Washington and Lee Journal of Civil Rights and Social Justice

Volume 17 | Issue 1 Article 10

9-1-2010

Appropriate Responses of Campus Security Forces

Donald Challis

Follow this and additional works at: http://scholarlycommons.law.wlu.edu/crsj

 Part of the Education Law Commons, and the Juveniles Commons

Recommended Citation

Donald Challis, *Appropriate Responses of Campus Security Forces*, 17 Wash. & Lee J. Civ. Rts. & Soc. Just. 169 (2010).
Available at: http://scholarlycommons.law.wlu.edu/crsj/vol17/iss1/10

This Article is brought to you for free and open access by the Law School Journals at Washington & Lee University School of Law Scholarly Commons. It has been accepted for inclusion in Washington and Lee Journal of Civil Rights and Social Justice by an authorized administrator of Washington & Lee University School of Law Scholarly Commons. For more information, please contact osbornecl@wlu.edu.

Appropriate Responses of Campus Security Forces[†]

Donald Challis[*]

Table of Contents

Introduction

I have been involved in law enforcement on college campuses for over twenty-two years, even serving as a police officer during my own college experience at the University of Iowa. It was during my time at Iowa that I experienced my first campus shooting.

On November 1, 1991, there was an active shooter on Iowa's campus.[1] The shooter killed six people, and I was the first responding officer.[2] Being a first responder is an experience that has stuck with me. Expertise comes from shared experiences and observations. I am not an expert, but I have

---

[†] Transcript of presentation given on Friday, November 6, 2009, at the Violence on Campus Symposium, held by the Washington and Lee Journal of Civil Rights and Social Justice.

[*] Chief of Police, The College of William and Mary; Graduate, 2010, Federal Bureau of Investigation National Academy; M.S. in Criminal Justice, 2001, St. Ambrose University; B.A. in History, 1993, The University of Iowa. I would like to thank Mike Young, Director of Public Safety at Washington and Lee University and Anna Martin, Vice President for Administration at The College of William and Mary, for their support.

1. *See* Steven Lee Myers, *Student Opens Fire at U. of Iowa, Killing 4 Before Shooting Himself*, N.Y. TIMES, Nov. 2, 1991, at 18 (reporting a shooting at the University of Iowa which occurred on November 1, 1991).

2. *See id.* ("A distraught graduate student went on a shooting rampage in two buildings on the University of Iowa campus in Iowa City yesterday, killing four people and critically wounding two others before fatally shooting himself in the head.").

been around long enough to develop some of my own thoughts on the subject.

When I was asked to present today it was to talk about the appropriate response for law enforcement or security. I was having a great deal of difficulty until I realized that I had made a mistake—there is no single, appropriate response to a major incident. Emergency response is discussed as if there is a single course of action, universal to all situations and locations.[3] The environments in which we work are dynamic, as are the potential hazards we face.[4] There is no response suitable for all of these different possibilities.[5] Instead, a framework and procedure should be in place that takes into consideration national standards and the abilities of the responders, yet is sufficiently flexible to address the specific needs of the threat.[6]

The desire to have a universal response creates expectations that are unrealistic and rarely attainable.[7] The best example of unrealistic expectations is the notion of a campus lockdown.[8] Lockdowns are all we hear about as practitioners. While lockdowns may work for a few small campuses, the idea of a campus-wide lockdown has been the default response of nonpractitioners.[9] Yet, in most cases a lockdown cannot be accomplished.[10] Response is a collective and comprehensive approach to

---

3. *See* MARY ELLEN O'TOOLE, THE SCHOOL SHOOTER: A THREAT ASSESSMENT PERSPECTIVE 2 (1999) ("In a knee-jerk reaction, communities may resort to inflexible, one-size-fits-all policies on preventing or reacting to violence.").

4. *See id.* at 5 (explaining that all threats are different and present unique challenges requiring different approaches).

5. *See id.* ("[S]chools must recognize that every threat does not represent the same danger or require the same level of response.").

6. *See id.* (advocating a nationwide, systematic approach to threat assessment so that every school has a comprehensive violence-prevention plan).

7. *See id.* (explaining that because all threats are unique, one approach to violence prevention is not sufficient).

8. *See* JOHN NICOLETTI ET AL., VIOLENCE GOES TO COLLEGE: THE AUTHORITATIVE GUIDE TO PREVENTION AND INTERVENTION 238 (2009) (noting that the Virginia Tech campus did not shut down or initiate a lockdown during the shooting on campus in 2007).

