VOLUME 2, ISSUE 4
DECEMBER 2010

WHAT'S INSIDE

atap chapter updates
page 2
weathering the social media storm
page 4
can competition cause violence?
page 6
opsec
page 8
is your incident reporting system putting your organization at risk?
page 9

atap newsletter

THE QUARTERLY PRINTED PUBLICATION OF THE
ASSOCIATION OF THREAT ASSESSMENT PROFESSIONALS

PRODUCED BY
KRISTA GIACCIO, WASHINGTON, D.C. CHAPTER PRESIDENT
CATHERINE A. SMITH, EXECUTIVE DIRECTOR
ASHLEY BRADLEY, COMMUNICATIONS SPECIALIST

president's message

Rachel Solov, JD

Happy Holidays from your ATAP Board of Directors

ATAP Board of Directors

Rachel Solov
President

Debbie Hollan
First Vice President

Jeff Dunn
Second Vice President

Paul Bristow
Treasurer

Jeff Gentry
Secretary

Chuck Tobin
Sergeant at Arms

Catherine Smith
Executive Director

Association Headquarters
1215 K Street, Suite 2290
Sacramento, CA 95814
p 916.231.2146, f 916.231.2141
www.atapworldwide.org

atap chapter updates

great plains chapter

On Friday, October 15, the ATAP Great Plains Chapter hosted a full-day workshop at the Cornhusker Marriott in downtown Lincoln, Nebraska. Nearly 100 participants were in attendance representing backgrounds in law enforcement, post-secondary education, mental health, private industry and more. Special Agent Andre Simons from the FBI's Behavioral Analysis Unit (BAU) gave an in-depth presentation regarding campus attacks, examining trends in campus violence and discussing case studies and warning signs. After the morning presentation, an ATAP business meeting was held during lunch, which provided the opportunity for recruiting new members and networking. The afternoon presentation featured Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) Special Agent Ron Tunkel, who works as an ATF representative to the FBI. He spoke about applying threat assessment strategies to case materials, discussing the ATAP model for risk assessment, and analyzing an offender's language in communications from case files. Both presentations were well received and the Great Plains Chapter received positive feedback about the entire event.

ATAP Great Plains Vice President, Dr. Mario Scalora; Special Agent Ron Tunkel; Special Agent Andre Simons; and ATAP-GP President, Chief Owen Yardley

January 21, 2011
CTAP Webinar

February 18, 2011
ATAP-GP Chapter meeting (Lincoln, NE)

calendar of events

2011

February 18 - Great Plains Chapter's "Legal Issues in Threat Assessment"

April 12-15 - AETAP's conference (click here for more information)

April 18 - ATAP Spring Regional Conference

August 16-19 - ATAP Annual Threat Management Conference

tmc sponsorship opportunities

ATAP's annual Threat Management Conference attracts individuals from all over the world who specialize in assessing and managing violent individuals and organizations for the protection of countries, communities, organizations and individuals.

TMC Sponsors receive exposure in the form of: special recognition on every general session video screen, verbal recognition, advertisement in the conference notebook, a FREE conference registration, one year on the ATAP website as a sponsor with a link to your website, a display table in the conference vendor area, and much, much more!

Interested? Download the Sponsor/Donor Packet

north east chapter

The North East Chapter met Monday, September 27 during lunch in donated space at The McGraw-Hill Company Offices. The speaker was Dr. Robert A. Leonard, Professor of Linguistics at Hofstra University and Director of the Forensic Linguistics Project. Dr. Leonard addressed the use of linguistic analysis in threat assessment and demographic profiling. Forty one members and guests attended and were advised that the chapter is in good financial condition, and that we were able to sponsor attendance of two members at the August 2010 Annual Meeting in Anaheim, CA. Chapter President Richard Chapman reported that the national organization has continued the contractual arrangement with the Disneyland Hotel for the next five annual meetings, locking in good rates for rooms and services. The North East Chapter is considering hosting a Spring Regional Conference in 2012, and members are requested to advise Rich if they would like to join an exploratory committee.

