CI 2.0:

Expanding the Role of Intelligence in Threat Awareness

By T.W. Powell, The Knowledge Agency and George Karshner, ARISING Group

The most important benefit produced by you, the competitive intelligence practitioner, is one you may not even be aware of.

Let's look for a moment at the big picture. The overall health of a nation depends largely on its competitive position in the world marketplace. Without the ability to effectively conduct commerce and create wealth, a nation stagnates and eventually declines. (Paul Kennedy's book, *The Rise and Fall of Great Powers*, explores this theme in detail. See also Michael Porter's *The Competitive Advantage of Nations*.) Strong national economies are, in turn, produced by having competitively strong enterprises within them. Competitive enterprises are nourished by intelligence, among other factors, that keep them responding to new market conditions and industry developments.

So when you employ your competitive intelligence skills for your company, you are also contributing to global economic stability, without which sustainable corporate growth would be impossible.

Not only does economic strength directly affect a nation's position on the world stage; it also contributes greatly to domestic tranquility. The United States has maintained a stable middle position on the freedom-security continuum for so long that we almost take our stability for granted. However, an economic disaster (for example, a sharp oil price shock, followed by a prolonged recession) could quickly produce a shift toward instability or even anarchy. Such pressures could in turn trigger the imposition of extreme security measures, such as martial law.

Figure 1 illustrates the ideal balance between freedom and security, as well as the extreme situation when stability is compromised. Economic strength is essential for maintaining this balance.

A vivid example of political consequences brought on by sustained economic weakness is the dissolution of the former Soviet Union into several smaller states during the 1980s. The Soviet economy, laden with bureaucracy and poor in productivity and innovation, was neither able to sustain the needs of its population nor to compete in world markets.

In the United States, more than 80 percent of the country's infrastructure is in the hands of private enterprise.

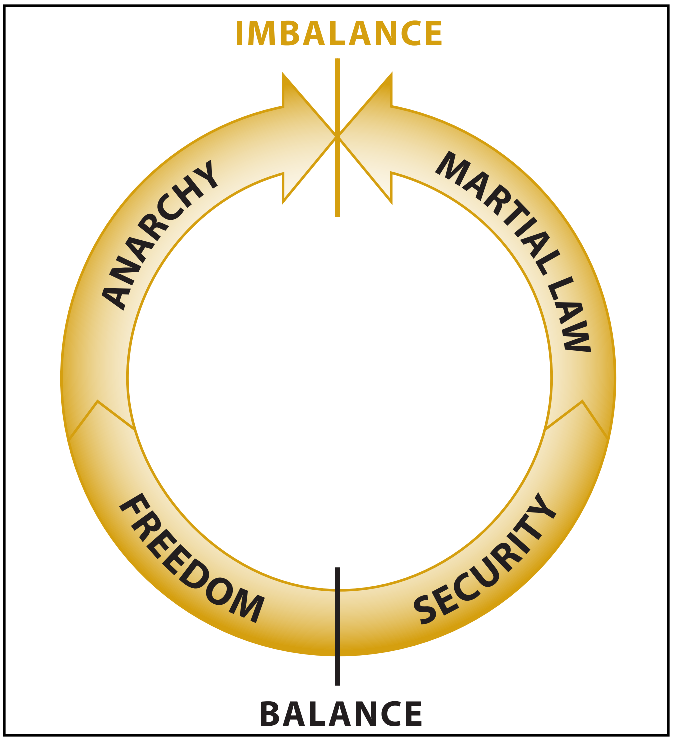

Figure 1: Balance and Imbalance

SIDEBAR 1: SPECTRUM OF ENTERPRISE THREATS

- Market preemption by a rival firm
- Industrial espionage
- IT hacking
- Theft and fraud
- Intellectual property attacks, such as counterfeits
- Physical infrastructure attacks
- Personnel attacks
- Reputation attacks
- Environmental disasters
- Financial trading losses

Assaults against that infrastructure degrade the nation's ability to create the wealth that ultimately funds government programs, including those more directly related to national security.

