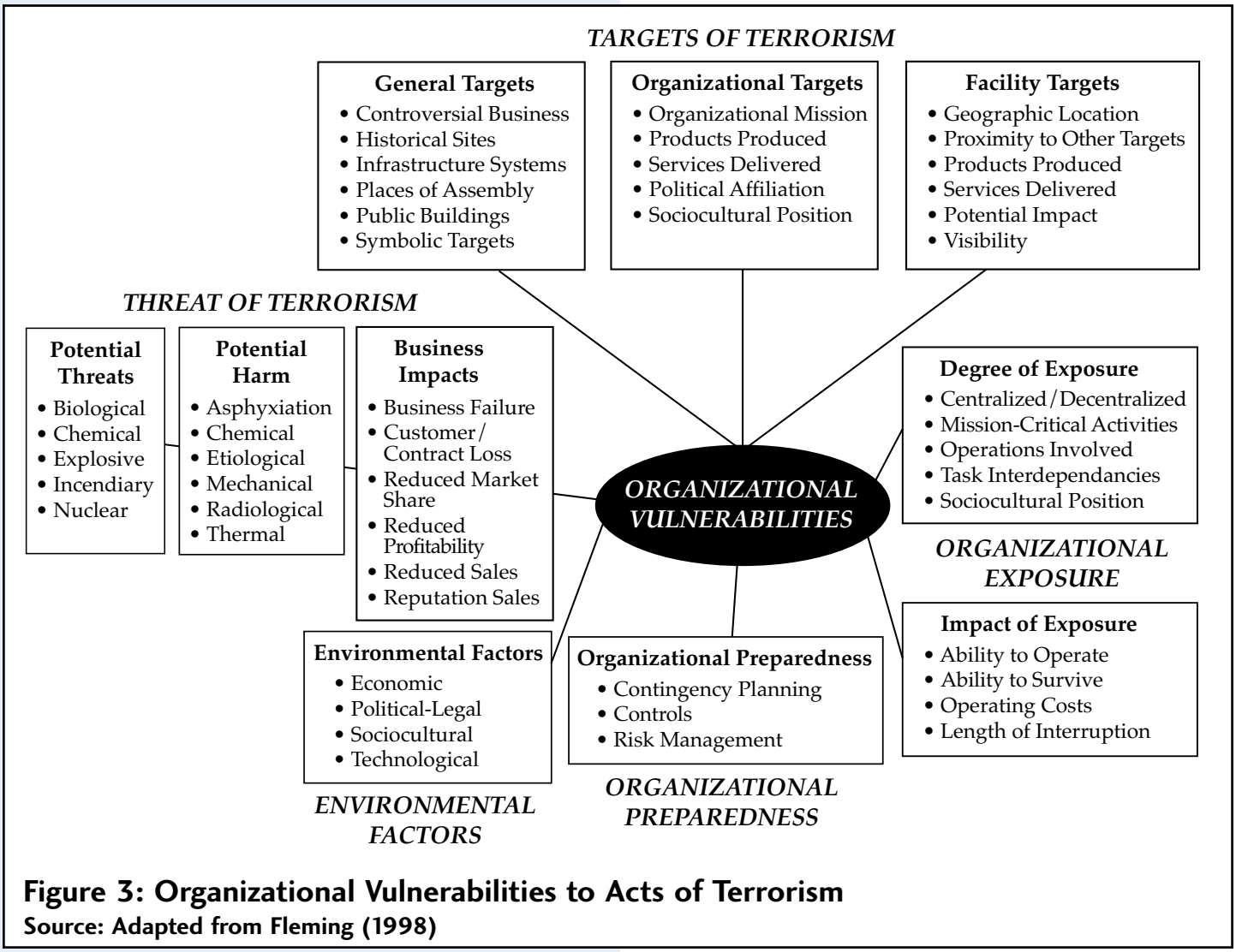


**Figure 3: Organizational Vulnerabilities to Acts of Terrorism**
**Source: Adapted from Fleming (1998)**

## Assessing Organizational Risks and Vulnerabilities to Acts of Terrorism

An important component of the protection intelligence process is the vulnerabilities analysis. In assessing organizational vulnerabilities, managers determine which assets (information and infrastructure) are critical for them. Fleming (1998) provides an interesting framework for assessing organizational vulnerability to acts of terrorism. It is presented in Figure 3. The five categories of the framework are the threat of terrorism, the targets of terrorism, environmental factors, organizational exposure, and organizational preparedness. Each area has its own components.

