Received January 2010
Revised March 2010
Accepted May 2010

A model for assessment and mitigation of threats on the college campus

Eileen Weisenbach Keller and Stephanie Hughes
Northern Kentucky University, Highland Heights, Kentucky, USA, and
Giles Hertz
The University of Tampa, Tampa, Florida, USA

Abstract

Purpose – An increase in the number of disruptive and violent events on college and university campuses instigated this review of the methods used to interrupt the trend, with the goal of identifying a preliminary model for systematic management of such threats. The intent is to instigate research, review and discussion in order to decrease the number and severity of threatening incidents on college campuses.

Design/methodology/approach – Thorough review of plans from primary and secondary education, plans in use in higher education, literature on risk and threat assessment, literature on "whistle blowers", and of violent events on college campuses was used to construct a model.

Findings – It was found that, in terms of managing and reducing threats to people who study, live and work in post-secondary educational institutions, insufficient attention has been given to the unique needs of this setting and therefore efforts to mitigate threats have been insufficient. The investigation resulted in the development of a model of assessment and management of threats on university and college campuses.

Research limitations/implications – College campus threat assessment research is very much in its infancy and will certainly develop over time. This paper is the first step in an effort to develop and ultimately test the plausibility of a model. Future research should be pursued to determinewhether the model holds up under a majority of situations on college campuses. Those involved in threat mitigation in university settings should be queried to determine their agreement with the proposed framework and for assistance in refining it.

Originality/value – This paper presents suggestions for the systematic management of threats and mitigation in university settings.

Keywords Violence, Individual behaviour, Universities, Management techniques

Paper type Conceptual paper

Introduction

There has been a surge of violent events on college campuses in recent years despite efforts to incorporate more aggressive risk mitigation techniques such as background checks, the hiring of additional campus police, and emergency notification tools. While most university administrators will agree that these tools have certainly helped reduce risk at some level, there is a general perception that these tools have done little to reduce the volume of disruptive or potentially alarming behavior being reported to campus administrators. In fact, many campus administrators believe that these incidents are increasing due to a number of complex factors. These factors include the increase in students with significant mental health issues who are now able to attend

Journal of Educational Administration
Vol. 49 No. 1, 2011
pp. 76-94

0957-8234
DOI 10.1108/09578231111102072

college due to increases in pharmacological treatment and therapy, the issue of returning veterans on campuses attempting to reintegrate into society, and the increased pressures resulting from the difficult economic conditions being experienced by students and their families along with the host of everyday pressures normally experienced by this age demographic.

While student-initiated violence represents one end of the continuum, issues involving faculty and staff are equally threatening to the wellbeing of the educational environment. Cases implicating both faculty and staff members at educational institutions ranging from sexual misconduct to murder suggest that the problem of violent or inappropriate behavior is an organization-wide phenomenon going well beyond the student population in both its reach and magnitude.

Despite the proliferation of guns and violence and the publicity surrounding violent events in the USA, the issue of campus violence is not just an "American" matter. For example, in 2007, a 20-year-old student shot and killed nine students at a vocational college in Kauhajok, Finland (PoliceOne.com, 2007), while in 2008, a 22-year-old student at another vocational school in Finland killed ten students before turning the gun on himself (*The Telegraph*, 2008). In both of these assaults, the gunmen had previously posted YouTube videos describing what they intended to do ahead of the actual shootings. More recently, in 2009, a 17-year-old student in Winnedun, Germany killed 16 fellow students and then killed himself after a shootout with police (*Sky News*, 2009). As these accounts demonstrate, crime occurs in a variety of educational environments regardless of geography. The model proposed in this research is about identifying a proactive approach to mitigating this type of risk going forward regardless of location. Initiating the development and discussion of this model of how teams proactively manage risk in their environments is designed to help prevent many of these same tragedies on campuses in the future, whether the institutions are located in the USA or abroad.

What appears to be lacking from this arsenal of tools is a process for both early detection of individuals who engage in behavior that is either potentially alarming or threatening and effective intervention before this behavior becomes a high profile, full-blown crises. While complete analysis of specific accounts is outside the realm of this paper, it is alleged that in all three instances mentioned above, the shooters had provided advance warning of their murderous intent through postings on YouTube and chat rooms. No one who saw those postings took action or tried to warn authorities ahead of time. The inaction may have been motivated by fear of making a mistake about the seriousness of the threat, fear of retaliation if identified as an informant or simply not knowing how to report it or to whom.

On the other hand, in the case of the shootings at Virginia Tech, it is alleged that the shooter, Seung-Hui Cho, had come to the attention of various authorities for different types of disruptive behavior a total of 31 separate times before going on his murderous rampage (Virginia Tech Review Panel, 2007). Recognizing that there is room for schools to become more proactive in their efforts to uncover potentially disruptive or disturbed individuals earlier in the investigative process, university and college administrators have recently begun to implement "threat assessment" or "behavioral intervention teams". These teams are intended to address the gaps in communication and crisis management among administrators that were so readily exposed in the Virginia Tech tragedy. According to the Director for the National Behavioral Intervention

Team Association (NBITA) there are an estimated 1,600 teams now in operation among colleges, schools and workplaces with a majority of them being established in just that past two years (Lipka, 2009).

While school shootings are few and far between, the volume of disruptive, threatening or criminal behavior appears to be on the rise based on the latest Clery Act[1] numbers for 2006. From 2004 to 2006, total Clery Act numbers for all categories reported (including arrests for drug, alcohol and weapon violations) increased approximately 5 percent from 94,066 to 98,811. In the category of murder/non-negligent manslaughter, there were a total of 15 in 2004, 11 in 2005 and eight in 2006.

In an analysis of the number of school shootings at the kindergarten through 12th grade (K-12) level conducted by the FBI and Secret Service, many of the shooters often communicated their intentions to other individuals, most often their peers (Vossekuil *et al.*, 2002). In those situations where school shootings were avoided altogether, the shooter's peers communicated the threats to authorities who then intervened to prevent violence from occurring. These observations led to the recommendation that schools adopt the Secret Service threat assessment model intended to prevent future acts of violence. The Secret Service threat assessment model evolved from the government's efforts to identify potential threats to public officials (Fein and Vossekuil, 1998). In these models, threat assessment involves efforts to identify, assess and manage individuals and groups who may pose threats of targeted violence (Fein *et al.*, 2002). Targeted violence is identified as violent incidents where both the perpetrator and target(s) are identified or identifiable prior to the incident (Borum *et al.*, 1999; Reddy *et al.*, 2001).