THE THREAT PORTFOLIO

Competitive intelligence practitioners always benefit from periodically standing back and taking the same look at the world and business environments as the people who run the enterprise (senior management, the board of directors, and even the owners or shareholders). We are struck by the extent to which "competitive" forces—those that assail or erode the economic value of an enterprise—go far beyond rival firms, what we traditionally think of as "competitors."

From the vantage point of the senior executive level, the world can look much different than it looks to a competitive intelligence analyst diligently churning out analyses on rival firms. From this perspective, a spectrum of threats to the enterprise affects its physical, financial, or intellectual property assets (see Sidebar 1 for examples). Each of these threats may be carried out by:

- an *external agent* (a rival firm, a hostile government, or even a terrorist group)
- an *internal agent* (an employee)
- a *combination* of both (which is typically the case with industrial espionage)

Some of these threats are illustrated in Figure 2.

Each threat carries with it an economic "expected value" cost, based on both the likelihood that it will occur (probability) and the economic and human cost incurred if it does occur (impact.) In mathematical terms,

EV = P x I

where EV = economic expected value of an individual threat

P= probability of an occurrence of that threat

I = impact of that threat (measured in financial terms)

Each one of these potential threats has a measurable economic value. This measurement allows the senior decision-makers to:

- prioritize which threats to address first
- set the appropriate level of effort to mitigate or defend against each threat
- make compensatory trade-offs rapidly if and when conditions change

Figure 3 illustrates the dynamics of probability and impact.

A high-impact event like the attacks on New York's World Trade Center has a catastrophic human and economic cost, but a relatively low probability. In contrast, computer viruses strike companies every day, but most of them do relatively little damage. Low-probability/low-impact events are by definition not worth being concerned about; high-probability/high-impact events will probably cause us to rethink our business model entirely.

THREAT AGENTS	THREAT METHODS						
	MARKET PRE-EMPTION	ECONOMIC ESPIONAGE	IT HACKING	THEFT AND FRAUD	BRAND PIRACY	INFRA-STRUCTURE ATTACKS	PERSONNEL ATTACKS
EXTERNAL							
Rival Firms	●	●	●				
Foreign Governments		●					
Criminals/ Terrorists			●	●	●	●	●
INTERNAL							
Employees		●	●	●	●		●
Management		●		●			

Figure 2: Matrix illustrating some of the threats that face business

Individual threats can be summed to value the entire "portfolio" of threats to the enterprise. The total expected value of all threats combined would be

$$EV_{total} = EV_1 + EV_2 + EV_3 \ldots + EV_n$$

The entire value of the "prevention plus insurance" program should be set with reference to this total expected value of the threat portfolio.

Working with a threat portfolio is very much like owning a portfolio of financial investments. You want to have some that are low risk and low return (like government bonds), and you may want to have some with higher risk and higher return (like growth stocks). When conditions change (for example, you finish paying off those student loans or you retire), you'll typically want to modify the portfolio mix to reflect your new "risk tolerance."

Corporations carry a portfolio of threats much like investments, except that threats usually cost you money rather than earning money for you. The problem arises when these threats are managed in a "silo-ized," nonintegrated way: finance manages the risk from financial losses; corporate security manages the risk of industrial espionage; information technology manages the risk of computer incursions; competitive intelligence manages strategic threats like market incursions; and so on.

Sometimes a team representing several disciplines manages emerging threats (for example, counterfeit products). This works when it is intended as a team effort. But often this effort results in more turf wars and budget battles than in productive activity.

So far we're consistent with the management guideline, "To manage it, measure it." But how do you measure something that has not yet occurred? The insurance business has a whole science called *casualty actuarial* that essentially does exactly this to determine how much to charge for insuring a particular risk.

Casualty actuarial assumptions are based on projections of the probability and impact of a given threat event. Such projections are heavily based on past experience with similar events. The insurance model provides economic compensation after an event has occurred. In contrast, intelligence focuses on trying to prevent events that will negatively affect the organization, and minimize their impact when they do. Neither model is better than the other—in fact, we believe they should work together much more often than they do.

CI 2.0: AN EXPANDED ROLE FOR INTELLIGENCE

The general level of these business threats is much higher than it was before 9/11. And all these threats point to a common response—the need for intelligence to serve as an early warning system. Yet traditional competitive intelligence departments (we'll call them "CI 1.0" practitioners) remain for the most part unchanged in their tasking and approach. With a few exceptions, competitive intelligence is not involved in threat assessment and early warning, beyond that posed by rival firms (Herring 2006).