The chapter will be electing a new Board of Directors next month. The nominees are:
President: Richard Chapman
Vice President: Anthony Burti
Treasurer: Kevin Green
Secretary: Ronnie Harmon
Sergeant At Arms: Robert Wiest

The next meeting was scheduled for Monday, November 30 and we were once again grateful to Frank DeMartino, Security Manager for the McGraw-Hill Companies, for offering to host our gathering at their office space at 1221 Avenue of the Americas in Manhattan. Lunch was provided by the chapter. Watch your e-mail for an announcement about a holiday cocktail party some time in December.

Save the Date!

ATAP Spring Regional
April 18-19, 2011
Chicago, IL

Visit www.atapworldwide.org for additional information.

weathering the social media storm: how to integrate social media into the threat assessment process

by: Terri Howard, FEI Behavioral Health

A core component of our service as threat assessment professionals is the compassionate, supportive delivery of accurate information to the friends, family and co-workers of crisis victims. It's been an emphasis at FEI for the last 20 years, through some of the largest crises the world has seen. As we help people face these unfortunate events, a constant companion in many crisis management centers has been a television tuned to CNN or another national news program.

We serve as a conduit of information for our clients and, to do that job most effectively, we must track the stories and events as they emerge and morph. This helps us anticipate the information people are likely to have when they call and affects how we best advise clients about the implementation of their crisis plan.

Old World vs. New Frontiers

For years, our main information sources have behaved according to a reliable set of rules. Stories were told in sound bites, reporter stand-ups and anchor chatter. The editorial process behind the business of news-gathering dictated a certain pace and also tended to ensure a certain level of reliability and objective accuracy.

Today, that approach has been largely replaced by one that is 140 characters wide. During recent crisis responses at FEI, we've noticed that social media is by far the most active and volatile method of dispersing information. This sudden and widespread emergence has led to several challenges for threat assessment professionals at all levels. However, with the right attitude and management approach, we believe social media offers new, unique opportunities to provide valuable services to our clients.

Challenges

• Increased Speed and Volume

Twitter, Facebook and blogs have created information flows of much greater velocity and volatility than previously imagined. The first inkling of a crisis event is now far more likely to occur through a Twitter feed or Facebook posting than a story on a cable news network. We need to establish proven, well-organized strategies and tactics that allow us to respond on a dime when needed.

• Pervasive Inaccuracies

There is no editorial process to moderate either the pace or accuracy of the information conveyed by social media. The co-mingling of fact, opinion, speculation and repetition creates a whole new class of information we may be faced with as we assist those closest to the crisis. We must be prepared to respond not only to the real crisis, but also to possible fears generated by rumors or false facts.

continues on next page

interested in contributing to the next issue of the atap newsletter?

If you have an article you've recently written, member news you'd like to share, or know of anything that may be of interest to ATAP members, please contact Krista Giaccio at kgiaccio@supremecourt.gov.

• Demand for Hyper-Transparency

Social media audiences seem to feel a right to know anything and everything about a crisis and the people and companies behind it. Any hesitation to communicate the latest facts risks being seen as a cover-up. It's something threat assessment professionals should be aware of in the new world.

Action Steps

• Create a "Listening Post" for Each Client

At FEI we have established listening posts to monitor this new flow of information during crisis events. Our purpose is not to repeat the information, but to understand how it is shaping the experience of those we are helping.

A "listening post" is simply a term for the electronic platform used to synthesize client news across all types of media—traditional print, blogs, Twitter, etc. It becomes a one-stop shop to learn what people are saying about a client or a crisis situation, in real-time. You can use the following to help feed your listening posts:

- Google Alerts – E-mail reports that track news stories, blogs and more, based on search keywords.
- Twitter Search and TweetBeep – Websites that act like the Google Alerts equivalent for Twitter. They help you monitor discussions occurring in the Twitter realm.
- TweetDeck and Seesmic – Desktop applications that allow you to monitor Facebook, MySpace and LinkedIn, as well as Twitter.
- Social Mention – A search tool that also tracks content from YouTube and Flickr, in addition to Facebook and Twitter.

• Monitor Emerging Threats

Social Media venues often are the first place people now go to share thoughts or vent. Diligent threat assessment professionals should have an awareness of what's being said about their clients or a particular situation even before a crisis hits. Careful monitoring of social media may allow you to identify emerging problems, spot disgruntled employees or address risks prior to escalation.