The 'Threat of Terrorism' category includes potential threats, potential harm, and business impacts. The 'Targets of Terrorism' category can be divided into general targets, organizational targets, and facility targets. Which targets are on a terrorist's list depends on the objectives of the terrorists. The World Trade Center Towers and the Pentagon are public buildings and were also symbolic targets for the terrorists involved; hence they fall under the category of general targets. The category of 'Environmental Factors' refers to the external environment. In the case of the 9/11 tragedy, there was an important socio-cultural dimension. The 'Organizational Exposure' category of an organization is divided between the degree of exposure and the impact of exposure. The category of

'Organizational Preparedness' includes all the steps required for preparation.

## Implications for Canadian Corporations

This section develops the implications of terrorist events for Canadian corporations. The implications for corporations are examined from three perspectives, with direct and indirect consequences for each. The three perspectives are the governmental level, the general organizational level and, more specifically within the organization, the intelligence-gathering process.

### Governmental Level

Immediately following the September 11 tragedy, North American society entered an era of profound changes that have had impacts on citizens and on the business community. Governments have responded with revisions of existing legislation and the introduction of new laws.

The Canadian Anti-Terrorism Act came into effect on December 24, 2001 (Canadian Security Intelligence Service, 2002a). This new Canadian Act amended or introduced legislation regarding the Criminal Code, the Official Secrets, money laundering and terrorist financing, access to information and privacy, Canadian Security Intelligence Service, National Defense, and charities registration. It takes into account new realities, including new players (governments of traditional states, governments-in-waiting, governments in exile, other foreign powers, terrorist groups) and new threats (against ethno-cultural communities in Canada, trade secrets, and essential infrastructure).

The United States has taken several actions following the tragedy, such as the USA Patriot Act, creation of the Office of Homeland Security, law enforcement actions, and creation of barriers to terrorism funding (Alexander & Alexander, 2002; U.S. Office of Homeland Security, 2002). The U.S. government already had in place the Economic Espionage Act of 1996 regarding the protection of proprietary economic information (Pooley & Halligan, 2000). On the international front, the aim of the United Nations Security Council resolution 1373 is to freeze the assets of those associated with terrorist activities (Canadian Security Intelligence Service, 2002b). Governments, especially those in North America, have addressed the problem by allocating new funds and by varying the allocation of resources between programs and priorities (Canadian Security Intelligence Service, 2002b; Newton, 2002).

The September 11 tragedy may well have an impact on our democratic way of life, the liberties we have come to take for granted, national and local security, the free market system, and other aspects of our society and culture. The security measures that have been adopted carry with them the risk of infringement on individual liberties and civil rights such as freedom of expression, freedom of religion, freedom of movement, property rights, and freedom from unlawful discrimination (Canadian Security Intelligence Service 2002a; Hughes, 2001; McGoey, 2001; U.S. Office of Homeland Security, 2002).

One potential risk to the right of privacy, for example, is the collection by government security establishments of private communications (Hughes, 2001). Longer waiting times while passing through airport security and armed presence in public places are also direct impacts of the tragedy. As another example, the barriers outside buildings like the U.S. embassy in Ottawa withdraw some public space in exchange for a higher perception of security.

### Organizational Level

Terrorism can have important business impacts on corporations (Alexander & Alexander, 2002). As Figure 3 shows, potential business impacts are multiple: business failure, customer loss, contract loss, reduced market share, reduced profitability, and reduced sales. Following 9/11, some transactions were cancelled or delayed; corporations experienced difficulties with sourcing, inventory levels, and logistics; there were disruptions to manufacturing and distribution; corporate security augmented in importance; and some corporations had trouble with debt repayment. In addition, enterprises face increases in financial scams and fraud (Blakeley, 2002) and in economic espionage (Canadian Security Intelligence Service, 2002b) since September 11.

As Alexander and Alexander (2002) have stated, the 9/11 "attacks damaged confidence and lessened

demand, leading companies to reduce production, eliminate business units, freeze investments, and dismiss workers." The impact of 9/11 on a short-term basis was real and severe. The evidence includes declines in stock markets, declines in capitalization of corporations in selected sectors (e.g., airlines and insurance), and fluctuations in commodity prices such as oil and gold (Alexander & Alexander, 2002). The attacks didn't help the economy, but it is difficult to attribute a direct causal link to a specific terrorist act. As a mediating factor, the U.S. economy, like the Canadian economy, was on the brink of recession prior to September 11, 2001.