The issue of threat assessment, however, is not just a school-based problem. Violence in the workplace has been increasing at even faster rates than their educational counterparts. As legislators moved to adopt legislation addressing workplace safety by increasing occupational health and safety standards and implementing tougher penalties for those engaged in stalking and targeted violence, new threat assessment models developed specifically for organizations began to emerge. Turner and Gelles (2003) suggested that while threat assessment in organizations share many of the same characteristics of the "targeted violence" models adopted for the K-12 school settings, there are some distinct differences. For example a violent act perpetrated in an organizational setting may also involve legal and human resource issues not applicable in the K-12 settings.

While there are elements of the K-12 and workplace models that can be applied to a university or campus threat assessment model, neither model is sufficient as each is predicated on the assumption that all environments are "controlled" to some extent, have centralized reporting, command and control characteristics and the threat is a known entity. These characteristics do not reflect the fluid geographical boundaries, open organizational culture or decentralized operating environment associated with most institutions of higher education. This reality calls for the development of a new model of threat assessment specific to the unique characteristics of the college campus environment.

There are four objectives for this research. First, this research is intended to provide an overview of existing risk and threat assessment literature along with an understanding of existing gaps in the structure, capabilities, technologies, policies and procedures that support these teams as they apply to a university or campus setting.

Second, the literature on "whistle blowers" is reviewed and referenced as many aspects of this research relate directly to the actual implementation issues associated with the proposed model. Third, this research proposes a new comprehensive threat assessment/behavioral intervention model designed to reduce the potential risk posed by the inappropriate, disruptive or violent behavior of individuals in university and campus settings. This new model will identify different channels of information (data sources) and methods of reporting potential threats (data collection), the assessment of the risk of the potential threats (data analysis), the establishment of protocol for interface with legal, law enforcement and mental health professionals and the provision of training content to mitigate identified issues (response) and finally, the analysis of the effectiveness of actions (evaluation of response) taken over time. The fourth and final objective is to instigate deeper discussion and more research on the subject. As the number of violent outbreaks on college campuses continue to accumulate, it is critically important to discuss and determine means of mitigating threats and preserving the campus environment. The review of the literature reveals that too little has been conducted on this specific topic.

Risk assessment research

The techniques used to assess the likelihood of a person committing violence have moved from those that suggest a person's risk for violence is fixed, independent of environmental considerations and dependent solely on an individual's characteristics, to a method that suggests that a person's predisposition to violence or the risk they pose is dependent on circumstances, dynamic in nature and occurring within a range of probability (Borum *et al.*, 1999). The question about the best way to evaluate the range of contributing factors led to debates about whether "clinical" approaches where clinicians using their own clinical judgment are better than "actuarial" techniques, where statistical formulas are used, at determining the likelihood of a person becoming violent.

Statistical or actuarial techniques rely on weighted risk factors combined in an equation to yield a decision about the likelihood of a condition or an outcome (Dawes *et al.*, 1989). According to Reddy *et al.* (2001), the primary criticisms are that they do not yet have a sufficient theoretical base of antecedents and risk factors for targeted violence in schools and not enough data points to empirically test an equation sufficiently.

By comparison, clinical methods rely on interviews and evaluation of a subject, by trained and licensed mental health professionals, that is informed by base rates for violence within the individual's population and by relevant risk factors known to be related to the risk of violent behavior (Reddy *et al.*, 2001; Borum, 2000). The primary criticisms of this approach include the higher probability of the possibility of committing a Type I error, which is assessing the student as not posing a risk when in reality he or she does (Reddy *et al.*, 2001). Finally, the utility of standard psychological tests and instruments have been questioned since there is no known research demonstrating the relationship between the results of these tests and the risk of targeted violence in schools (Borum, 2000). Thus, while both actuarial and clinical techniques have their advocates, each approach is fundamentally flawed in its ability to "predict" the potential of an individual to commit violence at some future point in time.

A third technique, originally developed by the Federal Bureau of Investigation's (FBI's) Behavioral Science Unit, relies on information gathered from a crime scene to generate a series of hypotheses about the characteristics (physical, demographic, personality, etc.) of the person who has most likely committed the crime (Homant and Kennedy, 1998; Reddy *et al.*, 2001). This profile is then used to identify types of individuals who are most likely to become perpetrators and/or to assess the risk posed by someone who has already been identified by displaying some type of disturbing or disruptive behavior (Randozza *et al.*, 2006).

The reality is that none of the prior models actually incorporates contextual information about a situation or person, collected from numerous sources or stakeholders over some period of time that could be utilized before an event escalates into a crisis (Randozza *et al.*, 2006). The key here is to help decision makers make critical judgments about an emerging situation before a crisis erupts. The prior overview highlights the need for an alternate approach, focusing more on proactive measures, to help mitigate the risk of an individual to engage in school-based targeted violence.

Whistleblower research

Because so little research has been conducted in the area of campus threat assessment and mitigation an adjacent body of literature on whistleblowers was analyzed to determine if insights might be transferrable to the university campus situation[2]. Both scenarios require consideration of how the identity of a possible wrongdoer becomes known to authorities. Whistleblower literature may provide some insight into this process. Whistle-blowing is the process of disclosing illegal or illegitimate acts or omissions to parties who can take action to correct the wrongdoing (Near and Miceli, 1985). It has been estimated that upwards of 34 percent of all business or workplace fraud that has been identified was revealed through tips provided by employees or other key informants (Sweeney, 2008). In 2009, the total fraud claims under the *qui tam*, or whistleblower provisions, pursued by the federal government were in excess of $1.9 billion with an estimated $250 million going to whistleblowers (Civil Division, US Department of Justice, 2009). The problem with the original law was the lack of protection afforded individuals who reported acts of fraud to the US government. There were many instances where these individuals were retaliated against because the claims they made often opposed very powerful individuals. In 2002, Sarbanes-Oxley legislation was introduced into law and provided increased protection to corporate whistleblowers of publicly-held companies. Under this law, the tighter protections afforded whistleblowers included the adoption of anonymous reporting mechanisms such as hotlines or web-based systems, a requirement that whistleblowers not be harassed, suspended or demoted because of their reports and increased protection against retaliation by imposing fines or even jail sentences for those guilty of retaliation (Kleckner and Johnson, 2004).