9. *See* John Cloud, *What Can the Schools Do?*, TIME, May 3, 1999, at 6 ("[T]hey [frightened school employees] want lock-downs and detector dogs and strapped rent-a-cops to be a regular feature of school life.").

10. *See* Brett A. Sokolow et al., *College and University Liability for Violent Campus Attacks*, 34 J.C. & U.L. 319, 332 (2008) (questioning the ability of large universities to effectively lock down campuses).

disaster management and is as much about anticipation, prevention, mitigation, and training as it is about the actual, physical response.[11]

In the first Part of this discussion I will broadly examine campus security responses. Then, in the second Part of this discussion I will specifically consider the topic of shooters on campus, suicides, and similar types of threats.

I. A General Framework for Responding to On-Campus Threats

A comprehensive framework for responding to on-campus threats requires us to broaden our concept of response through three different but related activities. First is the anticipation of, and planning for, a variety of potential hazards and incidents.[12] Second is the actual response to the incident.[13] Third is the response to the actions of the responders—in other words, the response to the response. Let us look at each of these activities, individually.

There are two types of potential hazards and threats. Some threats are general, affecting large areas, such as severe weather, pandemics, or infectious disease outbreaks.[14] General threats typically require a campus or community-wide response over a period of time.[15] The other types of threats are more site-specific, such as a fire or an active shooter.[16] Site-specific threats are typically much shorter in duration and have an

---

11. *See* SCOTT NEWGASS & DAVID J. SCHONFELD, CRISIS INTERVENTION HANDBOOK 505 (Albert R. Roberts ed., 3d ed. 2005) (creating a plan to respond to disasters on campus beginning with mental health providers and faculty members anticipating and preventing disasters and then incorporating emergency response teams that respond to the actual occurrence of a disaster).

12. *See* O'TOOLE, *supra* note 3, at 26 (recommending that schools create multidisciplinary teams prepared to deal with various types of threats at various levels).

13. *See id.* at 28 (explaining that response to a threat must meet the level of the threat, involving law enforcement officers as necessary).

14. *See* Eugene L. Zdziarski et al., *The Crisis Matrix*, *in* CAMPUS CRISIS MANAGEMENT: A COMPREHENSIVE GUIDE TO PLANNING, PREVENTION, RESPONSE, AND RECOVERY 35, 39 (Eugene L. Zdziarski ed., 2007) ("[S]ome crisis events have a major impact well beyond the border of the campus. Perhaps the most obvious example is Hurricane Katrina.").

15. *See id.* (explaining that certain types of disasters affect the larger community as well as the campus, so resources must be shared, thus delaying the recovery process).

16. *See id.* at 38 ("A campus emergency is defined as an event that disrupts the orderly operations of the institution.").

identifiable start and end.[17] The management of both types of incidents requires planning.[18]

A. Comprehensive Planning

Disaster planning must be a comprehensive activity, which operates from an all-hazards perspective, looking at all possible threats regardless of their likelihood.[19] What is something that never happens here in this part of the country, or is very unlikely? A plane crashing here in the middle of campus is unlikely, so you would not plan for that.[20] Planning requires looking at the whole range of things that may happen and have happened and working from there.[21] Focusing on an active shooter event is common because of its dramatic impact, even though a college is more likely to experience a fire or a weather incident.[22] Whether or not an emergency is general or specific, there should be an understanding of emergency response protocols, and the protocols should be consistent with national response guidelines.[23]

All response guidelines should follow the National Incident Management System (NIMS)[24] or Instant Command Systems (ICS).[25] All

---

17. *See id.* (expounding that specific emergencies can require the campus to shut down for a defined period of time).

18. *See id.* at 47 ("The institution must give deliberate thought to crisis management planning.").

19. *See* Maureen E. Wilson, *Crisis Training*, *in* CAMPUS CRISIS MANAGEMENT: A COMPREHENSIVE GUIDE TO PLANNING, PREVENTION, RESPONSE, AND RECOVERY 183, 184 (Eugene L. Zdziarski ed., 2007) (explaining that because a crisis cannot always be predicted, it is necessary to plan the most important elements of general responses that can apply to any situation).

20. *See* Zdziarski et al., *supra* note 14, at 48 (noting that it is most effective to evaluate which emergency situations are probable and plan accordingly for the most likely scenarios).

21. *See id.* ("Knowing the types of incidents a campus is likely to experience, such as large-scale events, weather incidents, and the possibility of exterior threats . . . can provide opportunities to avoid serious incidents from happening or at least mitigate their impact.").

22. *See* MELISSA ALLEN HEATH, SCHOOL-BASED CRISIS INTERVENTION 3 (2005) ("Although dramatic events covered by the media such as school shooting, bomb threats, and natural disasters garner the bulk of public attention, providing secondary intervention for a wide variety . . . [of] needs is of paramount importance.").

