



## ASJA LAW AND POLICY REPORT

Thursday February 21, 2008

No. 277

\*\*\*\*\*

ASJA Law and Policy Report (LPR) is written by Gary Pavela ([www.garypavela.com](http://www.garypavela.com)) and published weekly (except weeks of national holidays; during the ASJA National Conference and Gehring Academy; from mid-December to mid-January; and the month of August). Copyright: ASJA and Gary Pavela: All rights reserved. Further transmission within ASJA member institutions is permitted, if the author and ASJA are credited as the source. Index, archives, and additional source materials will be available to ASJA members at [www.asjaonline.org](http://www.asjaonline.org). The information and comments provided here are designed to encourage discussion and analysis. They represent the views of the authors (not ASJA) and do not constitute legal advice. For legal advice the services of an attorney in your jurisdiction should be sought.

\*\*\*\*\*

### TOPICS IN THIS ISSUE

08.7 Creating a college threat assessment program

08.8 READINGS

[a] The copycat phenomenon is real

[b] There is no "accurate or useful" profile of school shooters

[c] "Discretion is an important tool for keeping order"

\*\*\*\*\*

08.7 Threat assessment

#### **Creating a college threat assessment program: An interview with Dr. Gene Deisinger**

*Editor's note: This interview appeared last month in The Pavela Report. We share it with ASJA members in light the recent rampage shooting at Northern Illinois University.*

State and national reports after the Virginia Tech shootings called for the prompt implementation of such programs at colleges nationwide. What's been difficult to find, however, are model programs with established records. For help in that regard we turned to Gene Deisinger, Ph.D., Commander of the Special Operations Unit with the Iowa State University Police Division and a founding member of the Iowa State Critical Incident Response Team (CIRT), created in 1994. Dr. Deisinger is licensed psychologist, a certified health service provider in psychology, and a certified peace officer. He has served as the primary threat manager for CIRT since the team's inception. In addition to his duties at Iowa State, Dr. Deisinger provides operational support and training for several local, state, and federal law enforcement agencies and serves as a Special Deputy United States Marshal with the FBI Joint Terrorism Task Force. He can be reached at: [erdeisin@iastate.edu](mailto:erdeisin@iastate.edu)

#### **LPR: Your program started long before the Virginia Tech shootings. What prompted you to create it?**

*Deisinger:* In the early 1990's we experienced a set of crisis situations that illustrated the need for greater communication, collaboration and coordination among university departments. We identified situations where individual departments had (or were aware of) information that turned out to be relevant. However key decision makers in other

departments, impacted upon by the person or situation, were not aware of that information. Therefore, they held an incomplete picture of the situation as it actually existed.

We also observed that individual departments brought to bear a wide range of expertise and resources, but typically implemented their approaches to crisis situations independent of other involved departments. On occasion, this resulted in an escalation of the crisis that was not anticipated (because no one was looking for it), and for which we were not adequately prepared to manage.

Finally, we noted that there was no agreed upon plan or authorization for decision-making in such complicated situations. Each department (based on their own training, views, resources and methods) controlled their responses, but no one entity had authority to coordinate a collaborative response to the crisis.

Based on those observations, representatives from university police and student affairs, developed a proposal for a multi-disciplinary group that would manage crises impacting upon the institution. This group would consist of key decision-makers who were in roles already identified as key to effective sharing of information and incident management. The group includes representatives from campus police, human resources, employee relations, provost's office, student counseling, dean of student's office, residence, university relations, risk management and university counsel. Persons in these roles were regularly involved in dealing with crisis situations and already held authority for decision-making in their respective areas. The group, the Critical Incident Response Team (CIRT) was authorized by the university president to manage campus crises.

The Team would be supported by a Threat Management Team consisting of a subset of CIRT members from police, student affairs and human resources. The Threat Management Team would conduct assessments of threatening situations and then develop & implement management strategies.

**LPR: Please outline the core components of your program.**

*Deisinger:* The core components of the Iowa State University crisis management approach include:

- Clear policy and standards of behavior
- Community awareness and training regarding risk indicators
- Centralized reporting of threatening situations
- Multi-disciplinary approach to threat assessment and management
- Timely assessment of and response to developing concerns
- Collaboration and coordination with a variety of resources
- Support and assistance for resolution of the situation

**LPR: How does threat assessment differ from profiling?**

*Deisinger:* Profiling is an investigative technique that utilizes observations about a crime scene (or pattern of crimes) to generate hypotheses about characteristics of an unknown suspect. These characteristics are presumed to be relatively stable over time. The purpose is to aid law enforcement in generating potential suspects when few (or none) have been previously identified; or to help reduce a suspect pool to a subset of people who more closely resemble those who are known to have previously committed similar crimes. In essence a profile is providing an indication of the degree of similarity between a suspect and characteristics of known offenders.