In many of the cases involving school violence the perpetrator's actions have been witnessed or identified by others but often these individuals are afraid to report the activities or feel unsure of how or to whom they should report them (Lamberg, 1998). Fear of retaliation has been offered as a major reason why individuals are hesitant to report the alleged illegal activities of others (Keenan, 1995). History proves this fear to be well-founded; attempts at retaliation were more common when the whistleblower

tried to remain anonymous (Miceli and Near, 1994). As such, creating an efficient process that can ensure an individual's anonymity in the course of reporting on another person's disruptive or criminal actions is crucial to a successful and effective reporting methodology.

Threat assessment models

Threat assessment models today, whether practiced in K-12, university or corporate environments, have their roots in the efforts of the US Secret Service who have long been tasked with the responsibility to prevent attacks on US leaders, most notably the President and leaders of Congress (Fein and Vossekuil, 1999). Threat assessment in these contexts, is more than focusing on overt acts of violence; instead the focus has been on identifying behaviors, actions and statements, in advance of physical confrontations, that cause concern about the safety of specific persons under protection and then managing relevant factors to reduce the likelihood of physical violence, intimidation or emotional distress on those that have been targeted (Turner and Gelles, 2003). The threat assessment model differs from prior methods of violence prediction in two fundamental ways: there is no reliance on profiling as a determinant or predictor of violent behavior and, it does not depend on the presence of verbal or written threats as evidence of risk (Fein and Vossekuil, 1998). The importance of not relying on the existence of a verbal or written threat is critical to note because Secret Service case files suggest that of the 43 individuals who attacked a public figure in the 50 years preceding 1999, not one of them ever communicated a threat directly to the intended target (Fein and Vossekuil, 1999).

Some elements of K-12 or corporate threat assessment models are a necessity for the development of a comprehensive university or college campus threat assessment model. However, when considered in aggregate, the K-12 models fail to specifically address six key areas pertinent to the higher education environment. First, on the front end, each of these models assumes a known or existing threat. In many instances though, the issue may not have fully materialized into a known threat or have been properly communicated to authorities. Thus, there is a failure to acknowledge the importance and difficulty of eliciting/soliciting information before a threat actually materializes. This issue becomes even more difficult in a university/college setting where individuals often are reticent to communicate concerns to authorities because of peer pressure or may be unaware of the seriousness of a particular incident when placed in the larger context of the campus community's welfare.

Second, there is an assumption that all individuals know how and to whom to report issues of concern when confronted with situations that are often discreet, dynamic and difficult to discern. This issue of the lack of a centralized reporting structure results because universities often have three sets of rules and separate command, control and reporting structures as they apply to their different constituencies: faculty, staff and students.

Third, these models assume that individuals tasked with evaluating the information about a perceived threat have the right training and background to properly evaluate and assess the seriousness of the threat. In essence, these models assume everyone operating in a position of authority who receives the information from a source has the proper training to evaluate and assess the threat posed by the behavior. In a college setting, there are often multiple layers of authority such as professors, residence life

directors, campus safety officers, staff management and senior academic authorities. Not all of these individuals have the proper training, if any, to recognize threats and/or deal with crises situations so merely communicating to an 'authority" does not ensure the information is being properly handled.

Fourth, these models were developed primarily for a "controlled campus" environment more likely associated with a K-12 or corporate environment. In these environments, most of the individuals who may potentially present as threats are typically known to authorities ahead of time. The controlled nature of these settings makes intruders more immediately obvious. Individuals who are native to the organization, but pose a threat of disruption or violence, often come to the attention of those in authority and their behavior is often more closely monitored as a result. The centralized nature of most K-12 schools and businesses ensures that information is channeled through a centralized reporting structure thus limiting fragmentation of data as typically occurs in more decentralized environments. By contrast, access to college and university campuses is normally open and accessible to nearly everyone at any time, with the possible exception of dormitories, where access tends to be more restricted. In higher education environments, multiple discreet pieces of information pertaining to one potentially violent individual may be submitted to different authority figures depending upon where on campus the incident occurs. History reveals that a person causing a problem or concern in a dorm setting may be disciplined by a resident advisor, but the incident is never reported outside the residence system. An academic department head dealing with problems related to the same individual might never report the issue up the chain of command. If a central data collection process is not expressly established and utilized, different individuals in authority may receive discreet pieces of information that are never shared. Because of the open and autonomous nature of college campuses there is a dangerous likelihood that a critical, telltale pattern will go unrecognized.

Fifth, these models fail to assess the effectiveness of steps taken to mitigate the threat. There is little utilization of the knowledge gained from the analysis to create proactive prevention programs to limit or mitigate future risk associated with the threats. A large part of this gap may be attributed to how information is currently being collected and analyzed. In the absence of a system to facilitate reporting of threats and the analysis of these threats, there is little measurable learning that can take place outside of anecdotal feedback to ensure that if similar circumstances present in the future, the team knows what and what not to do as the pressure increases. The fluid boundaries, decentralized organizational structure and open organizational culture suggests that the current model of threat assessment really needs a significant amount of adaptation in order to more specifically and effectively fit it to the unique characteristics of university environments.

Finally, these models assume that the teams are comprised of individuals whose primary responsibility is to the threat assessment team itself and all other responsibilities are a secondary consideration. The problem with this model of team composition in a university setting is that the team members have their primary responsibilities (teaching, research or administrative) and then their team responsibilities which are, by nature, secondary. According to current models of threat assessment, when a crisis arises, the team must convene immediately and decide on a course of action. This cannot happen consistently in a university setting because

all team members have to attend to their primary responsibilities first. This raises the issue of whether the current models of threat assessment are fundamentally flawed with respect to their suggestions for the composition of the teams because the structure of the team calls for individuals who cannot possibly meet the mandate of the team on a consistent basis.

Evidence of the need for a campus threat assessment model

On April 16, 2007, Seung-Hui Cho, an undergraduate student at Virginia Tech University, killed 32 students and faculty members before turning the gun on himself. A panel convened in the aftermath of the tragedy concluded that Cho's odd and often threatening behavior was noted by numerous members of the campus community but there was no centralized group in place, with the experience necessary, to connect all of the data that had been previously reported (Virginia Tech Review Panel, 2007). As outlined by the panel's report, Cho had come to the attention of Virginia Tech faculty, administrators, fellow students and outside legal and mental health authorities, a total of 31 separate times. In addition, school and mental health professionals who interacted with him in the years prior to his arrival at Virginia Tech, also knew of his disturbing behavior, including writing an essay about carrying out a Columbine-style attack at his school (Deisinger *et al.*, 2008).