Competitive intelligence practitioners should not ignore potential threats posed by rival firms. But they should re-scope and refocus their efforts to include a more comprehensive range of threats to the enterprise, however senior managers define these threats.

Competitive intelligence practitioners are uniquely suited for front-line threat assessment and monitoring. Through study, training, and experience, they develop the skills to obtain valuable information on their organizational rivals, as well as other threats from the business environment. They know where the potential sources of this information are and where their own companies may be vulnerable to such threats.

The narrowness of the "CI 1.0" focus is usually not the fault of competitive intelligence practitioners, since their tasking comes from CI managers and ultimately, from senior management. For various reasons, the prevailing corporate response to increased threat levels has not included engaging corporate intelligence in the security effort. These companies do themselves—and their stakeholders—a great disservice. A skilled competitive intelligence practitioner will have mastered a

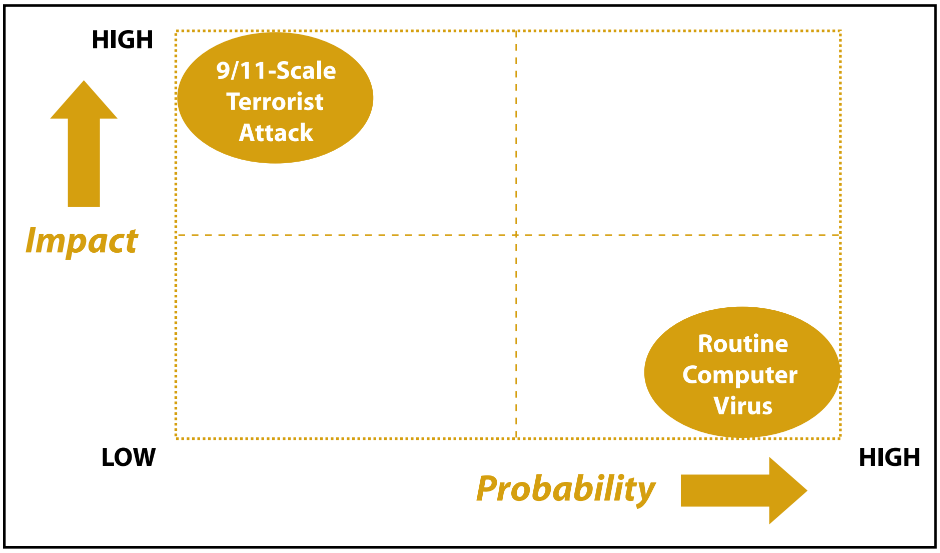

Figure 3: Probability and Impact

SIDEBAR 2: MONITORING SOURCES

- Google Alerts, www.google.com/alerts
- Technorati, www.technorati.com
- Newsgator, www.newsgator.com/ngs/default.aspx • Bloglines, www.bloglines.com/search
- Overseas Security Advisory Council (OSAC), www.osac.gov
- The Multi-State Information Sharing and Analysis Center (MS-ISAC), www.cscic.state.ny.us/msisac
- Homeland Security's Computer Emergency Readiness Team (US CERT), www.us-cert.gov

range of skills, techniques, and sources that could add value in many, if not all, threat areas.

Instead, companies have typically hired senior security executives, many of whom have government service (especially FBI or Secret Service) in their background. This naturally brings a law enforcement mindset to the process, which tends to be more reactive than preemptive by nature.

We know of only a few companies that asked their competitive intelligence professionals to lead an assessment of the full-threat spectrum. These practitioners provided a comprehensive picture that enabled the C-suite to make decisions and take actions to mitigate upcoming threats (Herring 2006). We call this expanded outlook "CI 2.0." Competitive intelligence departments and practitioners who embrace the challenge of this extended responsibility will provide far greater value to their corporate clients, will enhance their own careers in the process, and will earn the right to feel much better about the work they do.

