



# Business Threat Awareness Council

*Awareness to Strengthen America's Commerce*

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

March 2, 2005  
New York City

### ***Attending:***

Jonathan Blumberg  
Mead Westvaco

Ken Damstrom  
Lehman Brothers

George Karshner  
Arising Group

Shawn Lewis  
ESL International

Brad Lynch  
NYMEX

Joe Macchiaroli  
DHS/Customs

Tim Powell  
The Knowledge Agency

George Karshner chaired the meeting. He first presented a brief overview of ONCIX and its charter. The ONCIX outreach program for the private sector was started after 9/11/01. The November 2004 meeting in New York City was a first step, now this group is ready to explore next steps.

### ***Key discussion points from the meeting:***

- How can the public and private sector work together? There is currently a lot of lip service, but not much tangible.
- The focus of the BTAC initiative has been expanded from just counterintelligence, to include this as well as many other threats to business. ONCIX supports this change of scope.



- ❑ The External Fraud Committee could serve as a model. Business representatives meet with public officials to discuss issues related to credit card fraud, identity theft, etc. Focus is on the financial services sector. The group meets once a month, has a speaker and open discussion.
- ❑ There is good public-private sharing of information at the case level (“the trees”). Businesses need a higher level of information (“the forest”), especially from overseas.
- ❑ The financial services sector seems to have the most highly-evolved mechanisms for sharing information, probably since it is heavily-regulated. But now the needs have moved to include a range of sectors.
- ❑ DHS has identified 13 critical industry sectors. BTAC might eventually be structured along the lines of industry interest groups, which in turn roll up to a “master” BTAC.
- ❑ Any sharing of information has to take place in controlled conditions, so that competitive advantage is not compromised, and so that anti-trust laws are not violated.
- ❑ The information shared can be “redacted” so as to exclude specific company identifiers, but to nonetheless provide information useful to other companies looking to prevent or respond to a similar threat.
- ❑ Threat Awareness needs to be “sold” to senior management – but until now, in many cases they do not have it on their radar. The message needs to be crafted in terms of “risks to value”, measured by revenues, profits, and shareholder value.
- ❑ The El Dorado task force represents a good “best practices” model, in that several agencies from the federal government as well as the states of New York and New Jersey cooperate to deal with issues related to money laundering and illicit diversion of funds.
- ❑ The same information that the public sector now uses for prosecutions could be redacted, aggregated, and “re-purposed” to serve the early-warning needs of businesses.



- In many (if not most) other countries, there is routine and wide-accepted sharing of intelligence between public and private sectors. This does not currently happen in the US.
- Where public-private information sharing does occur, it typically happens through informal networks of ex-federal employees now in the private sector. BTAC's mission should include formalizing this process and make it available to people who do not have access to such networks.
- Process-level information can also be shared (for example, lessons learned; vendors who have specific expertise; checklists and templates; etc.) without adverse consequences.
- There needs to be a business case built to present Threat Awareness to senior management. Now, when there are "no incidents", the security budget is often cut, rather than sustained or expanded. A "model" business case detailing the economics of Threat Awareness is something that BTAC can create.
- Even middle-management often does not have a central point of contact for Threat Awareness issues. Sometimes it is Security, sometimes it is Legal – and typically there are several poorly-coordinated points of contact.

*Ideas for what BTAC needs to do:*

- Establish a single point of contact in Central Intelligence.
- Develop an electronic communication system and information repository for members.
- Hold "awareness" meetings every 4-8 weeks, each with a speaker and open discussion.
- Develop relationships with other conferences, for example ASIS.
- Develop an entry point for corporations – Legal? Security?
- Get a letter from the National Counterintelligence Executive, Michelle Van Cleave, endorsing the BTAC initiative.



- A two page white paper, or business case, containing the best current statistics on threats, costs to business, etc., that can be used to “sell” BTAC involvement to C-level management and other potential members and could be used to obtain corporate sponsorships and/or in-kind donations. Possible source: Dr. Dean Carver.
- Develop a BTAC web site - a virtual “community of interest” for Threat Awareness.
- Lobby Washington to look at the “forest” (the whole impact on business), not just the “Trees” (individual case-level information).
- Develop other ways to maximize the interactions between NCIX and the private sector.
- Possibility of getting a rep/contact person from other agencies in addition to Central and ONCIX
- George or Joe planned some follow-up with DHS to inquire about funding

Next Steering Committee Meeting will be held:

Thursday 21 April 2005 at 8:00AM

Location: TBD