23. *See* Zdziarski et al., *supra* note 14, at 47 (explaining that a plan for crisis response must be made in advance of the incident and that training should be done to assure that the plan is understood by all staff and resources); *see also*, U.S. DEP'T OF EDUC. OFFICE OF SPECIAL EDUC. & REHAB. SERVS., EARLY WARNING, TIMELY RESPONSE: A GUIDE TO SAFE SCHOOLS 23 (1998) ("The plan must be consistent with federal, state, and local laws.").

24. *See* Anice I. Anderson et al., *Managing in a Dangerous World: The National*

responders and administrators should have a working knowledge of NIMS and ICS protocols.[26] Once this framework and its applications are understood and implemented, the basis for response to all situations is established.[27] Preparing for one specific event, whether it is a fire or something else, means that you are prepared, potentially, to respond to anything, because the structure is in place: who is in charge, who reports where, who is responsible for what.[28]

B. Establishing a Hierarchy of Responsibility

For many years there has been confusion on college campuses about who is in charge during a disaster.[29] I want to clarify: any incident that requires a tactical response by police or fire is under the control of the appropriate fire or police on-scene incident commander.[30] Civilians, regardless of their status at the institution, cannot and should not direct the actions of police or fire personnel.[31] For practitioners, such as myself, this

---

Incident Management System, 16 ENGINEERING MGMT. J. 3, 4 (2004) ("NIMS is the first standardized management approach that unifies Federal, state, and local lines of government for incident response.").

25. *See id.* at 4 ("NIMS establishes ICS as a standard incident management organization with five functional areas—command, operations, planning, logistics, and finance/administration—for management of all major incidents.").

26. *See* Norbert W. Dunkel & Linda J. Stump, *Working with Emergency Agency Personnel and Outside Agencies*, *in* CAMPUS CRISIS MANAGEMENT: A COMPREHENSIVE GUIDE TO PLANNING, PREVENTION, RESPONSE, AND RECOVERY 121, 127 (Eugene L. Zdziarski ed., 2007) (noting that preparedness requires training, education, and knowledge of codes for successful management of an incident).

27. *See id.* at 123 ("It [NIMS and ICS] gives responders an integrated organizational structure that meets the complexity of any incident or multiple incidents.").

28. *See* Zdziarski et al., *supra* note 14, at 48 (noting that during the planning phase it is important to establish who will respond to what and when they will respond).

29. *See* HEATH, *supra* note 22, at 3 (explaining that unless crisis-management plans are previously coordinated and planned, assistance from outside sources can add to confusion); *see also* J. Michael Rollo & Eugene L. Zdziarski, *Developing a Crisis Management Plan*, *in* CAMPUS CRISIS MANAGEMENT: A COMPREHENSIVE GUIDE TO PLANNING, PREVENTION, RESPONSE, AND RECOVERY 73, 74 (Eugene L. Zdziarski ed., 2007) (noting that creating a written plan on how to respond that includes specifics about who is in charge helps lessen confusion during an actual crisis).

30. *See* Grant P. Sherwood & David McKelfresh, *Crisis Management Teams*, *in* CAMPUS CRISIS MANAGEMENT: A COMPREHENSIVE GUIDE TO PLANNING, PREVENTION, RESPONSE, AND RECOVERY 55, 65–66 (Eugene L. Zdziarski ed., 2007) ("[I]n any situation where outside emergency agencies (for example, the police or fire department) are involved, they will secure the situation and take jurisdiction of all activities.").

31. *See id.* at 66 (explaining that once the police or fire department arrives, the crisis

is a no-brainer: we have had to draw a line in the sand saying "this is ours."[32]

There are several reasons for this separation of responsibility. Responders are trained and equipped to address the incident, plan and practice their response, and act in accordance with national standards.[33] Responders understand the concept of the incident command and the tactics necessary to resolve the incident.[34] Second, from a practical standpoint, most incidents that require police response or fire response would be handled long before administrators can be located, assembled, informed, and a judgment made.[35] The fact that civilians do not direct the response or emergency personnel does not mean that they are unimportant to the management of the incident.[36] The civilian role is key to disaster management.[37] The response to the response is comprised of the actions taken by the institution in reaction to actions taken by responders.[38] This is the best way I have found to explain to my administration the separation of authority and duties.

Actions by response personnel are typically short in duration with a definable start and end, whereas the response to the response can last for

---

management team established by the institution must become supportive to the outside emergency agency).

