SECURITY MANAGEMENT
SECURITY'S WEB CONNECTION

Published on Security Management (http://www.securitymanagement.com)

Teaming Up to Reduce Risk

By Matthew Harwood
April 2008

When a former Iowa State University employee applied for a weapon permit late last year in another jurisdiction, the school had cause for concern. The employee had recently been fired for behavior that negatively affected his work and the work of others. Fortunately, Commander Gene Deisinger, a member of the university police's Special Operations Unit and a licensed psychologist, had already reached out to the local county sheriff's office, where he knew some officers. He had asked that they contact him if the former employee applied for a weapon permit, explaining that his threat assessment team checked the subject's background and found worrisome signs that the person could pose a threat to himself or others.

Due to Deisinger's proactive approach, the sheriff's office kept him in the loop. He was informed when the former employee applied for a gun permit, and Deisinger was told that, based on information the sheriff's office had locally, the application was denied.

Informed of this development, Deisinger's threat assessment team members could reassess the risk. They asked themselves, "Is there a nexus of threat to our locale?" With their subject unable to procure a weapon, and no evidence of other access to weapons or changes in the situation, they decided that there was no need to adjust security measures on campus at that time, though they would continue to monitor the case.

Iowa State's program has been in place for years, but other campuses are only now recognizing the potential benefits of threat assessment teams. They are acting in response to the 2007 Virginia Tech tragedy in which a disturbed student, Seung Hui Cho, murdered 32 people and then killed himself.

These teams, sometimes referred to as threat management teams or critical analysis teams, provide schools with a formal mechanism for analyzing sensitive information on troubled persons to assess whther there is a threat and to develop a plan of response.

In the Beginning

The concept of threat assessment teams is not new. The first behavioral threat assessment unit was created inside the Los Angeles Police Department (LAPD) in 1989 by then Captain Bob Martin. Not long after, the idea found its way onto college and university campuses, says Martin, who is now vice president of Gavin de Becker and Associates, a leading threat assessment and management firm.

Some of the more prominent universities that adopted the approach include Arizona State, Iowa State, Pennsylvania State, and the University of Maryland. Each of these schools shared similar advice about how to establish effective programs. Their suggestions track recommendations from the Virginia Tech task force and from other private sector behavioral analysis experts interviewed for this article. Key issues include how to form a team, how to raise awareness, and how to work a case until it is neutralized.

Team Formation

Team members must bring to the table the right spectrum of skills. They should be recruited from across the campus community to make the team as representational as possible. But team members must not only be knowledgeable; they must also be senior level personnel with the authority to take action. Anyone selected to serve on a behavioral threat assessment team should be "at a level where they can commit or make a decision for their organization," says Martin.

Virginia Tech had no formal threat assessment team, but it did have what it called the Care Team, responsible for identifying and helping students with problems. That team, however, lacked a representative from the Virginia Tech Police Department.

As a result, the Care Team had no knowledge that Cho had been warned twice against stalking, "that he had threatened suicide, that a magistrate had issued a temporary detention order, and that Cho had spent a night at [a psychiatric ward] as a result of such detention order," said the Virginia Tech Review Panel's report.

The review panel recommended that key players in any threat assessment team should include representatives from law enforcement, human resources, student and academic affairs, legal counsel, and mental health functions.

Similarly, New Jersey's Campus Security Task Force, in its own report on campus violence, recommended assembling a team broad enough that "there is a greater possibility of identifying a student who may be displaying patterns of behavior that cause concern."

In including a representative from human resources, the team should also keep in mind that threats don't just come from the student body; they come from faculty and staff too, says Deisinger.

As the recent shooting at Northern Illinois University (NIU) proves, threats can also arise from former students with no history of problems. A former award-winning graduate student, Steven P. Kazmierczak, was described as "gentle" and "hard-working" with "no record of trouble." On Valentine's Day, he burst into a lecture hall and shot five students dead before taking his own life. Because Kazmierczak, who was no longer a student at NIU, had no known history of aggressive or violent behavior, it would have been impossible for him to have appeared on a behavioral threat assessment team's radar, no matter how representational of the university the team was.

Once membership is determined, officials must next establish team structure. No one should have significantly more power than anyone else in the group, says Martin. That does not preclude having a leader, but because each member of the team shares the same relative status within the university, the team works best when it functions more as a democracy than as a dictatorship. "You want an environment where people are comfortable sharing their point of view," he says.