• Incorporate Social Media in Crisis Planning

While advising clients in proactive crisis planning, find ways to coordinate with marketing or public relations departments on a social media component. Although the roles of threat assessment and communications are very different during an actual crisis event, your efforts should work together to address trouble areas, share accurate information and calm those involved. This team approach is more important than ever, given the nature of social media.

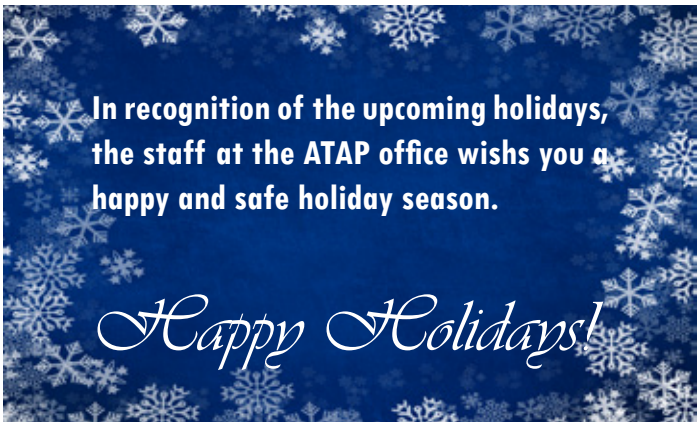
• Provide the Most Appropriate Solutions

Comments made in the social media realm often contain emotion that is absent in objective journalistic stories. This can give threat assessment professionals key insights to help manage the human aspect of a crisis situation. At FEI, for example, we can read in real-time about the specific emotions people are experiencing and then craft the best support solutions to address those particular concerns.

• Evaluate the Impact of Your Response

Establish baselines regarding the number of conversations that typically occur about your client or a situation. Note how many people talk about it, how often and for how long. This will help you quickly gauge the impact of a crisis — through a swift uptick in chatter — as well as the impact of your response. You'll also be able to track how the tone of conversation changes — positively or negatively — throughout a crisis situation, which may influence your response tactics.

In today's world of fast-paced social media, threat assessment professionals must be proactive and flexible in monitoring a wide variety of information sources — for the good of our clients.



can competition cause violence?

by: Dr. Ronald J. Coughlin, Ed.D. President, New Jersey Violence Prevention Institute

The Robbers Cave Experiments

In the caucus race in Alice in Wonderland (Carroll, 1960), "participants began running when they liked and left off when they liked." The DoDo bird who ran the race, further stated "Everybody has won and all must have prizes." This description of the caucus race is not competition as we know it. As several social scientists have observed (May and Doob, 1937), competition is an arrangement where two or more individuals are attempting to achieve a goal that cannot be achieved by all of them. In this type of competition someone's success is dependent on someone's failure.

Between 1949 and 1954 Muzafer Sherif and his colleagues (Sherif, 1961) conducted a series of studies concerning factors which would reduce hostility between different groups. Their main purpose was to find out if any procedures could be introduced in a frictional group situation that would reduce the friction and conflict between the groups.

The studies were held at Robbers Cave State Park in Oklahoma and involved 22 eleven-year-old and twelve-year-old boys. All subjects came from the same social, economic, cultural, religious and household backgrounds. There were no reported behavior problems or other noted differences among the subjects. In the final study of the series in 1954, the boys were picked up by bus and transported to the camp. They were randomly divided into two matched groups by the researchers. The subjects did not know they were in a research project and were unaware that the camp counselors were actually researchers. The subjects named their groups the "Rattlers" and the "Eagles."

The first goal of the research was to build up a within-group identity and cohesiveness among the experimentally created group. This was accomplished by having each group work on projects. During the phase of within-group team building, the two groups were not aware of each other and did not have any interactions.

After cohesive within-groups had been formed (which took about a week), the researchers attempted to develop a pattern of hostility and strained relations between the two groups by conducting a series of competitive events

including baseball and tug of war. The competitive games lasted for a week. It was announced to the teams that only one team could win the trophy for its team as well as individual pocket knives for all its members by securing the most points. There would be no consolation prizes given to the losers.

In describing this series of competitive encounters, the researchers stated that in the beginning of the competition the winners would show good sportsmanship such as giving "three cheers for the losers." However, such sportsmanship quickly dissipated and was replaced by name calling, destruction of each others property, fist fights and other threats of violence including stuffing socks with rocks.