32. *See id.* ("One assumption should be in writing: in any situation where outside emergency agencies (for example, the police or fire department) are involved, they will secure the situation and take jurisdiction of all activities.").

33. *See* Norbert W. Dunkel & Linda J. Stump, *Working with Emergency Agency Personnel and Outside Agencies*, *in* CAMPUS CRISIS MANAGEMENT: A COMPREHENSIVE GUIDE TO PLANNING, PREVENTION, RESPONSE, AND RECOVERY 121, 130–33 (Eugene L. Zdziarski ed., 2007) (noting that preparedness requires training, education, and knowledge of codes for successful management of an incident).

34. *See id.* at 132 (explaining that the police work with a commander or director in charge of the operation, who has worked with the school to create crisis-management plans and is trained to handle crisis situations).

35. *See* Kelly J. Asmussen & John W. Creswell, *Campus Response to a Student Gunman*, 66 J. HIGHER EDUC. 575, 577 (1995) (describing how campus police are the first to arrive at shooting situations and how campus administrations respond to events after police have handled the situation).

36. *See* Sherwood & McKelfresh, *supra* note 30, at 66 (explaining that although police and other emergency agencies must be in charge of handling situations, the institution's administrators should stand for the institution as well as support the police).

37. *See* Sean K. Murphy, *Crisis Management Demystified: Here's How to Prevent a Crisis from Ruining Your Institution's Reputation*, 6 U. BUS. 36, 37 (2003) (noting that, as part of a good crisis-management plan, administrators should address the event to the public, conduct a press conference, and organize the institution).

38. *See id.* (emphasizing that the key to crisis management is fast communication within and by the institution as the crisis is occurring and directly after the crisis).

weeks, days, months, and in some instances years.[39] The response to the response defines the institution's mitigation and public perception of the overall management of the incident. There remain decisions that need to be made during and in the aftermath of the event. These include, but are not limited to:

- What information to give to the public or the media;
- Do you close or reduce the operations of the institution;
- What do you do with the affected members of the community; and
- How to return to normal operations as quickly as possible?[40]

The administration must also decide how to handle information from the first responders.[41] That is the role of the administration.[42] For example, fires, chemical spills, or gas leaks may last for a long period of time, requiring relocation of members of the community.[43] The logistics of this scenario require planning and organization.[44] This is the exact function of the administrators, and usually falls under the umbrella of the institution's emergency-management team.[45] We talked about NIMS and ICS.[46] State

---

39. *See* Cynthia J. Lawson, *Crisis Communication*, *in* CAMPUS CRISIS MANAGEMENT: A COMPREHENSIVE GUIDE TO PLANNING, PREVENTION, RESPONSE, AND RECOVERY 97, 116 (Eugene L. Zdziarski ed., 2007) (noting that in the recovery phase of crisis management long-term action must sometimes be taken).

40. *See* BRENDA PHILLIPS, DISASTER RECOVERY 242 (2009) (explaining that after a disaster, a university must question how much downtime is needed before normal operating conditions can be resumed); *see also* Scott Cowen, *Tulane University: From Recovery to Renewal*, 93 LIBERAL EDUC. 6, 7 (2007) (noting that in the aftermath of Hurricane Katrina, Tulane University had to question how to deal with the displacement of almost the entire city of New Orleans); *see also* Murphy, *supra* note 37, at 7 (stating that institutions must question how and when to deal with the media after a crisis).

41. *See* Rollo & Zdziarski, *supra* note 29, at 88 (noting that the institution, in its crisis-management plan, should decide how to work with first responders and how to communicate information received from first responders to the community and to the rest of the university).

42. *See id.* at 78–79 (explaining that the institution's administration has the responsibility of creating a crisis-management plan and following that plan during a crisis).

43. *See* Cowen, *supra* note 40, at 6 (noting that Hurricane Katrina caused over eighty percent of the population of New Orleans to relocate and that Tulane University's student body was evacuated to Houston, Texas, requiring the University to rebuild over a long period of time).

44. *See* John Lawson, *A Look Back at a Disaster Plan: What Went Wrong—and Right*, 52 CHRON. OF HIGHER EDUC. 20, 21 (2005) (explaining the plan that Tulane University had in place prior to Hurricane Katrina for various hurricane levels, which included a detailed evacuation plan).

45. *See* Rollo & Zdziarski, *supra* note 29, at 73 (explaining that developing a crisis-

institutions are required to follow NIMS and ICS, especially if the institution wants grant funding, or is expecting reimbursement for losses in a disaster.[47] Private schools would also be well served to adopt ICS and NIMS processes in their disaster management plans.