Impacts vary, too, depending on industrial sector. Sales increased for defense, newspapers, security equipment, and health related items, and decreased for airlines, tourism, hospitality, real estate, media, and sporting goods sectors (Alexander & Alexander, 2002; Bhonslay, 2002; Bourassa, 2002; Taylor & Enz, 2002). "At Air Canada, reservations declined by 30% and place occupancy fell by 50% several weeks following the September 11, 2001 terrorist attacks. This decline led to 5,000 jobs cut, the grounding of 84 aircraft, and the reduction of flight schedules by 20%. In late October 2001, the Canadian government provided $45 million to Air Canada to compensate the carrier for losses sustained in the aftermath of the September 11 incidents." (Alexander & Alexander, 2002)

The tragedy highlighted business vulnerabilities and risks with regard to crisis. Insurance protection was affected: there were problems with some coverage and an increase in premiums. The costs of reducing risks in corporations include such precautions as adding new security guards, providing security training, and purchasing surveillance, bomb and chemical agent detection equipment (Alexander & Alexander, 2002). The risks are present and their costs should be examined.

## The Intelligence-Gathering Process

The intelligence-gathering or environmental scanning process occurs within the internal environment of the organization. In addition to the organizational strategy, the internal environment encompasses the culture, the management leadership, the resources, and the structure of the organization (Liu, 1998; Strand, 1983). Each component of the internal environment has a counterpart in the intelligence process.

The September 2001 tragedy underlines the importance of some of these components. As the crisis management literature points out, early warning signal detection is an important part of a complete management system. The 9/11 events increased awareness of the importance of an early warning signal system. One result has been an improved corporate culture in terms of knowledge, which is considered the lifeblood of an organization (Davenport & Prusak, 1997). Another has been the improvement of values sharing among organization personnel. On the other hand, some organizations have also encountered ethics stretching and morality problems. The 9/11 events also resulted in greater receptiveness on the part of management teams. Buy-in by the management team decreases resistance to change and to business intelligence implementation (Hambrick, 1981).

The heightened awareness of security has increased pressure in the area of personnel. It has become more difficult to find security personnel, and the cost of hiring security personnel has increased (Bronskill, 2002). Miller (2002a) found that it is now easier for former government intelligence officers to sell their previously "unacceptable" skills to corporations. With the retirement or death of their personnel, corporations may be faced with the replacement of key employees, some essential to operations.

Another problem that surfaced during the crisis was the incompatibility of communication equipment. Problems in communication between the fire and police departments in New York may have caused the deaths of some firefighters; this was an important lesson learned during the September 11 events (Gray, 2002). A crisis requires a crisis management team and an incident command system that has been prepared in advance and can spring into action at a moment's notice.

In a recent survey of 118 competitive intelligence professionals representing 25 industries in 7 countries (including Canada, but primarily the United States), Miller (2002a; 2002b) examined the status of competitive intelligence after 9/11.

Among the results: 32% (governments) and 53%

(corporations) have found it more difficult to gather information from government and corporate websites. Since 9/11, 49% have experienced differences in the willingness of people to talk with them when they conduct primary research. Since it is difficult to get people to talk, a majority of respondents (54%) think practitioners are working more in the "grey area" now than they have in the past. The research targets, methodologies and budgets have changed for 72% of respondents. Since 9/11, a majority of respondents (58%) have changed the way they protect their proprietary information and 68% have heightened their security efforts.

## Action

Business intelligence is an activity geared towards action. Managers and directors must take action in all phases of crisis management (Canadian Institute of Chartered Accountants, 2001). Using the frameworks presented above, this section suggests some actions that corporations can take to protect themselves from a terrorist attack. Action measures regarding terrorism are oriented primarily towards the defensive dimension, in particular that of the protection intelligence process. Protection measures include both counter-intelligence and security (Nolan & Quinn, 2000). In accordance with the crisis management process, this section is divided into five sub-sections: awareness, preparation, protection, recovery, and learning.