The preceding example underscores the three guiding principals involved in threat assessment as outlined by Fein and Vossekuil (1998). First, targeted violence is often the result of a process of deliberate and discernible behavior and way of thinking. It is therefore not a random event. Often, individuals communicate their ideas to others and the process of planning and thinking about the attack dominates their entire existence (Borum *et al.*, 1999). As early as high school, it has been reported that Cho communicated thoughts about engaging in a "Columbine-style" attack. In addition, Cho often expressed, through his writing and actions, his feelings of being an outcast and his desire to make someone pay for these feelings.

Second, targeted violence stems from "An interaction among the potential attacker, past stressful events, a current situation, and the target" (Borum *et al.*, 1999). Cho often sought out the affection of females, but his odd behavior worked to push him into further social isolation as his advances had little social appropriateness to them and often made the women feel extremely uncomfortable. This may have pushed him further into feelings of despair and outrage and may have been the impetus for the shooting of his first two victims who were a couple in the dormitory where he lived.

The third guiding principle is that the key to investigation and resolution of an incident is to identify the subject's attack-related behaviors. Those who engage in targeted acts of violence engage in discrete behaviors that precede and are linked to their attack, including thinking, planning and logistical preparations (Fein *et al.*, 1995; Borum *et al.*, 1999). Cho's behavior in the months and weeks leading up to the attack highlight the degree of planning he engaged in including the purchase of guns over a several month period, the preparation of a videotape to be distributed after the attack had been carried out and the locking of doors to academic building to prevent individuals from getting out as he began his final assault where he took the lives of 30 students and faculty members.

We suggest a fourth principle be added to the equation; one that can help identify and track a subject's attack-related behavior. What seems fundamentally necessary to

assist threat assessment team members in getting "out in front" of a possible threat is the use of some centralized reporting system to facilitate communication between the campus community and authorities who are responsible for ensuring the safety and security of the campus community. As previously highlighted, Cho's odd, disruptive and, at times, threatening behavior was witnessed by a whole host of individuals on at least 31 separate occasions. However, despite the volume of attention he generated, no single entity had a "comprehensive" view of his disruptive behavior. If the existing care team that was in place had some way to both facilitate centralized reporting across campus and track various reports, it is likely that the pattern and escalation of behavior might have been identified and some coordinated intervention might have occurred.

A new model for threat assessment

The proposed model aggregates the critical components of risk or threat mitigation and crisis management systems and customizes them to fit the highly unique college campus environment. It captures the components necessary for gathering information, identifying and assessing the nature and degree of the threat, a means of alleviating the threat or managing the crisis if it is not averted and a feedback loop that allows the system to be improved and refined as experience grows. Many of these components have been studied individually and in combination, but the critical step of combining them into one effective system is undertaken here. Furthermore, while there have been adaptations to existing threat assessment models to make them more applicable to the higher education environment, outside of a recently published "how to" book for campus threat assessment teams (Deisinger *et al.*, 2008), we have found no evidence that a threat assessment model, customized to the uniquely open and porous college campus, has been defined.

The model we propose for the higher education environment involves five fundamental components: data sources, data collection, data analysis, incident response and incident response evaluation and feedback (see Figure 1). The model begins with the assumption that there can be multiple data sources of potential information including students, administrators, faculty, staff or other university employees, vendor's employees, community members, law enforcement, information supplied through the admissions process, anonymous sources and even, possibly, self-reports submitted by individuals who know of no other way to ask for help. These data sources are intended to provide as many channels of information into the process as possible.

The issue of allowing anonymous reports is probably the single biggest issue that teams have to address before finalizing the protocols used to govern the solicitation of information from possible data sources. There are strong advocates on both sides of the argument. For those who argue for allowing anonymous reports, the belief is that some individuals will not submit a report unless they feel that their identity will be protected, so by providing anonymous reporting capability, the team will likely receive more information rather than less. On the other hand, for those who advocate against anonymous reporting, the feeling is that this may contribute to a greater number of false reports from individuals because their identity will be protected. Prior research suggests that the majority of schools that did allow for anonymous reporting did not report an increase in reports (Hughes *et al.*, 2008).