Responding to violence is inherently reactive to the situation, and at best can minimize casualties.[48] The most recent example occurred yesterday at Fort Hood, Texas.[49] Ft. Hood is a very secure place,[50] with a lot of military personnel. The soldiers are talented, armed, trained, and equipped to take-on a small country.[51] That said, I have lost track—thirteen are dead, twenty-nine injured.[52] Then we look at Columbine,[53] and the response before and after.[54] At Columbine, the response was: shots are being fired; law enforcement shows up and waits until they have sufficient

---

management plan is the duty of campus administrators).

46. *See* Anderson et al., *supra* note 24 and accompanying text.

47. *See id.* at 6 ("[F]unding recipients are required to utilize the new National Incident Management System (NIMS) for organizing any critical emergency responses to a terrorist attack, disaster, or other critical response requirement.").

48. *See* ALAN M. LEVITT, DISASTER PLANNING AND RECOVERY: A GUIDE FOR FACILITY PROFESSIONALS 104 (1997) ("In the During Phase, the preplanned, tested, and practiced processes of countering the consequences and affects of the impact are put into use and action so that the number of casualties (both injuries and deaths) will be as few as possible.").

49. *See* Robert D. McFadden, *12 Killed, 31 Wounded in Rampage at Army Post; Officer Is Suspect*, N.Y. TIMES, Nov. 6, 2009, at A1 ("An Army psychiatrist facing deployment to one of America's war zones killed 12 people and wounded 31 others on Thursday in a shooting rampage with two handguns at the sprawling Fort Hood Army post in central Texas."). The shooting at Fort Hood took place on November 5, 2009. *Id.*

50. *See id.* ("Fort Hood . . . is the largest active duty military post in the United States, 340 square miles of training and support facilities and homes, a virtual city for more than 50,000 military personnel.").

51. *See id.* (stating that the Fort Hood base serves as a prime deployment point for conflicts overseas).

52. *See id.* (reporting that thirteen people were killed while thirty were injured, according to U.S. military officials).

53. *See Gun Spree at Columbine High*, N.Y. TIMES, Apr. 21, 1999, at A22 (reporting that two students opened fire on unsuspecting students at the Littleton, Colorado, high school); *see also* Elliot Aronson, *How the Columbine High School Tragedy Could Have Been Prevented*, 60 J. INDIVIDUAL PSYCHOL. 355, 355 (2004) (describing how the Columbine tragedy, which resulted in the loss of a teacher and fourteen students, could have been prevented through interventionist techniques, such as group re-organization).

54. *See* Kenneth S. Trump, *Columbine's 10th Anniversary Finds Lessons Learned: Substantial Strides Have Been Made in School Security, but Glaring Gaps Remain*, DISTRICT ADMIN., Apr. 2009, at 26, 28 (2009) (discussing the overall security lessons learned from the Columbine incident).

numbers—such as SWAT reinforcements—while people are being killed.[55] We have learned from that.[56] The operation orders are now the first person who gets there, if he does not have backup coming soon, locates and eliminates the threat.[57] By sheer force of power or noise, responding officers want to eliminate the threat or apply such pressure that the shooter takes his or her own life.[58] You will see this often with active shooters, at the first sign of pressure they will commit suicide.[59] That has been the response to campuses by law enforcement: Do not wait for backup, because while you are waiting, people are dying.[60] The Virginia Tech response was a very good response by a very good department.[61] But unfortunately, many casualties resulted.[62]

---

55. *See* Dirk Johnson, *As They Mourn, They Are Left to Wonder*, N.Y. TIMES, Apr. 28, 1999, at A24 (questioning whether law-enforcement agencies have effective policies for addressing crises similar to Columbine). The article further remarks that local law officials arrived several hours after the assailants fired their first shots, waiting even longer before entering the building. *Id*. Police officials, however, justified their delay, suggesting that they believed the gunmen were still firing and, thus, did not intend on placing their personnel in danger. *Id.*

56. *See, e.g.*, *MSU Emergency Management Information: Violence Involving Firearms or Other Weapons*, MICH. ST. U. POLICE, http://police.msu.edu/resources/eminfo.pdf (last visited Jan. 26, 2011) [hereinafter *MSU Emergency Management Information*] (describing the implementation of the nationally-recognized "rapid-response" approach when someone is actively using a weapon); *see also* Trump, *supra* note 54, at 28 (outlining several new school security measures adopted post-Columbine, including reducing school access, utilizing surveillance cameras, and enhancing communications).