Before proposing actions that can be taken, it is essential to examine the internal environment of the organization in terms of the intelligence process. The strengths and weaknesses of the intelligence process can be assessed by an audit or diagnostic of the organization's practices (Brouard, 2002; Sawka, Francis & Herring, 1996). The audit systematically evaluates current capabilities and deficiencies, and performs a vulnerabilities analysis, a risk assessment, and a threat assessment. The audit can focus on the culture, management/leadership, resources, and structure of the corporation and on each phase of the intelligence-gathering and protection intelligence process. Information should be considered as an asset by corporations, and bearers of bad news should be recognized for their contributions. Finally, it is important that countermeasures be subject to a cost-benefit analysis and evaluation (McGoey, 2002; Nolan & Quinn, 2000).

### Awareness

Awareness of the danger of terrorism and of the security required to prevent it is the most basic countermeasure (Desmond, 2001; Fuld, 1989; Levitin, 1998). Corporations should initiate employee awareness programs to increase user awareness by means of education and sensitization of all employees to the threat that terrorism may pose to job security and the organization's economic well-being. Such training can take the form of a formal education program or short-term informal programs such as briefing employees before trade shows. The programs should emphasize the sharing among all employees of responsibility for adhering to effective security policies and practices. Employees should be aware of their surroundings. Outside consultants or government programs, like the Canadian Security Intelligence Service national liaison/awareness program, can be of considerable help in this process.

### Preparation

It is recognized that effective response to terrorist crises or other crises depends on being prepared (Adams, 2002; Lanter Brown, 2002; U.S. Office of Homeland Security, 2002); this means being ready when the crisis arises. Preparation is helpful for the next stage, containment and damage limitation. The intelligence-gathering process offers a system of identification of potential risks for the corporation based on the information available.

Preparation requires planning for emergencies and testing the plan. Planning consists of setting a corporate disaster or emergency plan with very detailed information (Howard, 2002). The plan should include an exhaustive list of protective equipment and identify the persons who will take responsibility in the emergency. Plans must include policy and procedures for the corporation. For example, they could include mutual aid agreements with other organizations and the sites of recovery, if needed. The plan should be tested regularly for effectiveness. Inspection and testing of all emergency equipment and disaster practice drills, like fire drills, are examples of testing. Learning will come from the testing and will help to improve the corporate response.

## Protection

Protection measures include the protection of intangible assets, such as information (counter-intelligence), and the protection of physical assets (security).

Deception, or perception management, is one offensive information protection measure (Shaker & Gembicki, 1999). With deception, the aim is to confuse intelligence-gathering by competitors, including terrorists (Francq, 2001). Deception must be carried out with great caution to avoid use of false information by customers, partners, or industry analysts. With today's highly developed technology and convenient media access, information could be stolen or lost very easily.

For the protection of intangible and physical assets, vulnerabilities may be divided into five categories: operations, documentation, personnel, physical, and technical (Barrett, 2001).

Acts of terrorism require heightened diligence in the course of operations in investigating domestic and international clients and partners to ensure that entities with whom one conducts business are not fronts for domestic or international terrorists (Alexander & Alexander, 2002; Barrett, 2001).

The same applies to suppliers. Corporations should proceed with client background checks and selection supplier procedures. Contracts should be reviewed for cancellation of events clauses for acts of terrorism and other crises (Schuh, 2002). Signed contracts should contain non-disclosure agreements and appropriate legal boundaries in the administration and handling of information. In the presence of guests, information should be secured on a need-to-know basis. Following the recent anthrax episode, mail precautions in the form of identification and proper handling of suspicious packages in the workplace is necessary. Procedures should include precautions in case of attacks involving a variety of biological or chemical weapons.

Documentation and sensitive materials are essential assets and should be protected from leaks and overly broad dissemination (Canadian Security Intelligence Service, 2002a; Fuld, 1989). Spies and terrorists will probably not hesitate to "dumpster-dive," transforming trash into treasure. Some measures that can be taken to safeguard information are appropriate classification, control, and physical protection of sensitive documents. A classification system for documents should have the following categories: public, internal, confidential, secret, top secret. The classification system should apply not only to employees but also to suppliers and partners. Someone should be responsible for reviewing public relations documents or any public documents the firm releases, including conference papers and elimination of non-compliance information from government files.

Other suggestions for protection are proper storage and disposal of sensitive documents, requiring employees taking surveys to know the company and individual surveying them, requiring the surveyor to furnish a copy of the final product, limiting strategic in-house publications to employees only, posting announcements deemed sensitive in secure or compartmentalized portions of the building, requiring the press to send copies of all articles featuring personnel or the company and to submit a complimentary copy to the firm prior to its public production, establishing procedures for discarding classified information, and destroying carbons (Helms, Ettkin & Morris, 2000).