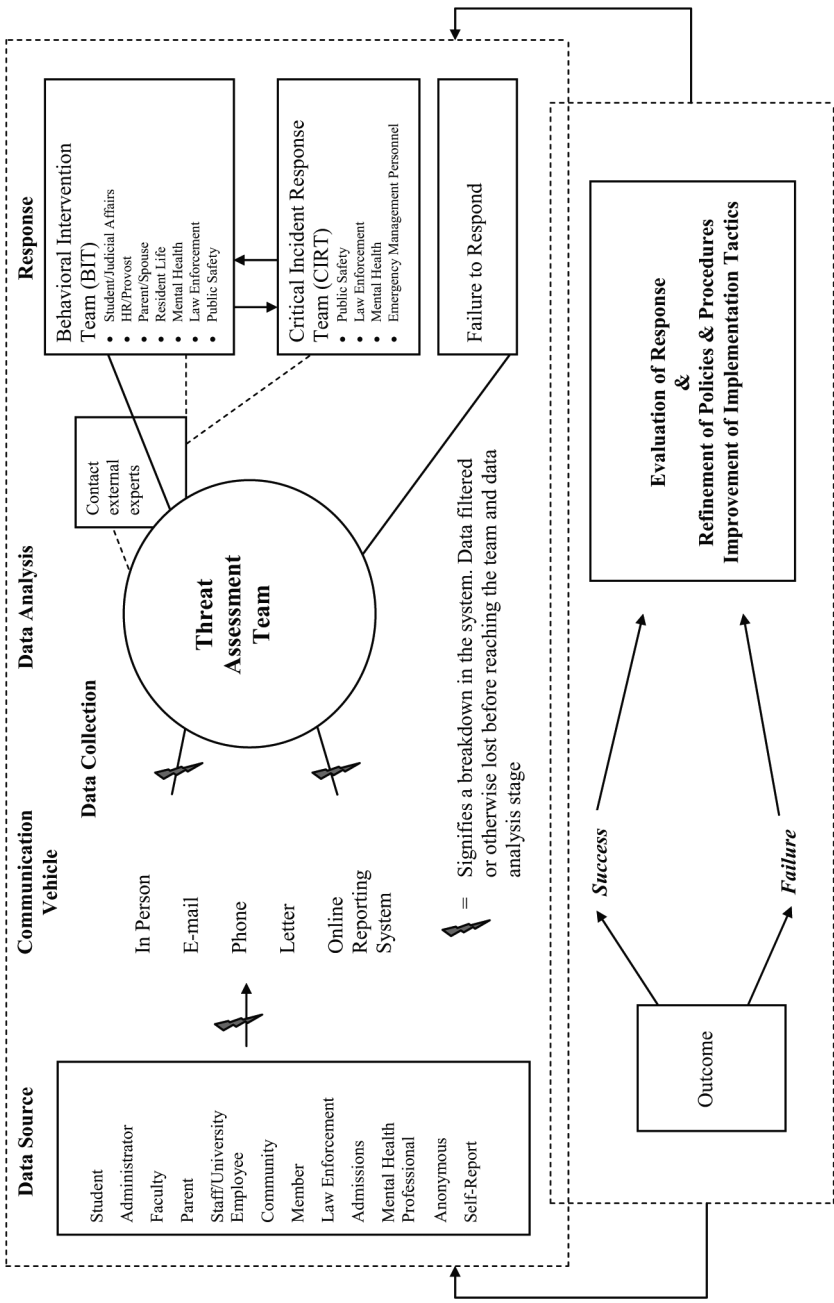

Figure 1.
College campus – threat assessment model

The second biggest issue that teams typically face is how to develop protocol to address myriad federal laws governing the handling of a student's educational records. The Family Educational Rights and Privacy Act of 1974 (FERPA) is a federal law that limits the disclosure of a student's educational records, "a term that the law defines quite broadly and is not limited to academic records"[3]. Thus, "education records" include not only registrar's office records, transcripts, papers, exams and the like, but also non-academic student information database systems, class schedules, financial aid records, financial account records, disability accommodation records and disciplinary records. (Tribbensee and McDonald, 2007).

The Act does contain a number of exceptions that may permit the dissemination of certain educational records to a limited number of persons with "legitimate educational interests." Particularly relevant to this paper is the "health or safety emergency" exception, which may permit disclosure of information concerning disciplinary actions taken against a student for conduct that posed a significant risk to the safety or well being of that student, other students, or other members of the community. Importantly, records maintained by an institution's law enforcement unit are not considered educational records under the Act and thus, may be shared among appropriate university officials, including BIT or CIRT type teams. (Tribbensee and McDonald, 2007).

The dissemination of students' personal information may also be restricted by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) which guarantee the security and privacy of healthcare information. However, it should be noted that the US Department of Health and Human Services and the US Department of Education have recently (November 2008) issued a "joint guidance" or clarification on the application of FERPA and HIPAA to student health records. According to the new guidance HIPAA does not specifically apply to either elementary or secondary schools because neither are "covered entities" under the Act or because the only health records maintained by such schools are "education records" or "treatment records" of eligible students under FERPA, both of which are excluded from coverage under the HIPAA Privacy Rule.

The purpose of the new guidance was to eliminate confusion as to how the two laws (FERPA and HIPAA) apply to student educational and health records. The guidance also clarifies when educational institutions may disclose such information without consent under the health and safety emergency exception; an exception that applies to both of these federal laws. The primary purpose of the agencies' "joint guidance" was to address confusion over privacy rules that were cited during the investigation of the April 2007 shootings at Virginia Tech University.

The model also incorporates multiple channels for submitting information into the threat assessment team to include email, in-person, phone, letter and web-based system submissions. We identify this as the data collection stage of the model. The inclusion of a web-based tool represents an addition to existing models, as these systems are relatively novel and have been used primarily in the past to report issues of financial fraud exclusively (Hughes *et al.*, 2008). Utilizing a web-based vehicle provides a centralized way for information to get to the right individuals in a timely manner. In a university setting the existence of a web-based reporting system, that can be accessed by anyone located anywhere within the system, is a critical need given the decentralized nature of university environments. In many university settings, there

exists a general lack of knowledge about where or whom to go to report issues of concern or instances of disruptive or potentially violent behavior. By providing a web-based tool and communicating the existence of this tool to the university community, administrators will go a long way to ensure that they have more data available to them to make appropriate decisions to ensure the safety of the community. It is important to recognize, however, that school administrators still need to accommodate the submission of reports through non-web-based mechanisms to ensure that as much information is reported about potential concerns or threats as possible. We suggest that schools that are utilizing multiple channels for data submission identify a single person who would be responsible for inputting all other types of reports into the system, regardless of their method of submission. Queries on this subject with administrators at a variety of universities revealed that some schools have begun to do just that and have created a position of "case manager" who reports to the head of the threat assessment team and is responsible for getting all relevant information into the system and making sure that appropriate follow-up is proceeding on all reports logged into the system.

The Behavioral Intervention Team (BIT) must also establish linkages to other outside organizations, such as law enforcement and mental health professionals, to ensure that all possible information is available to the team prior to the analysis and response stage. For example, it may be appropriate to have an outside law enforcement agency run a criminal check on an individual suspected of a possible disruptive incident to know the full details of that person's history. Most campus police forces do not have the resources or possible access to do this on their own. Often these linkages to outside groups are facilitated through informal relationships rather than officially recognized and sanctioned protocol.

The data analysis stage involves evaluation of the reported information and a determination of "next steps" by the threat assessment team. In some higher education settings these teams are commonly referred to as the BIT as the goal is to analyze behaviors and intervene before they lead to disturbances or violence on campus. The composition of the threat assessment team at the university level is going to look significantly different than the composition of these teams at the K-12 or corporate levels. In general, the size of the team is determined by the characteristics of the university, the workload of the team and the resources available to both staff and those who support the team. According to Deisinger *et al.* (2008), "Core team membership should be driven by the communication and working relationships that are necessary to achieve the mission of the team. The institution can decide on the team's initial membership, and then expand or contract as conditions dictate." We argue that the size and composition of such teams at the university level will also have to deal with the fact that team members will often have other responsibilities that have priority over their team responsibilities. This creates the potential for inattention, disruption or the inability of the team to respond as quickly as necessary to a developing or imminent crisis situation.