Jim Cawood, president of Factor One and the current president of the Association of Threat Assessment Professionals, agrees. It's easy to form teams, he says. "The question is once they're drafted and sitting in a room together, do they truly get along?

Raising Awareness

Colleges and universities are unique environments. Students and faculty alike see campuses as free and open places that celebrate difference and abhor conformity. This makes for a difficult world in which to encourage people to report concerns about each other to a higher authority, such as a behavioral threat analysis team.

Administrators can, however, reduce that hesitancy through public education campaigns that use educational and training sessions, combined with posters, mailers, e-mails, and Web pages. These programs should communicate the team's sensitivity to confidentiality and discretion, emphasizing that the team respects the privacy of both the person submitting the tip and the subject of the tip.

Any educational campaign must drive home the important role that the students and faculty play in providing information. Officials should stress that students and faculty who pass along concerns, however small, may help save lives. They should also stress that the system may not work without that input. The message the team must convey to the campus, says

Deisinger, is that "we have a process that works well with your help."

Arizona State University (ASU) holds educational and training sessions several times a year for students, faculty, and staff. All new students and parents are asked to attend a session during orientation to discuss how to report concerns, as are new employees when they come on board. The sessions are not mandatory, though, except for resident assistants and hall directors. "Because they live among the students," Commander Richard Wilson of the Arizona State University Police Department explains, "they have the broadest exposure to identifying students dealing with academic, social, family, or personal stressors. Early recognition allows early intervention and can prevent things from escalating."

ASU also maintains Web sites and Web links that provide further information on handling at-risk persons on campus. In addition, the school occasionally sends out e-mails reminding the university community to be on the lookout for at-risk students during times of high stress, such as during midterms and finals.

The goal of these outreach efforts is to make the campus community, especially students, comfortable reporting abnormal or threatening behavior to campus leaders. Sometimes making people more comfortable reporting concerns comes down to semantics, as Wilson learned during one session for faculty. During the gathering, team members were teaching professors how to initiate a threat assessment action by filling out an online complaint form to the dean of students.

A senior professor stood up and told team members that most faculty members would never fill out a complaint form, because the word “complaint” made the form seem negative. He suggested calling them “incident reports” instead.

“That was very insightful,” says Wilson. The team took the professor’s advice and revised the form.

The most important faculty members to train and educate in threat awareness, however, are teaching assistants, says Wilson. “Teaching assistants are critical because they have more contact with students,” he says. Moreover, as they are in a quasi-peer position, he notes, “they are more apt to pick up on leakage or observe behavioral changes.”

Not surprisingly, the Virginia Tech tragedy has helped to change attitudes about sharing information or reporting a suspicion that a person might be at risk. “If there’s anything good to come out of Virginia Tech,” says Assistant Chief of Police Clifford Lutz of Pennsylvania State University, “it’s that you have the opportunity to get buy-in from all the stakeholders, because everyone realizes how catastrophic one of these types of incidents can be to a university community.”

But as Virginia Tech fades from the collective memory, the former reluctance to report suspicions may return. It is, therefore, important for public awareness and education initiatives to continue.

Working a Case

As tips flow in, assessment teams must determine quickly which issues “are the ones we have to pursue versus the ones we don’t have to pursue,” says Cawood.

Records. The first step in the process is fact finding. Teams should set up a centralized clearinghouse of information, with a smaller, specially trained squad to gather data. These specialists should coordinate information sharing with team stakeholders to access whatever unprotected departmental information they have on the student, faculty member, or staff member being investigated.

The team should check all available criminal, court, and driving records from all jurisdictions where the subject has lived. Because higher education students, faculty, and staff come from across the country, their background records will cross multiple jurisdictions. To that end, campus police should liaise with, or have mutual-aid agreements with, law enforcement in other jurisdictions.

Another good practice, Cawood says, is to interview the subject’s friends and associates, especially neighbors from past addresses. “This can be an excellent resource for information on disturbances, police responses, and past boy or girlfriends,” he says.

As the team collects information, the data should be entered into a centralized database so that the members can create a historical record and track any changes in an individual’s behavior over time.

Subject interviews. If a subject of interest raises enough concern within the threat assessment group, the next step is a direct interview. Depending on the context, that interview may be conducted by someone on the assessment team or by a third party selected by the team.