The hiring and managing of personnel is another source of vulnerability. Suggestions for corporations include proper training to improve awareness, background checks before hiring, a badge system to compartmentalize the access right of an employee, employee contracts with non-disclosure agreements, discussion of sensitive company matters in appropriate locations, establishing a copier and faxing protocol, and establishing procedures for employee termination (Barrett, 2001; Helms, Ettkin & Morris 2000; Lachnit, 2002).

Physical vulnerabilities can be addressed in many ways, including locks, alarms, guards, gates, guns, or dogs. Among physical measures, suggestions from the literature include using computerized access control systems, video surveillance systems and security cameras, bomb-detection devices, x-ray equipment; locating printers, computers, and fax machines in appropriate areas; fortifying plants and storage facilities; placing locks on drawers or doors to rooms with sensitive materials; using safes, security guards, and investigators; having guests escorted in and out of the building, requiring them to wear badges that clearly indicate floors they are allowed to visit, and to routinely prove their identity; controlling access electronically; and placing realistic controls on employ-

ees' and visitors' access to sensitive facilities, materials, etc. based on the "need to know" principle (Helms, Ettkin & Morris, 2000; Hodgson, 2002).

Technical vulnerability is a more specific kind of physical vulnerability, embodied as it is in cyberspace and information technology. Among technical countermeasures, suggestions include using encryption devices; analyzing log-ins; using and regularly updating anti-virus software and firewalls; carefully examining non-commercial programs; storing all downloads on floppy discs rather than the hard drive; stopping hostile attachments at the e-mail server; utilizing filters for e-mail; separating internal network and external servers; ensuring intrusion detection; restricting access with passwords; regular back-up of data; protecting computer databases and network links from unauthorized access; preventing creation of electronic back doors by programmers; exercising sensitivity and caution in the choice of medium used for business communications (i.e., cellular telephones, open fax); using a secure line and a room protected from radiation; regular clearing of hard drives, print queue, Internet caches; clearing out of hard drive before disposal; closing of unused accounts; regular training; employing a security manager; and trusting no one (Desmond, 2001; Helms, Ettkin & Morris, 2000; Moser & Borry, 2001; Technews, 2002).

### Recovery

Even with the best warning system, preparation and protection, it is impossible to avoid all crises, in particular those that are created by terrorists. A recovery plan permits the continuity of business operations in both the short term and the long term. Recovery plans should address all the core and critical activities involving information, computers, and operations. An incident command system should be deployed immediately upon a crisis arising. In addition to physical and operational recovery, psychological recovery measures for employees should be in place, if needed.

### Learning

Following a crisis, an examination is necessary to learn from the crisis and improve the future reaction to the next crisis. Simon and Pauchant (2000) suggest three levels of learning that managers can derive from the experience of crisis: behavioural, paradigmatic, and systemic levels. Learning also takes place at the individual and organizational levels. At the behavioural level, the aim is to pursue the same goals as before by modifying or amplifying the means used. One example is to increase the frequency of password changes. The paradigmatic level offers the possibility of radically changing the means used. It helps managers re-examine their old paradigms and modify them, when necessary, to take a totally new conceptual approach to they way they operate. The systemic level leads to a better global understanding and better strategies when dealing with very complex issues, such as international terrorism.

## Conclusion

The events of September 11, 2001, are a serious wake-up call for all of us. They are an indication that the world and the nature of the threat environment has changed, and our thinking has changed as a consequence. In some respects, the new environment is not totally new; change had already begun before that fateful day. In that sense, the events of September 11 were a proof as well as a cause of change. Every person and corporation will have to learn to adjust to change in the environment. Environmental scanning and business intelligence can assist in this learning by issuing early warnings to corporations. Business intelligence can help Canadian corporations rise to the challenge of crisis management and initiate new thinking.

The main lesson learned from the September 11 attacks is that we are vulnerable and we should prepare and protect ourselves, individually and collectively. Preparation and protection are essential if Canadian organizations are to survive. Even if Canadian organizations are, fortunately, less likely than the United States to become direct targets for terrorists, no organization can afford to discount a potential impact resulting directly or indirectly from terrorist activities. Our proximity to and our close relationship with the United States puts us at risk.