This scenario raises the possibility that eventually, universities may be forced to install permanent, skilled team members, to include individuals with legal, law enforcement and mental health backgrounds, whose sole responsibility is to the function of the team and nothing else. Under this proposed scenario, the permanent team members are the first point of contact. They then access additional university

"experts" on a "need to know" basis. If the team has been tasked to oversee all reports, including those involving faculty, staff and students then, a university's threat assessment team will require access to a larger number of university experts than if the team were just responsible for student reports. These experts could include some or all of the following departments: Academic Affairs or Provost, Legal Counsel, Psychologist, Campus Law Enforcement, Residence Life, Student Affairs, Media Relations, Office of the President and Graduate Council (Deisinger *et al.*, 2008). The key is to have dedicated, trained personnel who regularly monitor and evaluate information entering through the data collection process to identify troubling patterns or abnormalities and avert problems when possible. This team should be as lean and agile as possible so that when a crisis or situation does develop, the team can convene quickly, make decisions about next steps and implement these decisions as swiftly as possible (Sokolow and Hughes, 2008). It is also possible that a specialized expert or consultant may be accessed at this time to deal with the unique circumstances of some of the cases the team has been tasked to handle.

Often, universities will also employ a second team in addition to the threat assessment team that is intended to deal with high level public relation issues that may arise from incidents being handled by the team or from issues impacting the campus arising from natural disaster. These teams often go by the title of Critical Incident Response Team (CIRT) and involve members of the campus senior management staff and emergency management personnel. The CIRT is more externally focused than the BIT. This team concentrates on alerting and managing external constituents (parents, press, government . . .) while the BIT manages the crisis internally, on campus.

Data analysis should be constant and ongoing. As various sources submit information to the system the data points should be examined for a pattern of violence, escalation of threat or an abhorrent event. If such a configuration is discerned, the team is tasked with gathering additional information on the incident or the person (if already identified). During this part of the data-gathering process, the team should look to as many possible sources of information as possible including, admissions records, employment records, law enforcement records, interviews with roommates or fellow employees, grievance boards, judicial affairs records, legal counsel, residence hall directors (if student lived on-campus), internet postings (i.e. social networking sites) and interviews with the target of the investigation (if known) (Deisinger *et al.*, 2008)[4]. Once this information has been gathered, the team must then set out to answer the following ten questions before making their recommendations about next steps (Fein and Vossekuil, 1998; Borum *et al.*, 1999):

(1) What motivated the subject to make the statements, or to take the action, that caused him/her to come to the attention of the team?

(2) What has the subject communicated to anyone concerning his/her intentions?

(3) Has the subject shown an interest in targeted violence, perpetrators of targeted violence, weapons, extremist groups, or murder?

(4) Has the subject engaged in attack-related behavior including any menacing, harassing, and/or stalking-like behavior?

(5) Does the subject have a history of mental illness involving command hallucinations, delusional ideas, feelings of persecution, etc. with indications that the subject has acted on those beliefs?

(6) How organized is the subject? Is he or she capable of developing and carrying out a plan?

(7) Has the subject experienced a recent loss and or a loss of status and has this led to feelings of desperation or despair?

(8) Corroboration – what is the subject saying and is it consistent with his/her actions?

(9) Is there concern among those that know the subject that he/she might take action based on inappropriate ideas?

(10) What factors in the subject's life and/or environment might increase/decrease the likelihood of the subject attempting to attack a target?

The fourth stage of the model involves incident response. During this stage, the team implements a set of processes or recommendations for handling the incident or the disruptive behavior posed by an individual. A major part of the success of this stage of the model is to ensure that team members have proper training to address the type of incidents they are being asked to deal with as members of the threat assessment team (Deisinger *et al.*, 2008). Once again, the use of outside experts may be required to assist the team in meeting the special needs of an individual involved in an incident. Access to any institutional knowledge about how the university handled similar incidents in the past and the outcomes associated with these actions (see incident response evaluation stage below) is a critical component to the training of this team. It is through this iterative process of engagement and evaluation that both individuals and teams improve on prior performance. As such, it is critical to the success of this model that teams be equipped with technological platforms that can provide the team with proactive tracking and trending capabilities regarding past incidents that involved the same individual or circumstances to ensure that plans or decisions are made with as much available "context" as possible to ensure some measure of success going forward. There is also a possibility that information that gets reported to the threat assessment team never gets acted upon at any level. We hope that this is a rare occurrence but one that must also be acknowledged as a possibility, especially if the volume of reports is such that the team cannot address all of the incidents in a timely manner.

The fifth stage of the model involves incident response evaluation. During this stage, the team looks to evaluate what went right and what failed so that future protocols can be adapted to accommodate the knowledge gained from actions taken, irrespective of their outcome. Where failures or problems occurred the team must examine the issue to determine if the problem was created by the standard, established procedure or if it was an implementation error. If the underlying protocol is determined to be the source of the problem, it must be changed and the change communicated to all involved. If an implementation error occurred, further training may be warranted. The critical point regarding this new stage of the model is that the review of the outcomes and the processes that led to them becomes standard operating procedure. It is the collection and embedding of this institutional knowledge that will strengthen campus systems over time.

Continuing dialogue

As previously indicated, trends and recent events on college and university campuses instigated our analysis of the existing plans, methods and models for mitigation of threats

in schools. The outcome revealed a need for a model carefully fitted to the unique situation presented by the university or college campus environment. The model presented here is comprehensive in its scope, but developmental by nature of its newness.

Because the level of analysis in this work is a process within a university, the model does not address specific psychological issues that create the need for the system. For the same reason, the model does not include strategies for behavioral intervention. These areas are valuable and have been studied within the psychology, sociology and threat assessment literature. Relatively little analysis of the system for identifying and managing perpetrators with these psychologies is published.

Many others have examined the reasons why an individual becomes a perpetrator of campus violence. Although ultimately that is a very important query, it is one best dealt with by psychologists. In contrast, the work discussed here focuses on the planning and strategy associated with identifying and mitigating the threats posed by disruptive individuals in higher education environments.