The researchers described the ensuing hostilities between the groups as being due to the competitive nature of the activities in that there could only be one winner with no opportunities for the loser. The results of some of the competitive encounters were experimentally manipulated so that the overall score between the groups was kept fairly close. This action increased tensions between the groups. In addition to the violence towards each other and their properties, the groups refused to eat in the same mess hall together and would have nothing to do in anyway whatsoever with the other group.

continues on next page

The final phase of the research was to determine if the induced state of conflict between the groups could be dissolved. First attempts to reduce conflict involved contact opportunities between the groups. This involved a bean collecting contest, the showing of a popular film, and the shooting of firecrackers in connection with the Fourth of July. At this point in the study the competitive activities had ceased. However, it was noted by the researchers that the contact opportunities between the groups did not result in any appreciable lessoning of tensions between them. In actuality, several of the contact gatherings had resulted in food fights between the groups. Thus, hostility was still manifested between the groups, even at the conclusion of the competitive encounters.

The next experimental condition involved the introduction of desirable goals that affected each group but could not be attained by the resources or efforts of one group alone. The first situation involved a problem with drinking water for the camp as a whole. It became necessary for both groups to work together to secure the return of drinking water for the camp. Another situation required the cooperation of both groups to secure a popular movie at the time (either "Treasure Island" or "Kidnapped.") At this point in the study the groups began eating together. Further situations involved using a tug of war rope on a dangerous tree that had fallen. The final situation had both groups work on a truck that was stuck in a rut. The truck was carrying food for both groups and required considerable efforts of the boys. In all the situations both teams shared the attainment of the goals. After the truck situation it was clearly seen that there was a lessoning of tensions between the groups. On the last day of camp, at breakfast and lunch, the seating arrangements were mixed up as far as group membership was concerned. The majority of the boys agreed to return to their homes on the same bus together. The seating arrangements on the bus did not follow initial group lines.

The researchers concluded that it is possible to reduce hostility among groups by promoting cooperation on shared goals. The studies showed that simply stopping the competition or bringing the groups together was not enough to reduce the tension and hostility between them. In order for the hostility to be reduced, the different groups had to work together on common goals. Cooperation (i.e., I reach my goal only if you reach yours), was the determining factor in bringing about peace.

Finally, in interpreting these results no single experiment can by itself establish a principle of broad applicability. In addition, conditions of Sherif's experiments differ in some ways from many of our current competitive events for our youth. However, the one clear conclusion of this study is that cooperation and shared goals are key factors in resolving conflict peacefully.

By Dr. Ronald J. Coughlin, Ed.D. President, New Jersey Violence Prevention Institute. Contact Ron at 609-586-7757 or ronc2001@aol.com

References:

Carroll, Lewis. Alice's Adventures in Wonderland. New York: New American Library, 1960.

May, Mark A. and Leonard Doob. Cooperation in Competition. New York: Social Science Research Counsel, 1937.

Sherif, Muzafer, O. J. Harvey, B. J. White, W. R. Hood, M. C. W. Sherif. Intergroup Conflict and Cooperation: The Robbers Cave Experiment. Norman, Oklahoma: University book exchange, 1961.

threat assessment and management training seminar

The Federal Law Enforcement Training Center - Office of State and Local Training (FLETC-OSL) in partnership with the Naval Criminal Investigative Service (NCIS) is proud to announce a FREE three day seminar for law enforcement personnel. The seminar will consist of two days on threat assessment/management from SA Tess Berg and Dr. Russell Palarea of the NCIS Threat Management Unit. It will include the NCIS threat assessment models, conducting threat assessment investigations (stalking, workplace violence, domestic violence, school violence, etc.), assessment of communicated threats, interview recommendations for subjects and victim, conducting violence risk assessments, and developing management plans. The third day will consist of training on Domestic Terrorism by retired NCIS SA Jeff Norwitz.

The seminar will be held in Raleigh, NC on March 1-3, 2011 and in Seattle, WA June 7-9, 2011. Attendance is restricted to sworn law enforcement officers, professional staff, analysts, and other employees of local/state/campus/tribal/federal law enforcement agencies, as well as local/state/federal prosecutors and prosecution investigators. Tuition is free; students are responsible for travel, lodging, and meals. For further information, call 800-743-5382 or e-mail stateandlocaltraining@dhs.gov and reference the "Threat Assessment and Management Training Seminar."