USING CI TOOLS AND TECHNIQUES TO BUILD THREAT AWARENESS

Most competitive intelligence practitioners already have most of the skills, tools, and techniques in secondary and primary research that they need to advance into CI 2.0 mode. They will need to familiarize themselves with the specific threats that concern their management through the use of key intelligence topics as well as the threats that management may not yet be aware of. This requires a commitment to monitoring the news and trends in chatter (for example, op-eds, speeches, blogs). Many secondary research tools can simplify this work.

To be effective at CI 2.0, we follow threat developments and track trends, paying special attention to the capabilities, intentions, and actions of potential threat sources. Developed through analysis, these three factors will indicate the threat proximity and probability of occurrence.

Secondary Data Collection

Several secondary tools can help monitor news developments and chatter trends (see Sidebar 2). These include specific topic alerts from Google and RSS feeds from reliable news providers. Google Alerts is a program that crawls the Web looking for new items relating to your chosen topic and notifies you of them by e-mail. You choose the frequency of the search and notifications.

In every field, pundits are tracking their industry-specific concerns and posting comments on their Web pages. Weblogs or "blogs" abound on the Internet, and new content appears frequently. Technorati, Newsgator, and Bloglines are among the tools for tracking new information.

Government alerts are essential sources, especially those from the U.S. State Department's Overseas Security Advisory Council (OSAC), the Multi-State Information Sharing and Analysis Center (MS-ISAC), and Homeland Security's Computer Emergency Readiness Team (US CERT).

When choosing topics to track, consider the full length of your supply chain, including nontraditional places where you may be vulnerable. For example, the State Department reported that a route used to smuggle copra out of Southeast Asia in the 1950s was reused in 2002 to smuggle rainforest timber. This information was picked up by monitoring security reports for a geographical region several times removed from the company's immediate raw materials vendors. It proved useful in explaining a sudden drop in the price of a competitor's imported furniture.

Primary Data Collection

The people who can provide primary information on threats are in our same line of work: people up and down the chain of command. Peer networks like the ones we develop at SCIP are a great way to stay on top of risk developments.

Experts on threats—security people, government, and military people—are some of the best sources, although business people rarely have the opportunity to interact with them. Try attending topical speaker meetings hosted by the U.S. Department of Commerce, international chambers of commerce, Business Executives for National Security, Rotary, and other similar groups. (You can usually find these listed in business directories such as those published by Crain Communications.) Speaker luncheons are a great way to learn from subject experts and to expand your personal network.

If you work in an area that doesn't have groups like these, you can band together with local SCIP members and start your own. Call on local FBI, Homeland Security, and law enforcement officials for speakers on topics such as economic espionage, cybersecurity, fraud, and identity theft.

Your company's own employees can be a powerful data collection network if you train and manage them well. Commercial providers also offer primary data collection services.

OPPORTUNITIES AND OBSTACLES

As you work to bring your intelligence expertise to bear on the range of threats facing your company, you may encounter organizational obstacles. The following list describes some of these obstacles and our suggestions on how you might handle them.

My management doesn't really care about this "threat" stuff. True, senior management often seems more comfortable with generating sales, maximizing profit, and ensuring return on investment, while delegating loss prevention and physical security to the security people. However, in many companies—especially those that have been burned once—security is becoming a C-suite and even board-level concern.

Isn't security the security department's job? Yes, but the security department usually focuses more on physical security ("gates, guards, and guns") than on intellectual property security. The modern enterprise also has other threats, and here corporate intelligence can make security even more effective. Some companies even describe intelligence as the foundation of a comprehensive security program. And usually security isn't the only member of the team. Legal, information technology, and other functions may be involved—and may need the intelligence CI practitioners can provide.

Isn't national security the government's job? Partly, but as we pointed out earlier, it's really everyone's job, and the private sector actually has significant assets at risk. Most government intelligence officers are trained differently than corporate intelligence practitioners, and are at best resource-stretched and focused on areas more directly related to national security. This leaves business and industry in a highly vulnerable position.

