Behavioral Intervention v. Threat Assessment: Best Practices for Violence Prevention

By: Brett A. Sokolow, JD and W. Scott Lewis, JD

Across the country, colleges and universities are implementing or revising their models for proactive, early intervention with at-risk students and staff. We call these teams by varying names, including:

- BIT (Behavioral Intervention Team)
- BAT (Behavioral Assessment Team)
- SOC (Students of Concern)
- CARE (Campus Assessment, Response, Evaluation)
- TAT (Threat Assessment Team)
- CCT (College Concerns Team)
- TABI (Threat Assessment and Behavioral Intervention)
- CAT (Campus Assessment Team)

Combine the last two, and you'd have a TABI CAT, among a myriad of other names, acronyms and approaches across campuses. Some campuses have more than one team, while other campuses have only one. For those campuses that have more than one team, it is common to divide functions between one team that is responsible for threat assessment (TAT) and a second team that is responsible for behavioral intervention (BIT).[1] High-risk situations go to the TAT, lower risk to the BIT. While we think this approach can work, it would be an exception, not the rule. Separating these functions may prove literally fatal on some campuses.

Separate Behavioral Intervention and Threat Assessment Teams

Some campuses have separate teams because they already had a BIT of some form, and added the TAT later based upon recommendations made in the Virginia Tech Governor's Panel Report and by other panels and commissions that recommended threat assessment teams for campuses.[2] Other campuses developed two teams to keep the volume of reports from overwhelming any one team. Other campuses saw logic in separate functions because the BIT's lower-level situations implicated a counseling-led approach, whereas the TAT functions invoked law enforcement and high-level

---

[1] We are not referring here to the campus emergency management team (EMT) or Critical Incident Response Team (CIRT), which is a separate function entirely from a behavioral intervention or threat assessment team. Some campuses have also combined TAT and CIRT/EMT functions, and some may opt for three teams – CIRT/ERT (for natural disasters, etc), TAT (for threats) and BIT (for prevention), which may prove to be even more cumbersome. For our purposes, given all the different team names and functions, it may be helpful to distinguish between two needed functions and teams – prevention and response. The question is into which does threat assessment appropriately fall?

[2] One of the reasons that the Gubernatorial and Presidential reports used "Threat Assessment Team" language is because they only knew that term of art – being unfamiliar with higher education and its subtleties.

administrative crisis management.   Each of these rationales is seemingly logical, but is in reality antithetical to the goal of preventing violence.   Here's why…

The Threat Assessment Function on a College Campus

Threat assessment in an airport, shopping mall or stadium is usually threat-parallel, meaning that a threat becomes known, and we assess and react to it. Occasionally, we get a heads-up, such as a bomb threat or note that tells us a threat is coming, rather than that it is already upon us. But, for the most part this type of threat assessment involves processing present information to assess a risk.   Behavioral experts may be pulled in to address threats against individuals, such as political figures, if those threats are made in advance, but the history, character, and patterns of the threatener are usually unknown, especially when the source of the threat is unidentified. More history about the source of the threat may come into play in such situations, but it is still rare.

On a college campus, sometimes our threats are like those in a shopping mall -- originating from outside. Mostly, though, campus threats come from within the campus community. Thus, threat assessment on a college campus is by definition a different animal. We are much more likely to know the source of a threat, and we are much more likely to have access to the threatener's history, patterns, background and other salient and recent behavioral characteristics. Thus, the campus threat assessment function must be redefined by the quality of data that we are able to obtain about an at-risk student or staff member. We have conduct records, employment files, criminal background checks, witness reports, room searches, car searches, medical and counseling records and more. They're available for us to work with, and that is a game changer. It allows us to redefine threat assessment not as the crude reactive process it so often is elsewhere, but in its almost ideal form, as a refined, informed, proactive, preventive mechanism. We can literally get out ahead of much of the violence that occurs on college campuses if we do this right. Here's how…

We must create and empower a culture of reporting. We must create one centralized resource to which all reports are made. That resource is the BIT or TAT on most campuses, now.   The team investigates reports, culls available data, or even subjects the threatener to psychological assessment to collect better data. *The team establishes the baseline of behaviors for that individual*. We usually never get a baseline in other threat assessment venues. Once we understand the baseline, our culture of reporting and the data it shares can show us deviations from that baseline, can help us detect patterns, and can show us an individual unraveling as his/her downward spiral commences or worsens. We can then deploy our resources to intervene before a crisis level is reached, because we've seen it coming. Higher education is still developing the skill set for effectively defusing potential violence, because most threat assessment approaches are based on a crisis, and engaging law enforcement. The campus skill set for defusing is different, because we are able to engage pre-threat, and without being bound to the legal standards of probable cause or reasonable suspicion. But, that is the topic of a future article.