At Iowa State University, most of these interviews are performed by plain-clothed police officers, says Deisinger. At ASU, Wilson says, a representative from the department where the threat originated conducts the interview. Interviews at the University of Maryland are conducted by the head of the office for student conduct most of the time, simply because it is the body that has the authority to require the student to appear before it, says Jonathan Kandell, assistant director of the University of Maryland’s Counseling Center and chair of the school’s Behavioral Evaluation and Threat Assessment Resource Group, or BETA team.

Interviews serve several purposes. Most important, perhaps, interviews allow the assessor to look the subject in the eye. Public records and collateral information, while a guide, are historical and say nothing about the present. “Only the person, live and in front of you, knows what’s happening right now in their head,” says Cawood.

“If I get a chance to sit down and talk to an individual,” he says, “who better to tell me about whether or not they are serious than the individual himself?”

The interview locale can also make a difference. At Iowa State University, Deisinger remembers a male student who threatened to kill several teachers and threatened area businesses. Deisinger and a city detective interviewed the subject at home where they observed a cache of weapons, read his writings, and discussed his grievances. They determined that he did pose a significant threat.

But because they were talking to this young man in a nonthreatening way and listening to his side of the story, Deisinger and the detective also gained his trust enough to de-escalate the situation. Without incident, Deisinger was able to confiscate the subject's weapons, hospitalize him for psychiatric evaluation, and manage the situation into the future.

Deisinger made sure that the hospital notified him when the subject was released, allowing him to continually reassess and manage the situation. Deisinger continued to visit the subject at home, and he kept in contact with his potential targets to see whether they had been threatened again. In one instance, Deisinger even provided the subject transportation to and from one of his therapy appointments.

The interview also gives the subject a forum to air grievances. Sometimes, that's enough. The subject vents and feels that someone is listening, that someone cares, and that he or she is not alone.

This leads to the final reason for interviews: choice points. Interviews can show a possible aggressor that there are alternatives to violence. By understanding where a subject is coming from, even if his perspective is delusional, a well-trained interviewer can move him away from violence, says Cawood.

Subject interviews, however, present one potential pitfall: Some threat assessment practitioners believe that an interview may confirm a paranoid subject's irrational fear that the system is out to get him or her, making that person less reasonable and more aggressive.

The case manager must make that judgment call. Interviews should be considered as one of many options available when working on a case, says Martin.

Assessment and Response

After all possible information has been gathered, it is reviewed by the team to assess the level of risk and determine a course of action.

There are times when an assessment team finds that the subject is simply enraged about being charged administratively with a minor violation of a university rule. The situation then escalates because a campus bureaucrat holds strong and says he or she can't overlook the subject's infraction. "Sometimes," says Martin, "we have to say, 'Break the rule. Make the exception…if that's what it takes to defuse a volatile situation.'"

Of course, students also have to know that threats and violence are not the way to resolve such problems. So at the same time that the team may help to address the issue, it also has to address the student's behavior.

Most threat assessments determine that a subject is not a risk. But the process is constructive even in those cases, because it serves as an early warning for possible future problems. A record is established, and if a later report on the same person is brought to the assessment team, its database will show that a pattern may be developing. The two events will have more significance than each would have if the dots were not connected.

"Threat assessment isn't a snapshot, it's an ongoing process," says Wilson.

The team may also decide to proactively reassess a person of interest without waiting for another tip to come in. The team looks for signs of negative developments in situational factors, such as academic performance or social standing, which may become catalysts for violence. They seek out people who know the subject and interview them to see if any changes in behavior have been observed. Constant re-evaluation ensures that a potential threat won't fall off the radar screen as it grows.

The objective of assessment teams is not only to protect others from potentially violent individuals but also to help those exhibiting violent behaviors from harming themselves and their futures. As Wilson says, "You're looking for behaviors that you can address early to get people back on track to be successful."

No one knows what may have happened if Cho had remained under close observation and received the mental health assistance that he needed before his descent into darkness at Virginia Tech. The result could have been the same, or maybe he could have gotten help that would have saved him and his victims. By formalizing behavioral threat assessment teams and agreeing on a common methodology for their tasks, colleges and universities may improve the odds that at-risk individuals on campus are identified and given the help they need before tragedy strikes.

Links:
[1] http://www.securitymanagement.com/magazine/2008/04
[2] http://www.securitymanagement.com/navigating-privacy-protections