SIDEBAR 3: BUSINESS-GOVERNMENT INTERACTION AND COOPERATION

- There is growing public awareness of intelligence, which is increasingly finding its way into the business community in many countries.
- In the United States, intelligence flow between business and government is still largely one way, from business to the government but not back. (For more of this and related issues, see Flynn 2006.)
- Security departments remain the main point of government contact within corporations.
- A few—but only a few—competitive intelligence departments have been involved in company-wide threat assessment initiatives.
- Competitive intelligence activities seem to be for the most part relatively unchanged, with perhaps new skepticism about their value due to the controversial recent performance of U.S. government intelligence in the pre-9/11 and pre-Iraq war periods.
- In summary, the much closer relationship between corporate intelligence and security that some expected in the aftermath of 9/11 has largely not materialized (Herring 2006).

I don't even know my corporate security people. They'd likely say the same of you. Pick up the phone, or stop by and see them. Have a brown-bag lunch discussion. What are they interested in? How are they rewarded for a job well done? How can you make them look better?

Don't we have insurance for threats? Sure, but the goal of intelligence is preventing problems, not mopping up after they occur.

Can't I just keep doing what I do best? Sure, unless you care about having a job in a few years. The nature of competition has changed, and you must adapt or risk becoming irrelevant.

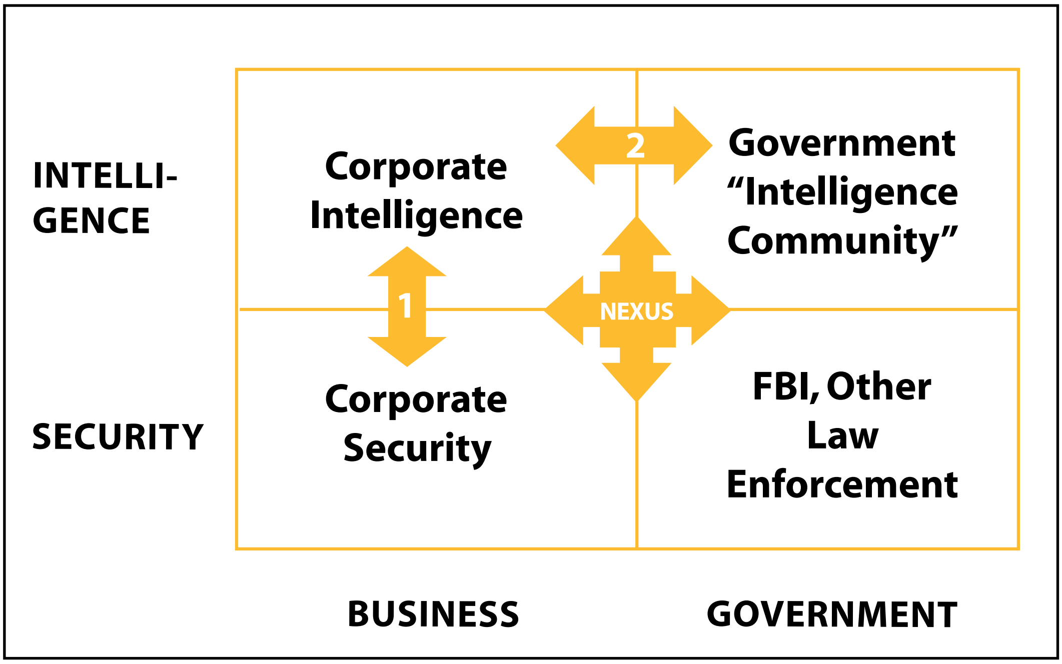

Figure 4: The Silos

Important things seem to be happening, but why has competitive intelligence not been "invited to the party"? As you build and develop relationships with internal and external sources, you need to have something to give back. "Casting bricks to attract jade" works for only so long. At some point sources may feel used; but not so if you can provide current and advance knowledge of threats. Providing interesting and pertinent knowledge as well as some actionable gems from time to time will earn you a place in the crowded memory banks of the right people.

BRIDGING THE SILOS

Jan Herring is one of those rare individuals who have achieved positions of senior leadership in both the public and private sectors of intelligence. Jan addressed the Business Threat Awareness Council (BTAC) in May 2006 about informal research he had conducted on "Business-Government Interaction and Cooperation in the Post-9/11 World." His principal findings are summarized in Sidebar 3.