Learn More

(Note: the opinions expressed herein are purely those of the author and not of the FBI or any federal agency.)

opsec

by: G. Wayne Tilman, CPP Unit Chief, Federal Bureau of Investigation, Member, FBI OPSEC Working Group

OPSEC—Operations Security—those of us in the intelligence and law enforcement sectors live it; it is a prevalent training theme of threat assessment professionals, regardless of whether we represent government or private infrastructure.

But, what is OPSEC, and how does it affect you?
The federal subject matter experts are located in the Interagency OPSEC Support Staff (IOS). The national OPSEC members are largely US Intelligence Community (IC) members, plus the General Services Administration. However, the IOS website, https://iad.gov/ioss, is informative and can be accessed by non-federal government individuals seeking further guidance. IOSS identifies five components in the mental process of maintaining good OPSEC:

- Identify critical information
- Analyze threat
- Analyze vulnerabilities
- Assess risk
- Initiate Countermeasures

Others have defined levels of OPSEC in their own terms. Lt. Col. Jeff Cooper, widely acclaimed as the father of modern pistol craft, broke awareness levels down to color codes. Fighter pilot John Boyd enumerated his approach to meeting challenges as the OODA Loop—Observe, Orient, Decide, Act. That sort of strategic planning is indicative of an OPSEC state of mind.

Association of Threat Assessment Professionals (ATAP) members likely perform a myriad of informal, mental threat assessments throughout the day, measuring the risk, probability and impact of day-to-day decisions. That awareness and approach is certainly a form of OPSEC.

Personal operations security is awareness about what your actions, image and demeanor signal to others. What do you wish to project? What about you or your organization do you want to hide from individuals or groups that represent potential threats? Who are those people and groups? They vary in number and identity according to your own

organization or personal history. Are they foreign agents? Terrorists? Criminals? Stalkers? Identity thieves/hackers? Do they represent a threat because of who you are, who you were, or who you represent? Or, have circumstances afforded an evil doer a crime (opportunity) of chance? In other words, assess the risks inherent in everyday actions. Does that make one paranoid? Maybe. Or, perhaps because of what you do, what you used to do, or who you represent, a little paranoia is a good thing…

Do you do follow those procedures that you instruct others to follow? Do you vary times and routes and avoid "give-away" logo wear?

It is safe to assume that a significant part of ATAP membership has an intelligence, military, and/or law enforcement background, without regard to the member's current employer. That very history colors how we approach life, even how we dress.

What signal does the photographer's vest, tactical sunglasses, buttpack, or cargo pants send? Should you wear such things, in combination or alone? Sure! I do. But, I try to be aware of where I should and should not wear them, of the image such outfits project, and whether I (and perhaps accompanying family members) am equipped and willing to deal with how others may perceive an unintended message. If you are the

continues on next page

opsec continued

person dressed as a tactical operator in a convenience store when a holdup occurs, who do you think will be the first target?

When walking, are you constantly aware of potential threats around you (both in your "space," and in reasonable proximity)? Tradecraft, such as stopping and checking reflections in a store front, can be valuable, as can abruptly changing direction and walking back from whence you came.

Despite television and movies, it takes a fairly sophisticated team with multiple vehicles to really "tail" someone effectively. But, just in case, do you check your rearview mirror for the same car behind you for too long? Sure, you may have the same SUV with a family matching your speed on a trip for a lengthy period, but how about in city or suburban traffic? Worried? "Square" the block and see if they are still there. If so, it is time for another threat assessment. But do remember that, trained security driver or not, dramatic turns and running amber or red lights is best left for the television cop shows.

Do you (and family members) generally travel with vehicle doors locked? You should. Do you leave sufficient space at a traffic signal to allow you to drive around the car in front of you, if necessary? In today's communication-intense society, suggesting that you carry a cell phone is superfluous. But, all of us should have reasonable access to a dependable, bright flashlight. It is a legal, always-handy part of good operations security. High lumen tactical lights are my favorite.