The events of September 11 have heightened our fears and highlighted vulnerabilities. "Terrorism today is more complex, more extreme, more sophisti-

cated, more transnational than ever before" (Canadian Security Intelligence Service, 2002b). As Canadian and United States authorities have said, the threat of another terrorist attack has not diminished (Canadian Security Intelligence Service, 2002b; Petersen, 2001). All organizations should scan their environment to be aware of the next threat and be prepared to react quickly.

## Notes

1. The author is grateful for the useful comments and suggestions received from Craig Fleisher (editor), Jerry Miller, Janet Shorten and two anonymous reviewers. Martin Rudner, as president of the Canadian Association for Security and Intelligence Studies (CASIS), was the initiator of this paper for the 2002 CASIS annual conference held in Ottawa, Ontario, Canada.

## References

Adams, S. (2002). "A Beginner's Guide to Learning Emergency Management," *Risk Management* 49(5): 24-28.

Aguilar, F.J. (1967). *Scanning the Business Environment*, New York: Macmillan.

Alexander, D.C., Alexander, Y. (2002). *Terrorism and Business: The Impact of September 11, 2001*, Ardsley, NY: Transnational Publishers Inc.

Barrett, P. (2001). "Reducing Vulnerability through Counterintelligence," pp. 29-39 in C.S. Fleisher and D.L. Blenkhorn (eds.) *Managing Frontiers in Competitive Intelligence*, Westport, CT: Quorum Books.

Bhonslay, M. (2002). "Back to Business," *Sporting Goods Business* 35(5): 16.

Blakeley, S. (2002). "Aftermath of September 11th: Business Fraud ad Bust-Outs on the Rise - Steps to Protect Your Credit Sales," *Business Credit* 104(2): 66-67.

Bourassa, M. (2002). ´Les quotidiens n'ont pas profité longtemps du 11 septembre," *Les Affaires*, 29 juin, 13.

Bourgeois, L.J. (1980). "Strategy and Environment: A Conceptual Integration," *Academy of Management Review* 5(1): 25-39.

Bronskill, J. (2002). "Hiring Spree Creates "Gaps" in Intelligence," *The Ottawa Citizen*, June 4: A3.

Brouard, F. (2000). "Que la veille stratégique se lève: faisons le point sur la terminologie et le concept," *Proceedings of the Joint Conference Administrative Sciences Association of Canada - International Federation of Scholarly Associations of Management (ASAC-IFSAM)* 21(6): 22-33.

Brouard, F. (2002). "Pertinence d'un outil diagnostique des pratiques de veille stratégique pour aider les PME", *Proceedings of 6e Congrès International Francophone de la PME (CIFPME)*, Montréal: October-November.

Canadian Institute of Chartered Accountants (CICA). (2001). *Crisis Management for Directors*. Toronto, ON: Canadian Institute of Chartered Accountants.

Canadian Security Intelligence Service (CSIS). (1999). *Counter-Terrorism*. Ottawa: Canadian Security Intelligence Service (CSIS), Backgrounder Series no. 8.

Canadian Security Intelligence Service (CSIS). (2002a). *Security of Information Act*, Ottawa: Canadian Security Intelligence Service (CSIS) Backgrounder Series no. 12.

Canadian Security Intelligence Service (CSIS). (2002b). *2001 Public Report*, Ottawa: Canadian Security Intelligence Service (CSIS).

Carter, A., Deutch, J., and P. Zelikow. (1998). "Catastrophic Terrorism Tackling the New Danger," *Foreign Affairs*, 77(6), p.80-94.

Daft, R.L. and K.E. Weick. (1984). "Toward a Model of Organizations as Interpretation Systems," *Academy of Management Review* 9(2): 284-295.

Daft, R.L., Sormunen, J. and D. Parks, D. (1988). "Chief Executive Scanning, Environmental Characteristics, and Company Performance: An Empirical Study," *Strategic Management Journal* 9(2): 123-139.

Davenport, T.H. and L. Prusak. (1997). *Information Ecology - Mastering the Information and Knowledge Environment*, New York, NY: Oxford University Press

Desmond, P. (2001). *IT Management - Finding Your Role After September 11*. < http://itmanagement.earthweb.com/secu/print.php/890371 >.

Elenkov, D.S. (1997). "Strategic Uncertainty and Environmental Scanning: The Case for Institutional Influences on Scanning Behavior," *Strategic Management Journal* 18(4): 287-302.