57. *See MSU Emergency Management Information*, *supra* note 56 (permitting initial responders to destabilize the threat—at least until a tactical team arrives); *see also* Darcia Harris Browman, *Police Adopt "Rapid Response" to Shootings*, EDUC. WK., Apr. 4, 2001, at 1, (reporting on the new "rapid response" approach adopted by local law officials, which requires first responders to address the situation before support arrives).

58. *See* David B. Kopel, *Pretend "Gun-Free School Zones: A Deadly Legal Fiction*, 42 CONN. L. REV. 515, 543–44 (2009) ("An attacker who is under fire will have much less freedom to aim his own shots carefully and kill his intended victims . . . . [A]ctive shooters tend to crumble at the first sign of active resistance."); *see also* Timothy Harper, *Shoot to Kill*, ATLANTIC MONTHLY, Oct. 2000, at 28, 30 ("The contact team is supposed to pursue the gunmen, pressure them to keep moving, and prevent them taking over populated areas."). According to the article, "rapid response" advocates focus on one theme: isolate the shooter and let him decide the outcome. *Id.*

59. *See* Kopel, *supra* note 58, at 542 (quoting a police officer who intimated that active shooters, if pressed, are likely to kill themselves); Harper, *supra* note 58, at 30 (discussing the inherent chaos involved in shooting scenes, which often results in the gunmen committing suicide).

60. *See MSU Emergency Management Information*, *supra* note 56 (adopting "rapid response" approach at Michigan State University campus).

61. *See* Gordon K. Davies, *Connecting the Dots: Lessons Learned from the Virginia Tech Shootings*, CHANGE, Jan.–Feb. 2008, at 8, 13 (noting that the response of police and

C. Identifying Threats

There has to be more to keeping our communities safe than the ability to respond with force when needed. While this is important, there may be no more important goal than having a process to identify those who have potential for harm to self or others.[63] This returns us to planning prevention and mitigation activities and responses. Nearly every investigation, and this goes back to my days at Iowa when there were flags there, shows that there was a history or series of flags or warnings indicating the potential for harm to self or others. These behaviors clearly indicate an ongoing and progressing threat. In most cases, people saw these flags but did not share the information. There are a couple of reasons for this. One, they did not recognize the flags and signals. Two they did not want to get involved. Or three because there was no formal mechanism to share the information. In most instances when there has been a mechanism to identify and manage such cases, it has been an informal process. While beneficial, these practices are not widespread and often contain gaps that make it hard to do full and complete assessments. Or, if an assessment was undertaken that called for after-care management, the ongoing care or monitoring fell short. Tragic events on campuses have required colleges to formalize their processes, and I think most schools now either have or are developing threat-assessment teams.

II. Responding to Potential Threats Posed by At-Risk Students

We must focus on three major areas: recognizing threats, reporting concerns or complaints, and managing the person who is identified. There is a lot of concern amongst faculty about privacy issues. So if we are going to market this threat-assessment plan—and you have to—this process should be viewed as something that is done *for* someone, not *to* someone. Threat assessment is not a punitive but rather a restorative process, designed to identify concerning behaviors so that appropriate actions can be

---

other emergency-rescue squads was "generally excellent" at Virginia Tech during the 2007 shooting).

62. *See id.* at 9 (reporting that Seung-Hui Cho, the Virginia Tech assailant, killed thirty-two people and himself).

63. *See* William N. Bender et al., *Invisible Kids: Preventing School Violence by Identifying Kids in Trouble*, 37 INTERVENTION SCH. & CLINIC 105, 106–07 (2001) (acknowledging that the foremost question in preventing school shootings turns on whether troubled students can be identified).

undertaken. It should be marketed as a community-wide effort to ensure the safety of the community, as the process is dependent on the involvement of all segments of the institution.[64] The threat-assessment team will identify persons at risk through their own information or from concerns and complaints from the community.[65] Based upon their investigation, the team will make a determination regarding the level of threat posed and the proper management of the individual.[66] Low-order behaviors will be identified so that they can be addressed by campus and community resources.[67] For those individuals who present a higher level of concern, the team will develop a management plan to lessen the potential harm to self or others.[68] Communication, external and internal, is essential to the success of the threat-assessment team.[69] This allows the team to make an accurate assessment.[70] The information becomes cumulative: if institutional personnel—including representatives from student health, student affairs, residence life, human resources, and faculty—have a high level or bar that must be cleared before they inform the threat-assessment team, many concerning behaviors may go undetected.[71] The behavior takes place in isolation and is unactionable. When independent concerns are

64. *See id.* at 14–15 (arguing that successful discourse among community officials, including university and public-service personnel, effectively diminishes the likelihood of these tragedies).