A threat assessment is a safety management tool that is based on information and observations about a specific situation. Threat assessment focuses on a subject's behavior and information about the situation to determine the likelihood of escalation in behavior. A threat assessment is a dynamic process, recognizing that threat levels are affected by a number of variables, many of which change over time and as interventions or stressors are modified. The purpose of a threat assessment is to anticipate reasonably foreseeable actions of a specified person, or to anticipate likely changes in a specific situation. The assessment allows for early identification of situations that are likely to pose a risk, provides a baseline against which to measure changes in the situation, and facilitates development and implementation of interventions to increase likelihood of a safe resolution.

### **LPR: Does threat assessment involve predicting future behavior?**

*Deisinger:* Threat assessment and management are much more about preparing for future behavior than they are about predicting behavior *per se*. Threat assessment and management are fundamental to our survival as human beings. Throughout our day we gather information, assess the risk to ourselves (and our projects, our jobs, our families, etc.) and we make changes in our lives to deal with those risks. While we are trying to look into the future we aren't primarily interested in predicting. Instead, we are more interested in preparing for potential (and reasonably likely) threats, and decreasing our vulnerability – this is threat assessment and management.

Let me give an example to illustrate. Imagine that we are driving our car and come to an uncontrolled intersection at the same time as another driver. We want to make a turn through the intersection that would take us in front of the other vehicle. Clearly we want to do that without hitting the other car or being hit by it. Do we just predict whether the other driver is going to yield to us and then go (or not go) based on the prediction? If so, we would likely be the exception to the rule. More likely we will attempt to gather information about the threat posed by the other vehicle. How fast is it approaching the intersection? Is it likely to be able to stop in time to avoid striking us? Is the driver showing any indication of their intended behavior? Does the other driver show any awareness of our presence near the intersection? Based on these (and numerous other observations) we make a decision about whether to proceed through the intersection. If we proceed, we adjust our speed and our movement through the intersection in a manner that allows us to adjust to the other driver's actions. Depending on our assessment of the risk, we may also set down our cell phone, put both hands on the steering wheel, reduce our focus on the song playing on our favorite CD and move our left foot closer to the brake – just in case!

### **LPR: Who should be on a threat assessment team?**

*Deisinger:* This varies by the needs of the institution, the threats likely to be encountered, and the resources available. However, it is critical that no one entity is placed in a position of being solely responsible for assessing and managing threats. Threat assessment is best done through consultation and collaboration with other persons who are trained in assessment and management of volatile situations. Campus law enforcement or security officials should play a key role in threat management teams as they are mostly likely to have the resources and training to deal with imminent threats to the community. Student affairs and human resource professionals are also key given the range of legal and procedural issues that may come into play.

### **LPR: How can mental health professionals serve on a threat assessment team if they are obligated to protect confidentiality?**

*Deisinger:* A licensed mental health professional is a key resource for a threat assessment and management program. Such a professional can offer significant insights that may aid threat assessors in understanding the behavior of mentally ill or emotionally disturbed persons and anticipating likely responses to interventions or further stressors. Most mental health professionals have extensive experience in dealing with emotional crises and can recommend interventions to help de-escalate a person in crisis. They are also likely aware of referral resources on campus and in the community that may be helpful support systems for the person of concern.

Confidentiality applies to situations where a person is a client/patient being served by the team's mental health consultant (or the agency in which the professional is employed). Even in those circumstances, the mental health professional can still provide general consultation to the team about mental health issues, resources, intervention approaches, etc. — so long as they do not provide personally identifiable information about the client or the client's involvement in services.

It is also important to remember that confidentiality is governed by the wishes of the client, not the mental health provider. That is, a client can sign a release authorizing the mental health professional to disclose personal health information to the team. My experience (both as a clinician and as a threat assessor) has been that clients generally cooperate with such requests for releases -- when the client understands how beneficial it is to them to take advantage of a team approach to their care and safety.

Finally, mental health professionals are allowed to share information in circumstances where they reasonably believe the client poses an imminent danger of serious injury to themselves or to others. In those circumstances, a mental health professional cannot usually share the client's entire mental health service history, but can and should share sufficient information to allow for warning and/or protection of any potential victims.

## **LPR: What does threat assessment training normally entail?**

*Deisinger:* There are two aspects of training. First is training for those who will conduct the actual threat assessment. This training should involve understanding of:

- Accepted principles in the practice of threat assessment and management;
- Role of mental health and substance abuse issues;
- Intervention strategies for de-escalation;
- Awareness of community resources, and
- Legal and policy issues

Training is also critical for people who are in gatekeeper roles, i.e., those that are likely to become aware of a threatening situation. This includes all members of the community — faculty, staff and students. Therefore there must be multiple methods of providing information and training about indicators of persons who may be at risk of:

- Harm to self
- Harm to others
- Diminished ability to care for self
- Significant disruption to the learning or working environment
- Awareness of reporting mechanisms
- Awareness of referral resources
- Basic de-escalation strategies
- Responses to violent incidents
- Resources for recovery following an incident.

## **LPR: Where is threat assessment training available?**

*Deisinger:* There are a variety of outstanding training opportunities and resources available:

The Association of Threat Assessment Professionals ([www.atapworldwide.org](http://www.atapworldwide.org)) hosts national and regional conferences with members from professions including law enforcement, prosecutors, mental health, research and academia, corporate security & protective services, and victim advocacy.

