Notes from Third Meeting of the Business Threat Awareness Council (BTAC)

May 24, 2005
Offices of MeadWestvaco
New York City

Attending:

George Karshner
Arising Group

Brad Leach
NY Mercantile Exchange

Lee Mason
WABC Radio Network

Bill Manning
Prudential Global Security

Bob Levey
The Long Shore Group

Carol Rubenstein
USPS

Frances Rosato, Esq.
Security consultant

Bill Fitzgerald
Donovan Fitzgerald

John Kessling
Consultant

Tim Powell
The Knowledge Agency

Rob Garber
The Knowledge Agency

Shawn Lewis
ESL International

Steve Walsky
ONCIX

Howard Greco
Anonymizer

Debbie Henry
Anonymizer

George Oxley
MeadWestvaco

Jonathan Blumberg
MeadWestvaco

Administrative Matters

George Karshner chaired the meeting. He opened by reading the BTAC mission statement. He reviewed the current state of the web site, which has been mounted in shell form at www.btac.us. He mentioned that planned future developments include an electronic "gated community" for the sharing of information.

A letter from National Counterintelligence Executive Michelle Van Cleave commending BTAC on its efforts was reviewed. A copy is available on the BTAC web site.

Notes from the previous BTAC meeting were reviewed by Tim Powell.

Speaker – Steve Walsky - Program Manager, NCIX

We were honored to have a distinguished speaker, Mr. Steve Walsky, ONCIX. Steve spearheaded the NCIX's outreach program, and was the ONCIX Program Manager for the New York City meeting in November 2004. Mr. Walsky's continued support has nurtured the formation of BTAC as a standing group.

Mr. Walsky's wide-ranging comments gave us an insider's view of the foundation of the NCIX outreach effort. According to him, "Business is the heartbeat of America, and our goal is to create a better dialogue with the private sector. The NCIX effort represents a first step in meeting this goal. While there are other groups that focus on security and government, BTAC is different in that we want to bring *other* strategic executives into the discussion."

Mr. Walsky outlined the history of NCIX. He explained that the NCIX focus is counter-intelligence (CI), which is governed by the National Counter-Intelligence Strategy for the United States. Each initiative of NCIX must fit within the CI strategy, which in turn must fit within the nation's overall intelligence strategy.

The primary focus of U.S. CI efforts in the 1990s and prior was the protection government classified information. The focus later expanded to include commercial technologies, but these were typically directly defense-related.

Defense-related technologies are still at the top of the list of sensitive U.S. technologies that need to be protected. But this list now includes emerging commercial technologies, for example nanotechnology. "America's future is in technologies—we need to be sure the information about them is secure. This means assuring that U.S. companies are not jeopardized by foreign intelligence operations."

There is a traditional separation between business and government intelligence in America that exists in few, if any, countries outside the U.S. This sometimes puts U.S. companies at a disadvantage when bidding against non-U.S. competitors, as they do in industries such as commercial aircraft. NCIX publishes the President's *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage* that summarizes activities by foreign governments and non-U.S. based companies to target U.S. strategic commercial interests. The unclassified version of this report is available at www.ncix.gov.

One of the key needs of NCIX is to find out what business decision-makers are thinking and doing with regards to foreign economic espionage. To this end, NCIX contemplates conducting focus groups with business leaders.

Mr. Walsky mentioned other related organizations, including the National Classification Membership Society (NCMS) (www.classmgmt.com), ASIS International (www.asisonline.org), and the Overseas Security Advisory Council (OSAC) (www.ds-osac.org).

Mr. Walsky related several recent stories related to industrial espionage, some from open sources, and some non-classified stories from his own casebook. He warned that "cyber-terrorism" has evolved from just defacing or shutting down web sites, and that some countries (North Korea, for example) employ small armies of hackers to try and steal sensitive technology information.

Sometimes a seemingly innocuous technology is sought because it has structural similarities to a sensitive technology. For example, in one case a foreign government attempted to gain access to the non-exportable source code from a U.S. company for a subway simulation system—because the underlying code was similar to that for an anti-missile system.

The U.S. Department of Defense (DoD) has created a Foreign Supplier Assessment Center to vet offshore suppliers to DoD. Mr. Walsky suggested that U.S. companies must consider putting procedures into place for offshore contracts, for example call center operators; have you considered what sensitive company proprietary, or competitive advantage, information is contained in the materials you provide to the call center?

Mr. Walsky reviewed the recent sales of U.S. technologies to foreign companies, for example Tyco's sale of undersea cables to VSNL of India, and Global Crossing's sale of satellite dishes to ST Telemedia of Singapore. He advocates that the U.S. look at itself as an individual company would, in terms of competitive advantage gained or lost.

Mr. Walsky answered questions from the group.

QUESTION: If the government reviews our emergency plans, how can we be sure these are secure?
ANSWER: When responding to any inquiry, it is best to disclose details only on a "need-to-know" basis. Group discussion indicated the information sought by Government agencies, such as Homeland Defense, concerned evacuation and personnel accountability data, and does not require the release of sensitive information.

QUESTION: How does corporate America benefit from the gathering of all this information on foreign threats to the private sector?
ANSWER: There are several ways. The NCIX annual report to Congress is one. The Defense Security Service monitors threats to defense contractors, and posts information on their web site. The State Department runs OSAC and runs various seminars. The FBI runs InfraGard, and can give targeted briefings on that and related issues.

QUESTION: The 9/11 Commission report recommends much more and better use of "open source" information—what is happening with that?
ANSWER: Full use hasn't happened yet, but is beginning to now, thanks to efforts in Congress.

QUESTION: Are there templates available for disaster contingency planning?
ANSWER: There are templates on the DHS web site. There is a working group within FEMA that is also addressing this.

QUESTION: I recently traveled in South America, and found that the information from our consulates was dated. I did find some good information from a private company called Intellibridge (www.intellibridge.com). Are there other sources?

ANSWER: The private sector tends to have the best information on safety in various regions. You could also check the International Chamber of Commerce and the Chamber for each country of interest. If you have specifics suggestions for improvements to what the State Department does, get in touch with OSAC.

QUESTION: To what extent does U.S. policy allow for both offensive and defensive strategies to be used against potential threats?
ANSWER: We are working on our capability to be "offensive", in the sense of proactive—not waiting for a threat to develop into actual targeting, but doing things in advance to deter it; such as our work with the BTAC. We are also still working on the challenge of better coordination among all the agencies that ideally need to be involved.

QUESTION: Business executives don't really understand security—they do understand money and time. How can we train our companies' senior management to be more proactive?
ANSWER: There already plenty of security-related discussion groups. But in the corporate world, security is seen as overhead, and not strategic. You need to use the language of business, and get managers in areas other than security involved.

QUESTION: Will the organization of the Intelligence Community under the new DNI make it more effective?
ANSWER: Yes. The strength of the DNI position - centralized leadership and coordinated objectives and mission execution - will make the Intelligence Community more effective. The leadership position of the NCIX, and the activities of the Office of the NCIX, will benefit from this.