

THREAT ASSESSMENT

ON THE BOOKS

Centralized and secure record-keeping is key for Virginia colleges

By Katie Johnson



Viadrin/Shutterstock.com

BY NOW, MOST COLLEGES HAVE TAKEN STEPS TO FORM A THREAT ASSESSMENT TEAM THAT INVESTIGATES A RANGE OF CONCERNING BEHAVIORS AND POTENTIALLY DANGEROUS SITUATIONS, INCLUDING THREATS MADE BY STUDENTS, EMPLOYEES, FACULTY AND OTHERS IN THE COMMUNITY.

Threat assessment teams typically include five to 10 members and should be multi-disciplinary, including representatives from college administration, law enforcement, mental health and legal counsel. Taking on the role of a threat assessment team member is an added and important responsibility. Lessons learned reveal the key to keep-

ing assessment teams from becoming overwhelmed is to ensure the right processes are outlined and the right tools are used.

A recent survey revealed 70 percent of campus threat teams are meeting once or twice a week to review current situations. With mounting job responsibilities, finding time to get together in person and discuss is difficult.

Several colleges in Virginia have implemented Awareity's threat assessment, incident management and prevention services (TIPS) platform to help manage and coordinate threat team efforts, saving valuable time and resources, while improving collaboration and information sharing.

THE FIRST THING TO DO

When a threat report is received, the first task of an assessment team is to collect as much information as possible to determine the potential for risk. Threat cases require an individualized approach, and the more information gathered the better. Gathering this information may include interviewing the individuals involved, speaking with faculty and friends, reviewing social media, and/or conducting a formal law enforcement investigation. Keeping track of the steps taken during this investigation and coordinating all actions and communications between team members is where TIPS delivers valuable advantages.

No longer do assessment teams need to find a time/place for everyone to meet, but team members can easily login and document their findings and case notes, set tasks for other team members, etc. and all other team members can review the investigation and ongoing updates in real-time, rather than waiting for their next meeting.

All actions are date/time stamped, providing legal-ready documentation and accountability, while also ensuring appropriate steps are taken to most effectively intervene and prevent a situation from escalating into something much worse.

Equipping your threat assessment team with a centralized platform is critical. Lessons learned reveal how organizations often fail to connect the dots. A working platform allows all team members to search related reports involving one or more people, review previous reports, investigations and actions, and assess a more comprehensive pattern of behavior. As we learned from the tragic Virginia Tech massacre, many people observed concerning behaviors prior, but these concerns were not routed to one central place to be connected and the seriousness of the threat(s) accurately identified.

KEEPING RECORDS

Threat assessment record-keeping can be difficult because records may include sensitive information or even criminal records that do not fit into previously established conventions, like student records systems. In fact, if your campus is currently placing threat records in your student conduct or student information system (SIS), you may be inadvertently putting this information at risk to unwanted exposure and liabilities.

This common misunderstanding about where to place and maintain threat records creates a disparity with FERPA and is costing colleges in numerous ways. Not only are threat records put at risk in an SIS, some assessment team members are not putting key information into the SIS, which means other team members are not seeing all details and are unable to make the right decisions. FERPA clearly identifies “law enforcement unit” records can and should be kept separate from SIS records.

The Virginia Threat Assessment State Law Guidance also recommends threat assessment teams keep threat records separate from student records and treat them as “law enforcement unit” records. These records should only be accessible to authorized team members and personnel.

The American National Standards Institute (ANSI) Workplace Violence Standard also clearly states that organizations should provide secure, “need to know” and anytime access to a centralized record keeping platform.

TIPS allows teams to be more efficient and track and document investigation notes in one place. Team members can, of course, still access SIS to locate information like class schedules or contact information, and share this information as needed within TIPS, but keeping the actual investigation details and assessment separate from your SIS is vital. Once the threat assessment process has been concluded or a

resolution has been determined, for instance, suspension from campus, a summary can/should be recorded in the SIS, but all investigation prior should only be discussed between team members and documented in the secure centralized platform.

Of course, connecting the right dots means collecting all the dots first. How can threat teams ensure they are receiving information? Use of a comprehensive platform offers an anonymous incident reporting option. A TIPS reporting button is strategically placed on the campus website allowing anyone to securely report concerning behaviors. Campus threat teams can determine what types of incidents should be reported (sexual misconduct, threats to harm, weapons, drug/alcohol abuse, self-harm/suicide threats, suspicious persons).

Thomas Nelson Community College, the first Virginia community college to implement the TIPS prevention platform in 2012, had established a web-based reporting form, but the customization features available in TIPS provided significant advantages.

“Being able to determine what types of incidents could be reported and design the forms and questions based on our current procedures made the transition to TIPS simple,” said campus police chief Kelvin Maxwell. “The way in which reports from different locations and incident types could be directed to the appropriate staff, helped us ensure the right people were being notified so immediate and proactive actions could be taken.”


In addition to Maxwell, Thomas Nelson’s Threat Team also includes the vice president for Finance and Administration, Human Resources, campus police and student counseling staff. General counsel is also added to specific reports; with TIPS third-party resources law enforcement, mental health, compliance, etc. can become involved and added to individual reports in the system, if, and only when, their guidance is requested.

Campus-wide awareness and education regarding reporting of concerning behaviors is critical—all resident advisors, mental health counselors, academic advisors, faculty members, etc. need to understand how concerns should be communicated. Ongoing reminders should emphasize how everyone plays a role in keeping their campus safe and helping people in distress, whether or not a direct threat has been made.

At the beginning of the semester, Germanna Community College posted several awareness posters around campus with examples of the different behaviors to be reported.

“Students really appreciate that we are taking extra steps to involve them in safety efforts on campus,” said Pam Frederick, dean of student development at Germanna. “They really are our best eyes and ears on campus.”

“TIPS allows anyone associated with the college community to come forward and anonymously share information with us,” Frederick said. “The information is immediately communicated to our team and proactively investigated so we can prevent situations from escalating.”

Once an investigation is determined to be “resolved,” it is also important to follow-up and monitor at-risk individuals. The follow up process may be as simple as checking in with the student (or parents, roommates, counselor of the individual involved) periodically and ensuring the situation is not escalating. TIPS provides a valuable reminder tool that ensures follow-up actions are taking place and no individuals slip through the cracks. 



Katie Johnson is the vice president of marketing and client services for Awareity.