Specialized Training Services ([www.specializedtraining.com](http://www.specializedtraining.com)) has provided training utilizing some of the mostly highly regarded professionals in the field.

Several private security and consulting company provide exceptional training opportunities. Gavin DeBecker & Associates host an Advanced Training Academy for a select group of threat assessment professionals representing governmental agencies, corporations and institutions of higher education.

## **LPR: Do colleges and universities have something to learn from schools in creating and managing threat assessment procedures?**

*Deisinger:* Yes, though we need to carefully consider the applicability of the lessons learned in other settings. All in all, a larger proportion of secondary school systems have been involved in threat management, for a longer time, than have many colleges and universities. Higher education can learn from some of the early mistakes made in school and

workplace settings such as rigid implementation of zero tolerance policies and concerns about adverse labeling of youth. Many schools have developed very effective methods of early identification, intervention and management of threatening situations. Applied effectively, such approaches have resulted in de-escalations of the threats posed and often facilitated (formerly) threatening subjects to be more effective and positive members of their community.

However, I caution against a procrustean approach to program development that is driven by a "one size fits all" mentality. Each institution needs to examine and assess its system, needs and resources to determine the approach that will best improve safety. There are certainly core principles that all programs will include, but the procedural implementation of those principles may vary widely.

**LPR: What common mistakes are made in creating and managing a threat assessment team?**

*Deisinger:* The most common mistake that I see when working with colleges and universities in establishing and developing their teams is lack of clear authority to fully manage threatening situations and to make critical decisions. Threat management cases regularly involve volatile and rapidly-evolving situations that necessitate thoughtful, timely and coordinated interventions. The power of team collaboration is immense. A multi-disciplinary team provides an opportunity for maximizing information streams, facilitates consideration of multiple perspectives, and increases the range of strategies and resources that can be brought to bear. However, there must ultimately be an identified decision-maker who reviews the information available, considers a range of reasonable interventions, and then directs implementation of a specified strategy. The team must ultimately speak with one voice so that there is shared understanding, acceptance, engagement and coordination with the intervention.

\*\*\*\*\*

08.8 READINGS:

[a] **The copycat phenomenon is real.** From the year 2000 FBI report "The School Shooter: A Threat Assessment Perspective" (National Center for the Analysis of Violent Crime, Federal Bureau of Investigation) ("FBI"):

School shootings and other violent incidents that receive intense media attention can generate threats or copycat violence elsewhere. Copycat behavior is very common . . . Anecdotal evidence strongly indicates that threats increase in schools nationwide after a shooting has occurred anywhere in the United States. *Students, teachers, school administrators and law enforcement officials should be more vigilant in noting disturbing student behavior in the days and weeks or even several months following a heavily publicized incident elsewhere in the country* (emphasis supplied) (p. 24).

See: <http://www.fbi.gov/publications/school/school2.pdf>

[b] **There is no "accurate or useful" profile of school shooters.** From the "Final Report and Findings of the Safe Schools Initiative" (United States Secret Service and United States Department of Education) (2002):

There is no accurate or useful profile of students who engaged in targeted school violence . . .

The demographic, personality, school history, and social characteristics of the attackers varied substantially. Knowing that a particular student shares characteristics, behaviors, features or traits with prior school shooters does not help in determining whether that student is thinking about or planning for a violent act.

The use of profiles in this way likewise is not an effective approach to identifying students who may pose a risk for targeted school violence at school or for assessing the risk that a particular student may pose for a school-based attack, once a particular student has been identified. Reliance on profiles to predict future school attacks carries two substantial risks: (1) the great majority of students who fit any given profile of a "school shooter" will not actually pose a risk of targeted violence; and, (2) using profiles will fail to identify some students who in fact pose a risk of violence but share few if any characteristics with prior attackers.

Rather than trying to determine the "type" of student who may engage in targeted school violence, an inquiry should focus instead on a student's behaviors and communications to determine if that student appears to be planning or preparing for an attack. Rather than asking whether a particular student "looks like" those who have launched school-based attacks before, it is more productive to ask whether the student is engaging in behaviors that suggest preparations for an attack, if so how fast the student is moving toward attack, and where intervention may be possible (p. 34).

[http://www.secretservice.gov/ntac/ssi\\_final\\_report.pdf](http://www.secretservice.gov/ntac/ssi_final_report.pdf)

[c] "**Discretion is an important tool for keeping order.**" From Katherine S. Newman, *Rampage: The Social Roots of School Shootings* (2004):

A 1994-95 study of seventh to twelfth graders found that students felt less connected to their school when it temporarily adopted a policy of expelling students for infractions such as possession of alcohol and for their first major rule infraction. Given what we have learned about the importance of breaking down communication barriers between adolescents and adults, the last thing we need are policies that widen the social gaps between them . . .

Discretion is an important tool for keeping order. If students believe that their teachers and administrators are unable to exercise any judgment, they are not likely to consider them people they can confide in or trust p. 285-286.