65. *See id.* (proposing that "threat-assessment teams" are integral to preventing critical incidents akin to the Virginia Tech shooting).

66. *See* FED. BUREAU OF INVESTIGATION, THE SCHOOL SHOOTER: A THREAT ASSESSMENT PERSPECTIVE 27–30 (2000) [hereinafter THREAT ASSESSMENT], *available at* http://www.fbi.gov/stats-services/publications/school-shooter (setting forth guidelines on how to approach various threats, ranging from low to high, and subsequently determining how to address different threat levels). Following the National Center for the Analysis of Violent Crime's (NCAVC) symposium on school shootings, the FBI published a report that recommends the adoption of the threat assessment approach for academic institutions. *Id.* at 1–2. The threat assessment approach is two-fold: First, identify possible offenders. *Id.* at 3. And second, intervene, so as to avoid potential violent conflicts. *Id.* at 3.

67. *See id.* at 27–28 (suggesting that the threat-assessment coordinator should handle low-level threats through interviews and other measures. if necessary).

68. *See id.* (suggesting that, in the case of high-level threats, schools should contact local law enforcement and enact pre-designated response plans to address the immediacy of the situation).

69. *See* Davies, *supra* note 61, at 14 ("Institutions need to break through current barriers to communication to ensure that information about potential threats is shared by everyone who needs to know.").

70. *See id.* (suggesting that effective communication among community officials helps disable potential threats).

71. *See id.* (reaffirming the proposition that the academic personnel need to communicate amongst themselves to identify and stabilize such threats).

shared the cumulative information may elevate the risk such that the risk is actionable That is the essence of a threat assessment team: you can take these things that are not otherwise on anybody's radar and now take action on them.[72] Past efforts to communicate have been hampered by misinterpretation of privacy laws.[73] A more correct interpretation of existing privacy laws allows for the sharing of information.[74] The safety needs of the community nearly always trump the privacy rights of the individual.[75]

This next part of this threat-assessment plan is about marketing and getting people comfortable with the process. It is important that the team understand that all concerns and complaints that come to its attention must be taken seriously, and that, at times, members of the community may come under the consideration of the team when little or no potential exists for further case management.[76] With this understanding, the team is aware of its responsibility regarding the sensitivity and security of confidential information gathered during the assessment, and it has established policies and procedures for the assimilation, dissemination, and destruction of records or other information when no reasonable threat has been determined.[77]

---

72. *See id.* (noting that threat-assessment teams overcome the inherent problem of "communicating on different frequencies" when threats are realized).

73. *See* Matthew Alex Ward, *Reexamining Student Privacy Laws in Response to the Virginia Tech* Tragedy, 11 J. HEALTH CARE L. & POL'Y 407, 412 ("Communication breakdowns at various stages prevented Virginia Tech educators from developing the full picture of Cho's unhealthy behavior."). This communication breakdown was further exasperated because Virginia Tech officials failed to understand the full picture of FERPA. *Id*. at 434.

74. *See id.* at 417–18 (suggesting that Virginia Tech personnel failed to take advantage of the "safety and health emergency" exception under FERPA, thereby permitting disclosure).

75. *See* Davies, *supra* note 61, at 15 (implying that privacy issues, such as those relating to health records, should be secondary to ensuring the overall safety of the community). *But cf.* Ward, *supra* note 73, at 434–35 (suggesting a better approach: amending, and therefore balancing, the requirements of FERPA with safety interests of the community).

76. *See* THREAT ASSESSMENT, *supra* note 66, at 27 (noting that low-level threats may require only interviews with the person-at-issue and nothing more, depending on school policy).

77. *See* Dewey Cornell, *Threat Assessment in College Settings*, CHANGE, Jan.–Feb. 2010, at 8, 13 (maintaining that effective threat assessment approaches require "clear policies and procedures that establish the team's authority and scope of action"). In campus settings, threat-assessment teams should maintain their own records and treat them with confidence—accessible only to the team. *Id.* at 14.