How about the personal computer sites? How much "give-away" information to you have on them? Do your family and friends know to not refer to your employer (if that represents a risk)? If even one person in your organization slips, a determined data miner can string together "friends" and come up with a fairly simply obtained list that reflects you and other associates. For those ATAP members, who are still looking for that special person, do not forget that dating sites provide an alarming amount of information about you, including your picture.

Try to make personal OPSEC part of your natural order of things…it will lessen your risks, enhance your confidence that you are doing all you can to keep yourself, your family and your organization as safe as you can. At some point—hopefully most of us are already there—it will become so normal that you will not have to consciously focus on it. It will then be one of the many attributes that characterize you as a cutting edge threat assessment professional.

is your incident reporting system putting your organization at risk?

by: Rick Shaw, CEO/President, Awareity

How is your incident reporting system working for you?
Or perhaps the question should be - Is your incident reporting system working against you?

Lessons learned continue to show that organizations find themselves in 'reaction mode' more than they are in 'prevention mode.' How can this be when most every organization claims to have an incident reporting system in place?

Are traditional incident reporting systems obsolete?
Multiple surveys reveal that 90 percent of bystanders who witness a bullying incident DO NOT report the incident. So why aren't bystanders not reporting incidents?

Perhaps bystanders are not reporting because of one or more of the following reasons:

- Scared to get involved
- Not sure how to report incidents
- Not comfortable with incident reporting options such as paper, in person, phone or text

continues on next page

- Lack of anonymity when reporting incidents
- Bystander does not trust the incident reporting system will work
- Bystander does not trust the organization will take action
- And many others…

Victims are also reluctant to use traditional incident reporting systems. Victims want to be heard, but many victims do not trust traditional incident reporting systems due to:

- They tried using the traditional incident reporting system and nothing happened
- No anonymous option to report incidents
- Not knowing who was on the other end of the incident reporting system
- Afraid their information would not be kept confidential
- And many others…

Like bullying and cyber bullying, workplace violence incidents seem to be increasing too. Mounting stress related to economic challenges, job layoffs and mortgage foreclosures continue to affect millions of individuals and families. And some individuals have taken out their frustration on their bosses, their co-workers or their family members where they work, and many of the incidents could have been prevented based on red flags that were discovered after the incident.

Suicides and bullycides seem to be increasing too. According to statistics from support organizations, 5,000 teenagers commit suicide a year and perhaps as many as 500,000 or more teenagers contemplate suicide or attempt suicide each year. What if these 5,000 teenagers had a trusted incident reporting option they could have reached out to for help?

So is your traditional incident reporting system really working for you if bystanders are not reporting incidents and victims are not reaching out for help?

Red Flags and Prevention

Without red flags, it is nearly impossible for security teams and threat assessment and intervention teams to prevent incidents from happening. Yet after almost every bullycide or workplace violence incident, people come forward and say they were aware of multiple suspicious incidents and red flags, but did not report the suspicious incidents because they did not know how to or did not understand what suspicious activities should be reported. In some cases, people DID report the incidents and unfortunately the organization did not connect the dots.

Legal Defensibility

In our highly regulated and litigious society, victims and their families are taking organizations to court when they fail to respond as mandated. Many lawsuits brought against organizations cite **"deliberate indifference"** or ***the conscious or reckless disregard of the consequences of one's acts or omissions.***

Deliberate indifference is often the result of:

- Lack of Awareness – meaning people did not know what to do in different situations even though previous incidents, legal obligations and regulatory mandates exist
- Lack of Follow Through – meaning people knew about the issues, but did not take immediate actions to end the issue and did not take appropriate actions to eliminate the hostile environment and prevent future incidents
- Failed efforts based on the situation, state mandates or organizational obligations

Experts seem to be in agreement that reacting to incidents is much more expensive (and embarrassing) than preventing the incidents from happening, but prevention requires a more comprehensive suite of incident reporting tools to ensure:

- Anonymous or non-anonymous incident reporting tools
- Threat Assessment and Security Team collaboration tools
- Secure and confidential information sharing tools
- Situational awareness tools for all appropriate individuals and team members
- Accessibility options for anytime access to suite of tools
- Documentation / Reporting tools of entire process for compliance and legal defensibility
- And adaptability options as needs and situations continue to change

Is your traditional incident reporting system helping you or working against you?