Fleming, R.S. (1998). "Assessing Organizational Vulnerability to Acts of Terrorism," *S.A.M. Advanced Management Journal* 63(4): 27-32.

Francq, A. (2001). "The Use of Counterintelligence, Security, and Countermeasures", pp. 40-50 in C.S. Fleisher and D.L. Blenkhorn (eds.) *Managing Frontiers in Competitive Intelligence*, Westport, CT: Quorum Books.

Fuld, L.M. (1989c). "Competitor Intelligence: Can You Plug the Leaks?" *Security Management* 33(8): 85-87.

Garg, V.K., Walters, B.A and R.L. Priem. (2003). "Chief Executive Scanning Emphases, Environmental Dynamism, and Manufacturing Firm Performance," *Strategic Management Journal* 24(8): 725-744.

Gips, M.A. (2002). "CEOs Are Mixed on Terrorism Concerns," *Security Management* 46(4):16.

Ghoshal, S. and D.E. Westney. (1991). "Organizing Competitor Analysis Systems," *Strategic Management Journal* 12(1): 17-31.

Gray, K. (2002). "Ottawa Could Learn from Sept. 11," *The Ottawa Citizen*, July 25: D7.

Grimaldi, R.J. (2002). "Why Do Business Continuity Plans Fail?" *Risk Management* 49(5): 34-39.

Hambrick, D.C. (1981). "Strategic Awareness within Top Management Teams," *Strategic Management Journal* 2(3): 263-279.

Hambrick, D.C. (1982). "Environmental Scanning and Organizational Strategy," *Strategic Management Journal* 3(2): 159-174.

Helms, M.M., Ettkin, L.P. and D.J. Morris. (2000). "Shielding Your Company against Information Compromise," *Information Management & Computer Security* 8(3): 117-130.

Hodgson, K. (2002). "Accessing the Future: Lessons Learned," *Security Distributing + Marketing* 32(2): 50-54.

Howard, L.S. (2002). "Contingency Plan Crucial After 9/11," *National Underwriter* 106(15): 12-14.

Hughes, P.M. (2001). *The Dilemmas of Terrorism*. Bethesda, MD: *World Future Society*. <http://www.wfs.org/hughes.htm>.

Kahaner, L. (1996). *Competitive Intelligence: How to Gather, Analyze, and Use Information to Move Your Business to the Top*, New York, NY: Simon & Schuster.

Lachnit, C. (2002). "Protecting People and Profits with Background Checks," *Workforce* 81(2): 50-54.

Lanter Brown, J. (2002). "What to Do Before Emergencies Happen?" *Occupational Health & Safety* 71(2): 42-46.

Levitin, H. (1998). "Preparing for Terrorism: What Every Manager Needs to Know," *Public Management* 80(12): 4-9.

Liu, S. (1998). "Strategic Scanning and Interpretation Revisiting: Foundations for a Software Agent Support System - Part 1: Understanding the Concept and Context of Strategic Scanning," *Industrial Management & Data Systems* 98(7): 295-312.

Marketing Magic. (2002). "Festival Marketers Revised Plans after September 11," *The Record*. March 20. <http://www.marketingmagic.ca/articles/Stratford.htm>.

Martinet, B. and J.M. Ribault. (1989). *La veille technologique, concurrentielle et commerciale. Sources, méthodologie, organisation*. Paris, France: Les Editions d'Organisation.

McGoey, C.E. (2001). *Racial Profiling Terrorist Among US*. <http://www.crimedoctor.com/racial_profiling_2.htm>.

McGoey, C.E. (2002). *Terrorism Security at All Cost?* <http://www.crimedoctor.com/terrorism_1.htm>.

Miller, J. (Ed.) (2000). *Millennium Intelligence - Understanding and Conducting Competitive Intelligence in the Digital Age*, Medford, NJ: CyberAge Books.

Miller, J.P. (2002a). "The Status of CI after 9/11", Unpublished 23 PowerPoint transparencies.

Miller, J.P. (2002b). "The Status of CI after 9/11," Society of Competitive Intelligence Professionals *SCIP.Online*, 1(11).

Mitroff, I.I. (1988). "Crisis Management: Cutting through the Confusion," *Sloan Management Review* 29(2): 15-20.