Implementation challenges for campus administrators

The focus of this research was on proposing a new model for managing threat assessment in a university or campus setting. Determining the framework, or model for a process is a first step which necessitates other equally important ones. Specifically, administrators must consider how best to implement the suggested structure. Although our research team has been unable to locate a university with a functioning threat assessment process as comprehensive as the one suggested here, many implementation hurdles can be anticipated based upon the programs we have studied. Prior models of threat assessment assumed a certain level of training as a precondition for existing threat assessment team members. Preliminary investigation reveals that few campus threat assessment team members have the proper professional training to handle crises and incidents of disruptive or potentially violent behavior that occur on college campuses. Training involving a broad range of areas is needed but initial areas of focus should include legal/mental health topics as they relate to campus environments such as FERPA and HIPAA requirements. Training should indicate the limits of the collective skills of team members and establish protocol for notifying and employing the assistance of external entities with specific expertise.

Additionally, training in the area of proper investigative techniques is also much needed. While individual team members may have this knowledge or these skill sets, the requirements of the team seem to mandate that this knowledge be ubiquitous among team members to ensure that proper procedures are being followed and laws are being adhered to on a consistent basis. Examination of breaches in homeland security in the USA and air travel safety worldwide reveal that isolated signs and symptoms offer needed foretelling of tragic events only when considered in aggregate. Training must include interpretive skills so that seemingly innocuous, solitary signs and symptoms are correctly understood when considered in the *Gestalt* to identify patterns that indicate potential threats.

There also needs to be a focus on providing training to multiple constituent groups in the campus community so that events are reported in a timely fashion and through the proper channels. The campus-wide training has to reinforce the importance of everyone contributing to a safe campus and the requirement that "if something doesn't feel right" then it should be reported. The delicacy of this process cannot be overstated.

As previously discussed, the goal is to encourage the increased safety of all who participate in campus life while maintaining the free and open environment that personifies the pursuit of higher education. The tone and delivery of the training must therefore be carefully considered before implementation is initiated and adjusted to fit each school's unique environment.

The model references the possible need to access external organizations/specialists but does not explain how this process ultimately develops. It is possible that some teams will rely on an informal network of specialists/entities that can be accessed on an "on-demand" basis. It might also be the case that existing team members lack these informal ties and a more formalized relationship may need to be established. To ensure that these important external linkages become embedded and distributed beyond the relationship of a single team member, the BIT/BAT group should emphasize the need to develop formal protocols for how to interface with these groups that supersede any one individual's personal network.

The composition of the threat assessment team also is an area of potential concern and liability to the campus. Currently, teams are composed of members of the campus community who have responsibilities in many other areas. Their service on the team has been requested by the team leader or another individual, but is often the new member's second or third job responsibility, taking a low priority behind other duties. This raises two distinct and troubling possibilities. First, clues that develop into patterns may easily be missed by individuals who have part time and tertiary responsibility for campus safety. Even with specific training the recognition of subtle, emerging patterns may be crowded out by the sheer volume and weight of other, prevailing job responsibilities. Second, when a crisis erupts, not all team members will be available to convene, discuss and move on the issue in a timely manner. This may create a potential liability for the university in the future if qualified team members are unavailable to discuss a situation and then the situation "explodes" before a plan can be executed.

This raises yet another issue regarding the tenure of the threat assessment team when the team relies primarily on part-time team membership. In high volume environments where many incidents are being managed on a daily, weekly or monthly basis, the possibility of team member burnout is quite high. If the tenure on the team suffers because team members resign from the stress, the loss of institutional knowledge becomes a critical management and performance issue as it relates to the team's handling of future crisis incidents. This issue may create the real possibility of the need for permanent threat assessment team members whose sole responsibility is to the team and whose professional background and qualifications are well suited to the needs of the team going forward.

Once these teams are in place, record keeping, evaluation of effectiveness, and corresponding redesign and restructuring must take place. Feedback mechanisms such as this ensure that a measure of institutional knowledge can accumulate and guide future decisions in a way that will likely generate improving results for all parties involved in the process.

Finally, developing ways to assess overall effectiveness of the program is going to be needed in the long run to substantiate the investment of the university's time and resources. Linking the existence of the team to a reduced risk profile for the university will go a long way to reinforcing the utility of these teams and justifying the sometimes

steep personal investment of team members along with the obvious financial investment of the university.

Future research

Future research should include analysis of existing university threat assessment teams, their composition and effectiveness with the goal of identifying a standard team makeup. Also, research should address the merging of the understanding of individuals responsible for campus violence and the system described here for collecting the data about them. Predictive models must be developed that allow collected data points to be sorted and prioritized, based upon past incidents, behaviors and outcomes, so that each team has a baseline of acceptable activity as well as a threshold beyond which behaviors are considered out of the ordinary and threatening to campus safety. Subsequent research should evaluate the effectiveness of suggested changes, once employed, by measuring changes in violent, disruptive and threatening events on campus. Today, most of this measurement is being done on an anecdotal level. The methods suggested here improve the ability to identify, map and assess disparate pieces of data that may ultimately be connected in a way to help administrators anticipate issues created by disruptive individuals and manage these individuals and situations to a less threatening level.

Notes

1. The Jeanne Clery Disclosure of Campus Security Policy and Campus Crime and Statistics Act (20 USC § 1092 (f)) is the landmark federal law, originally known as the Campus Security Act, that requires colleges and universities across the US to disclose information about crime on and around their campuses (Security on Campus, Inc. A national non-profit 501(C)(3)). This disclosure to students and families creates an outlet for marketing the safety and security of a campus or becomes a liability for colleges and universities that have struggled to manage campus security.
2. The authors wish to thank an anonymous reviewer who suggested this avenue of discovery.
3. The information concerning the Family Educational Rights and Privacy Act (FERPA) and Health Insurance Portability and Accountability Act (HIPAA) and their application is provided for general explanation purposes only and should not be considered legal advice. It is highly recommended that any and all questions regarding the specific applications of these laws should be directed to competent legal counsel.
4. It should be noted that the availability of this information may be restricted due to various state and federal privacy laws (e.g. FERPA and HIPAA as previously noted).

References

Borum, R. (2000), "Assessing violence risk among youth", *Journal of Clinical Psychology*, Vol. 56, pp. 1263-88.

Borum, R., Fein, R., Vossekuil, B. and Berglund, J. (1999), "Threat assessment: defining an approach for evaluating risk of targeted violence", *Behavioral Sciences and the Law*, Vol. 17 No. 3, pp. 323-37.