Whether you see this situation as a problem or an opportunity depends on your appetite for innovation and challenge. We see these as a two-dimensional set of silos, as depicted in figure 4. If silos are the enemies of process, then our objective must be to bridge the gaps between them. Communication is largely nonexistent, as at arrow 1 in the diagram, or it is largely one way, as at arrow 2. As a result, in both cases the flow of intelligence is flawed, and this inhibits the types of concerted efforts that could otherwise result.

You can begin to bridge the silos in your company by

- identifying users most likely to benefit
- building relationships with them to better determine their motivations, needs, and concerns
- creating deliverables that respond to those needs and concerns
- finding a champion (or two) who likes what you're doing

Reading CSO magazine and attending selected security-related conferences, such as those produced by ASIS, can also help you bridge the culture gap. [Note: Web sites are listed below in references.]

The model presented here is a United States-based model, and we encourage those in other nations to develop their own similar models. For example, the separation of business and government intelligence that is traditional in the United States is less of a factor in many other countries, particularly those in Western Europe and in the Far East.

The formation of the Business Threat Awareness Council (BTAC) flowed directly from our frustration with these persistent gaps. We see BTAC as a nexus that begins to bridge these gaps and subsequently develops deeper and more permanent connections.

THE BTAC MODEL

BTAC is a not-for-profit, nonpartisan group based in New York City. Its core premise is that a secure nation rests on a strong economy. Its central mission is to improve threat awareness and promote best practices in threat management.

BTAC's initial meeting in November 2004 was held under the auspices of the Office of the National Counterintelligence Executive, part of the U.S. Directorate of Central Intelligence. BTAC's members are typically security and intelligence practitioners in both private and public sectors, representing a range of industries. (Individual membership in BTAC is currently free.)

BTAC's activities form a template that can easily be adapted by intelligence practitioners within corporations. The BTAC model consists of the following:

- **News link distributions** to open-source developments of interest. Captured by BTAC's correspondent network, then compiled and categorized by BTAC staff, this activity uses many of the sources and techniques described above. BTAC members receive these links in e-mails distributed once or twice weekly, and may redistribute them to internal clients without charge.
- **Monthly meetings**. These are held in New York about every four to six weeks. Subject-matter experts share their current work and insights and lead group discussions on current issues. Sound recordings of some of the meetings are available on the BTAC Web site. The meetings also provide opportunities to network with like-minded people.
- **Informal intelligence sharing**. Information is exchanged about current developments of interest to participants. This happens both in the meetings and by e-mail between meetings.

In creating BTAC, we've had to overcome many of the objections listed in this article. We'll be happy to share our experiences with you.

REFERENCES

ASIS (www.asisonline.org)

Business Threat Awareness Council (BTAC). (www.btac.us) Individual membership in BTAC is free.

CSO magazine (www.csoonline.com)

Flynn, Stephen E. and Prieto, Daniel B. (March 2006). "Neglected defense: mobilizing the private sector to support homeland security," Council on Foreign Relations, CSR No. 13, p 15. Available online at www.cfr.org/publication/10457/

Herring, Jan P. (May 25, 2006). "Business-government interaction and cooperation in the post 9/11 world," presentation to the Business Threat Awareness Council. Available in streaming audio at www.btac.us.

Kennedy, Paul (1987). *The Rise and Fall of Great Powers*. New York, Random House.

Porter, Michael (1998). *The Competitive Advantage of Nations*. New York, Free Press.

T.W. (Tim) Powell (tim.powell@knowledgeagency.com) is president and founder of The Knowledge Agency®, a business research firm. He is a long-time SCIP member, and is active in SCIP affairs. His interest in this topic was heightened after witnessing the attacks on New York's World Trade Center on 9/11/01 from about a mile away.

George Karshner (george@arising.net) is director of business development for the ARISING Group, an information technology company delivering business technology solutions to financial, health care, governmental, and nongovernmental organizations. Before joining ARISING, George conducted similar work for ATS Global and DuPont. George hails from a family of law enforcement and intelligence professionals and has been an active member of SCIP since 2000.

The authors are cofounders and officers of the Business Threat Awareness Council. George serves as its president and Tim is corporate secretary. The authors wish to thank Jan Herring for reviewing this manuscript, and Joan Wong of ARISING Creative (www.arisingcreative.com) for the graphics.