It is important to identify what behaviors should be reported to the team.[78] The challenge on a campus is separating the academic nuttiness from disruptive, destructive, and dangerous behaviors that can lead to extremely serious incidents.[79] While we work to avert a tragedy, we will find numerous behaviors that are disruptive and destructive, perhaps not to the community, but surely to the individual, and over time, if unchecked, they may lead to further problems.[80] Behaviors that affect the person's ability to develop personally, socially, and academically, left unchecked, may eventually affect the community.[81] The halo effect of the process is the identification of these behaviors.[82] There are many resources on college campuses. The key is to get people in need of service into the funnel.[83] This process may identify actions that are not criminal and may not become criminal, but are holding this person back from being productive, thriving, striving, and moving forward.[84] This is the mechanism that provides access and entry to appropriate resources while problems are small and more manageable.[85]

We do not profile. We look at behavioral changes over time. I wish my friend Mike Young was still in the room. I have known Mike for thirty years, he can be a difficult person, but he is consistently difficult. If Mike became more difficult, or if he became more intense in his "difficult-ness," or if it was more frequent, then I would worry about him. If this was tied to

---

78. *See id.* at 12 (suggesting that these behaviors include erratic behavior and angry outbursts). Once these types of behavior are identified, however, the person must alert the threat-assessment team, thereby triggering an appropriate response within the pre-designed plan. *Id.*

79. *See id.* (requiring the threat-assessment team to evaluate the risk level, once questionable behaviors are reported to the team).

80. *See id.* ("If the institution is able to help people who are upset, angry, depressed, or troubled in some way, many problems can be addressed before they rise to the level of a threat.").

81. *See id.* (citing the Virginia Tech shooting as a prime example of failing to report abnormal social tendencies). For example, many individuals, both students and academic personnel, raised concerns about the Virginia Tech shooter before the incident. *Id.* These concerns, however, were "not routed to one central place where the magnitude and seriousness of his problems could be identified." *Id.* The threat-assessment team addresses this critique. *Id.*

82. *See* Cornell, *supra* note 77, at 12 (noting that the first step in the "threat assessment decision-tree" centers on identifying the threat).

83. *See id.* ("It is essential that all persons in help-providing and supervisory roles in the institution . . . understand that all threats must be passed along to the threat assessment team.").

84. *See supra* note 80 and accompanying text.

85. *Id.*

work productivity or other issues, now I have a concern.[86] So it is not just the behaviors—and that is how we can ferret out some of the academic nuttiness—that have changed, it is the increase in intensity and frequency of the behaviors.[87]

It is important that we are able to report concerns to the threat-assessment team.[88] There have to be numerous access points; you have to market that, it has to be open, it has to protect the person bringing forward his or her fears or concerns.[89] The process has to be understood.[90] Concerns can be brought forward online; there should be many avenues to do that.[91] The threat-assessment team is one of many strategies used to prepare for, respond to, and mitigate threats from a variety of different hazards.[92] As we see, there is no one-size-fits-all.[93] The best that we can do is to develop policies, protocols, and tactics to help us respond, in the truest sense of response, so if something happens we are prepared for it.

In closing, I want to note that in terms of resource allocation, an ounce of prevention is much better than a ton of response. Response is too late; it

---

86. *See* Cornell, *supra* note 77, at 12–13 (differentiating non-threats from threats based on intent and intensity).

87. *See id.* (suggesting that threat-assessment teams should evaluate threats on a continuum, distinguishing low-level threats from high-level threats).

88. *See id.* at 12 ("The team should be notified anytime someone in the college observes or learns about a threat of violence or situation that appears to be threatening.").

89. *See id.* at 14 (placing the onus on the administration to support the team and provide clear policies and procedures for team administration, including mechanisms for communicating potential threats to the team).

90. *See id.* (discussing the importance of educating the entire institution—students, faculty, and staff—on the threat-assessment team's role). Such education includes instructing all institutional members on how to identify threats and subsequently communicate them to the team. *Id.*

91. *Cf.* Nicky Hutson & Helen Cowie, *Setting Up an Email Peer Support Scheme*, 25 PASTORAL CARE EDUC. 12, 13 (2007) (discussing the implementation of an email support system to combat bullying at an all-boys school in England). The young boys communicated via email namely because it permitted them to receive counseling anonymously. *Id.*

92. *See* Del Stover, *Threat Assessment Teams Target School Crisis*, 70 EDUC. DIG. 10, 12 (2005) (discussing that threat-assessment teams are available for analyzing the credibility of threats, while law-enforcement officials remain as the primary contact in bomb scares and other direct dangers).

93. *See, e.g.*, Ken Strong & Dewey Cornell, *Student Threat Assessment in Memphis City Schools: A Descriptive Report*, 34 BEHAV. DISORDERS 42, 44 (discussing Memphis City Schools' adaption of the threat-assessment team approach, which was tailored to fit the schools' needs and resources). In Memphis, the city school system adopted a variation of the traditional threat-assessment team approach by implementing a trial version through a single, centralized facility as opposed to several teams at fixed school sites. *Id.*

is after the fact. We spend a great deal of money and time on planning and training for our response; and we should, but we need to spend more money on prevention and awareness.