Civil Division, US Department of Justice (2009), "Fraud statistics – overview", available at: www.taf.org/FCAstats-2009.pdf

Dawes, R., Faust, D. and Meehl, P. (1989), "Clinical versus actuarial judgment", *Science*, No. 243, pp. 1668-74.

Deisinger, G., Randazzo, M., O'Neill, D. and Savage, J. (2008), *The Handbook for Campus Threat Assessment and Management Teams*, Applied Risk Management, Stoneham, MA.

Fein, R.A. and Vossekuil, B. (1998), *Protective Intelligence and Threat Assessment Investigations: A Guide for State and Local Law Enforcement Officials*, NIJ/OJP/DOJ Publication No. 170612, US Department of Justice, Washington, DC.

Fein, R.A. and Vossekuil, B. (1999), "Assassination in the United States: an operational study of recent assassins, attackers, and near-lethal approachers", *Journal of Forensic Sciences*, Vol. 44 No. 2, pp. 321-33.

Fein, R.A., Vossekuil, B. and Holden, G.A. (1995), "Threat assessment: an approach to prevent targeted violence", *National Institute of Justice: Research in Action*, September, pp. 1-7.

Fein, R.A., Vossekuil, B., Pollack, W.S., Borum, R., Modzeleski, W. and Reddy, M. (2002), *Threat Assessment in Schools: A Guide to Managing Threatening Situations and Creating Safe School Climates*, US Department of Education, Office of Elementary and Secondary Education, Safe and Drug-Free School Program and US Secret Service, National Threat Assessment Center, Washington, DC.

Homant, R.M. and Kennedy, D. (1998), "Psychological aspects of crime scene profiling: validity research", *Criminal Justice and Behavior*, Vol. 25 No. 3, pp. 319-43.

Hughes, S.F., Hertz, G. and White, R.J. (2008), "A new technique for mitigating risk on college campuses", *Journal of Higher Education Policy and Management*, Vol. 30 No. 3, pp. 309-18.

Keenan, J.P. (1995), "Whistleblowing and the first-level manager: determinants of feeling obliged to blow the whistle", *Journal of Social Behavior and Personality*, Vol. 10 No. 3, pp. 571-84.

Kleckner, P. and Johnson, C. (2004), "Sarbanes-Oxley and whistle-blower protections", *The CPA Journal*, June, p. 14.

Lamberg, L. (1998), "Preventing school violence: no easy answers", *Journal of the American Medical Association*, Vol. 280 No. 5, pp. 404-7.

Lipka, S. (2009), "Threat assessment teams get a professional group", *Chronicle of Higher Education*, Vol. 55 No. 20, pp. A17-A18.

Miceli, M.P. and Near, J. (1994), "Whistleblowing: reaping the benefits", *Academy of Management Executive*, Vol. 8 No. 3, pp. 65-72.

Near, J.P. and Miceli, M.P. (1985), "Organizational dissidence: the case of whistleblowing", *Journal of Business Ethics*, Vol. 4 No. 4, pp. 1-16.

PoliceOne.com (2007), "8 killed in Finland school shooting", available at: www.policeone.com/international/articles/1462419-8-killed-in-Finland-school-shooting/ (accessed December 13, 2009).

Randozza, M., Borum, R., Vossekuil, B., Fein, R., Modzeleski, W. and Pollack, W. (2006), "Threat assessment in schools: empirical support and comparison with other approaches", in Jimerson, S.R. and Furlong, M.J. (Eds), *The Handbook of School Violence and School Safety: From Research to Practice*, Lawrence Erlbaum Associates, Mahwah, NJ.

Reddy, M., Borum, R., Vossekuil, B., Fein, R., Berglund, J. and Modzeleski, W. (2001), "Evaluating risk for targeted violence in schools: comparing risk assessment, threat assessment and other approaches", *Psychology in the Schools*, Vol. 38 No. 2, pp. 157-72.

Sokolow, B. and Hughes, S. (2008), "Risk mitigation through the NCHERM behavior intervention and threat assessment model", white paper, available at: www.ncherm.org/pdfs/2008-whitepaper.pdf

Sweeney, P. (2008), "Hotlines helpful for blowing the whistle", *Financial Executive*, Vol. 24 No. 4, May, pp. 28-31.

(*The*) *Telegraph* (2008), "Finland school shooting: gunman opened fire during exam", September 24, available at: www.telegraph.co.uk/news/worldnews/europe/finland/3073462/Finland-school-shooting-Gunman-opened-fire-during-exam.html (accessed December 13, 2009).

Tribbensee, E. and McDonald, S. (2007), "FERPA and campus safety", *NACUA Notes*, Vol. 5 No. 4, August 6, p. 2.

Turner, J.T. and Gelles, M. (2003), *Threat Assessment: A Risk Management Approach*, Haworth Press, Binghamton, NY.

Sky News (2009), "Teen warned of German school shooting on web", March 12, available at: http://news.sky.com/skynews/Home/World-News/Winnenden-School-Shooting-In-Germany-Tim-Kretschmer-Bragged-On-Internet-And-Was-Under-Care/Article/200903215240061?f=rss (accessed December 13, 2009).

Virginia Tech Review Panel (2007), "Mental health history of Sheung Hui Cho", available at: www.governor.virginia.gov/TempContent/techPanelReport-docs/8%20CHAPTER%20IV%20LIFE%20AND%20MENTAL%20HEALTH20HISTORY%20OF%20CHOpdf.pdf

Vossekuil, B., Fein, R., Reddy, M., Borum, R. and Modzeleski, W. (2002), *The Final Report and Findings of the Safe School Initiative: Implications for the Prevention of School Attacks in the United States*, US Department of Education, Office of Elementary and Secondary Education, Safe and Drug-free Schools Program and US Secret Service, National Threat Assessment Center, Washington, DC.

Further reading

Cornell, D. and Williams, F. (2006), "Student threat assessment as a strategy to reduce school violence", in Jimerson, S.R. and Furlong, M.J. (Eds), *The Handbook of School Violence and School Safety: From Research to Practice*, Lawrence Erlbaum Associates, Mahwah, NJ.

US Department of Education (2006), available at: www.ope.ed.gov/security/Search.asp

US Department of Health and Human Services and the US Department of Education (2008), *Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to Student Health Records*, US Department of Health and Human Services and the US Department of Education, Washington, DC, November.

Corresponding author

Eileen Weisenbach Keller can be contacted at: weisenbace1@nku.edu