Mitroff, I.I., Pauchant, T.C. and P. Shrivastava. (1989a). "Crisis, Disaster, Catastrophe: Are You Ready?" *Security Management*, 33(2): 101-108.

Mitroff, I.I., Pauchant, T.C. and P. Shrivastava. (1989b). "Can Your Company Handle a Crisis?" *Business & Health* 7(5): 41-44.

Moser, F. and M. Borry. (2001). *Intelligence stratégique et espionage économique - cútès pile et face de l'information*. Bruxelles, Belgium: Editions Luc Pire / L'Harmattan.

Newton, C. (2002). "FBI cuts effort in war on drugs," *The Ottawa Citizen*, July 21†: A8.

Nolan, J.A. and J.F. Quinn. (2000). "Intelligence and Security," pp. 203-224 in J. Miller (ed.) *Millenium Intelligence*, Medford, NJ: CyberAge Books.

Pattakos, A.N. (1997). "Keeping Company Secrets Secret," *Competitive Intelligence Review* 8(3): 71-78.

Pearson, C. (2002). "A Blueprint for Crisis Management," *Ivey Business Journal* 66(3): 69-73.

Pearson, C.M. and J.A. Clair. (1998). "Reframing Crisis Management," *Academy of Management Review* 23(1): 59-76.

Pearson, C.M. and I.I. Mitroff. (1993). "From Crisis Prone to Crisis Prepared: A Framework for Crisis Management," *Academy of Management Executive* 7(1): 48-59.

Peteraf, M.A. (1993). "The Cornerstones of Competitive Advantage: A Resource-Based View," *Strategic Management Journal* 14(3): 179-191.

Petersen, J.L. (2001). *The Future of Terrorism.* Bethesda, MD: World Future Society. <http://www.wfs.org/petersen.htm>.

Peyrot, M., Childs, N., Van Doren, D. and K. Allen. (2002). "An Empirically Based Model of Competitor Intelligence Use," *Journal of Business Research* 55(9): 747-758.

Pooley, J. and R.M. Halligan. (2000). "Intelligence and the Law," pp. 171-187 in J. Miller (ed.) *Millennium Intelligence*, Medford, NJ: CyberAge Books.

Quinn, J.F. (1996). "Terrorism Comes to Tokyo: The Aum Shinri Ky Incident", *OPSEC Journal*, 3. <http://www.opsec.org/OPSJournal/Journal96/JohnQuinn.html>.

Raymond, L., Julien, P.A. and C. Ramangalahy. (2001). "Technological Scanning by Small Canadian Manufacturers," *Journal of Small Business Management* 39(2): 123-138.

Sawka, K.A., Francis, D.B. and J.P. Herring. (1996). "Evaluating Business Intelligence Systems: How Does Your Company Rate?" *Competitive Intelligence Review* 7(supp. 1)†: S65-S68.

Schuh, J.S. (2002). "Terrorist Attacks Trigger Legal Review of Meeting Contracts," *Association Management* 54(5): 22.

Simon, L. and T.C. Pauchant. (2000). "Developing the Three Levels of Learning in Crisis Management: A Case Study of the Hagerville Tire Fire," *Review of Business* 21(3/4): 6-11.

Shaker, S.M. and M.P. Gembicki. (1999). *The WarRoom Guide to Competitive Intelligence*. New York, NY: McGraw-Hill.

Strand, R. (1983). "A Systems Paradigm of Organizational Adaptations to the Social Environment," *Academy of Management Review* 8(1): 90-96.

Taylor, M.S. and C.A. Enz. (2002). "Voices from the Field: GMs' Responses to the Events of September 11, 2001," *Cornell Hotel and Restaurant Administration Quarterly* 43(1): 7-20.

Technews. (2002). "Security, After Sept. 11", *TechNews*, 8(2). <http://www.naa.org/technews/TNArtPage.cfm?AID=3954>.

Thomas, J.B., Clark, S.M. and D.A. Gioia. (1993). "Strategic Sensemaking and Organizational Performance: Linkages among Scanning, Interpretation, Action, and Outcomes," *Academy of Management Journal* 36(2): 239-270.

Thompson, J. (2002). "Ignoring Terrorism Doesn't Make It Go Away", *The Ottawa Citizen*, July 9: A13.

U.S. Office of Homeland Security. (2002). *National Strategy for Homeland Security*. Washington, DC: Office of the President of the United States - Office of Homeland Security, July.