Threat Assessment Teams

If your campus is using a two-team model, you have erected silos where one of our key charges is to tear them down. With two teams, the TAT will only be called in when a threshold of severity is reached. Yet, it will have been the BIT (or whatever you call it) that has the data on the baseline of the individual who is at-risk. The BIT will have been dealing with that individual up and until the crisis, when there is a handoff to the TAT. Now, precious time will be consumed in bringing the TAT up to speed on what the BIT already knows about this individual. And, risk will be assessed not by those who know the individual best, and have been dealing with him/her all along, but by a whole new team without the same depth on history, character, background and the other key aspects that could make all the difference.   To us, that makes no sense, and eviscerates the unique threat assessment advantage of intimate knowledge that college and universities have, as compared to other entities that assess threat.

Can You Make a Two-Team System Work?

Yes. If you have no other choice, there are ways to bridge the information gap. Here are some suggestions, if you must have a TAT and a BIT, or their equivalents.

1. Overlap the membership, such that the TAT is the BIT plus other key members needed in a crisis. In this way, the institutional memory and knowledge about the threatener is preserved across teams. Yet, if the point of two teams was to control the volume of information, combined membership will not be as efficient. We'd rather be effective than efficient, though, if faced with the choice.
2. Give the TAT access to the BIT's database, so that it can get up to speed quickly on a threatener's data points that are known to the BIT.
3. Create a liaison between the BIT and TAT, whose responsibility it is to get the TAT fully briefed on history as quickly as possible, and clearly define how much confidential medical and psychological information about the individual known to the BIT can be shared with the TAT in the event of a crisis or impending crisis.
4. While the handoff may require a threshold of severity, establish a lower threshold where the TAT starts to monitor a BIT case that is rapidly deteriorating or alarmingly concerning. This requires good coordination to avoid stepping on each other's toes, but again this is not our ideal approach, so compromises are inevitable.

What is the Best Practice?

We believe that campuses should combine the teams, such that threat assessment becomes a sub-set or sub-function of the behavioral intervention skill set. You still need a crisis management team, but its role is purely reactive. Threat assessment should be done -- for the most part -- proactively and preventatively within the behavioral intervention function.   If it is done correctly, the crisis management team will have less to do, focusing mostly on the unpredictable and/or external threats, while allowing the BIT to establish baselines, detect the patterns, observe deviations and coordinate interventions accordingly.

What Does a BIT Do?

In our framework, threat assessment is a very important function, but does not become the sole focus. Campuses must build cultures of reporting. They must develop the investigation skill-set of the team. They must develop mechanisms for culling and coordinating data.

In fact, a comprehensive list of the ideal functions of a BIT, in our view, looks like this:

- Centralize reporting
- Triage reports
- Assess threat/risk
- Assess available resources
- Perform or empower interventions
- Coordinate follow-up
- Assess long-term success/outcomes
- Educate the community

What Should We Call Our Team?

We joked above about the TABI CAT, but team naming should be taken seriously. Some team names, like the Student Update and Information Team (SUIT) don't tell you what the purpose of the team is or what it does. Some team names may associate a stigma with the team, such that members of your community might hesitate to report concerning behaviors for fear of an over-reaction or heavy-handed response. Risk Assessment Team (RAT) or Behavioral Assessment Report Team (BART) sound cute, but also somewhat ominous. Worst of all may be TAT/RAT, the Threat/Risk Assessment Team, because of the disconnect this creates with the culture of reporting concept. People will report threatening behavior to a Threat Assessment Team, which they associate (as we have here) with high-level risky behavior. Yet, as we have discussed, key to the success of behavioral intervention is learning about the precursor behaviors and low-level concerning acts that indicate a baseline and/or pattern. Giving your team a name that explains what it does, and encourages a broad range of reporting, will aid in the overall success of your team in protecting your community. We have even come to think of BIT as not ideally named, invoking as it does intervention rather than prevention. Names like SOC, CCT, BCT and CARE connote supportive, engaged resources, and a kinder, gentler set of actions and responses than do names like TAT, RAT or CAT. That is for the better.

<u>Conclusion</u>

Threat assessment in a campus environment can take advantage of the observation of baseline behaviors and patterns, such that deviation from patterns can be marked by the team, and used to identify concerning behaviors before they spiral into harm to self or others. While other models can be effective, they are likely to create impediments to successful communication and prevention. To best accomplish the goal of getting out ahead of violence, there should be one central team (or one for staff, one for students) whose responsibility is behavioral intervention, a subset of which is the skill-set of threat assessment.

Brett A. Sokolow, JD is the managing partner of the National Center for Higher Education Risk Management (www.ncherm.org) and the 2009 President of NaBITA, the National Behavioral Intervention Team Association (www.nabita.org).

W. Scott Lewis, JD is a partner with the National Center for Higher Education Risk Management (www.ncherm.org) and serves as Associate General Counsel to Saint Mary's College in Notre Dame, IN.