

Preventing the next campus shooting.

http://www.entrepreneur.com/tradejournals/article/171142115_1.html

by Harwood, Matt

[Security Management](#) • August, 2007 •

AT 7:15 A.M. ON APRIL 16, Virginia Tech Police received an emergency call alerting them to go to a dorm room in West Ambler Johnston Residence Hall. Once there, officers found two bodies in a fourth floor dorm room; they turned out to be students Ryan Clark and Emily Hilscher, both of whom had been killed by multiple gunshots.

That shooting was labeled "an isolated incident, domestic in nature."

Two hours and 11 minutes later an e-mail was sent by university police to faculty, staff, and students. It said simply that a "shooting incident occurred at West Amber Johnston [Residence Hall] earlier this morning. Police are on scene and are investigating. The university community is urged to be cautious and are asked to contact Virginia Tech Police if you observe anything suspicious or with information on the case."

That was 9:26 a.m. At 9:45 a.m., police received another emergency call to respond to Norris Hall, an engineering building north of the crime scene. Police arrived to find the front doors chained shut. By the time it was over, student Cho Seung-Hui had murdered 30 more people and ended his own life in what became the worst school massacre in U.S. history.

Shootings on U.S. campuses are rare. Among the 2,618 accredited four-year colleges and universities in the United States, there have been only six shooter incidents since 2000. But even that low number is too many. The question now before university and security professionals is: What policies and procedures can reduce the threat of such an incident and how can institutions best prepare to respond if one does occur?

The massacre at Virginia Tech has once again brought campus security under intense scrutiny. Though it is still early to draw specific lessons from how VT handled the incident, it is useful to look generally at policies and procedures in place at other universities as well as at advances in technology that facilitate emergency communications.

Threat Reduction

The most important preventive measure universities can implement is to identify potentially violent students as early as possible by establishing a behavioral threat assessment program, says

Chief Steven Healy, director of public safety for Princeton University, president of the International Association of Campus Law Enforcement Administrators (IACLEA), and a member of ASIS International's Educational Institutions Council.

Institutions should endeavor to implement programs that can assess threatening behavior, but they should be aware of two problems. One, standards do not exist. Two, privacy issues can hinder what can be done with the information, which, perhaps, was a factor in the VT case.

Standards. Unfortunately, there are no national standards governing threat assessment teams or protocols, but both the FBI and the U.S. Secret Service have reports outlining behavioral threat assessment methodologies distilled from previous school shooter incidents. The FBI, for example, suggests that the likelihood of a student carrying out a threat can be evaluated using four prongs: personality traits and behavior, family dynamics, school dynamics and the student's role in those dynamics, and social dynamics. Institutions that wish to establish such programs can look to the findings from both agencies for guidance.

They can also learn from institutions that have already developed programs, such as the University of Maryland.

Maryland developed its behavioral threat assessment program ten years ago after a student threatened to kill a teacher. In the Maryland program, once a threat or threatening behavior comes to the attention of the police, an officer questions the person who made the complaint or witnessed the threatening behavior. The threatening student isn't questioned at this stage, but police will check whether the subject has a criminal history or whether the office had any previous encounters with this person, says Major Cathy Atwell of the University of Maryland's Department of Public Safety.

Special officers trained in behavioral threat assessment techniques will contact relevant university departments, such as resident life and student conduct, for more information on the student.

The information obtained is then entered into a software program, which tabulates risk and helps officers determine whether they should intervene.

Officers also consult the relevant administrators to discuss their options. This becomes an ad hoc behavioral threat assessment team. For instance, if a complaint were generated out of resident life, the police officer would meet with the department director of resident life, the vice president of student affairs, and the director of the residence hall where the complaint started. It all depends on where the case comes from, says Atwell.

[ILLUSTRATION OMITTED]

After consulting, the team decides if a student has broken the code of conduct. If so, the case goes to the campus judicial board, which will take the requisite disciplinary action. It has the power to suspend or expel the student and can even restrict a student's access to particular places, such as a residence hall.

If the student is not in violation of the code, a course of action is laid out. If the team is worried a student is suffering psychologically, they may have the counseling center call the student in. "We transport at least ten, sometimes 20, students a semester for emergency evaluation," says Atwell.

Most of the time, students get a warning, either by the police or a relevant university administrator, such as the dean. Atwell described a few examples where the person that was threatened, or felt threatened, was allowed to confront the threatening student as a police officer stood by.

The university also has a Behavioral Evaluation and Threat Assessment Resource Group (BETA) team at the university level that meets monthly, but it can convene when needed to discuss both individual cases and big picture trends.

Established in 2005, the team is composed of five members representing the counseling center, the mental health service, the office of student conduct, and the head of the police's behavioral threat assessment team. It provides a forum for information sharing and makes recommendations to those who bring cases or concerns before it.

Its recommendations are not binding, however. It is a consultative body, says Dr. Jonathan Kandell, assistant director of counseling center and chair of the BETA team. It helps provide guidance and best options, but it's up to the official who brings the problem before them to decide what to do next.

The BETA team was created when the university realized that some problem students were sliding through the cracks. The team allows people in the campus community to bring attention to students exhibiting threatening or erratic behavior. It also allows members to discuss problem students and consult with colleagues on whether they have received similar complaints about a particular student. For example, if the team is hearing complaints about a student from the residence halls and student discipline hears that same student is acting out in class while the police have arrested the student for public drunkenness, the team can connect the dots and make a more informed recommendation about next steps.

The BETA team also watches trends. Not surprisingly, the trend since the incident at VT has been a dramatic increase in incident reports of students acting unusually. It's a result of heightened awareness and concern.

Kandell has already given a talk to one of the university's colleges about recognizing and evaluating threats, and he expects the BETA team to support educational activities universitywide that will raise awareness of threatening behavior, while promoting tolerance of other's idiosyncrasies to avoid excessive reporting.

Behavioral assessments are also discussed at freshman orientation, where undergraduate advisors act out skits that incorporate safety and security issues. "Virginia Tech is going to change how we all talk about things," says Gerry Strumpf, director of the orientation department and an orientation course instructor.

In addition to the basic en masse orientation, the university offers freshmen additional orientation courses, which students take in small groups of about 20. Strumpf says that this not only gives time to impart more information, but it also gives the instructors a chance to get a reading on the incoming students.

The orientation class, she believes, provides a great place to identify troubled students. "You know you pick up on troubled students. I have walked many a student down to psychological services, and I'm not the only one doing it."

Faculty members and teacher's assistants who run the orientation course are getting additional training in the wake of the Virginia Tech incident to help them spot troubled students and instruct them on what to do to assist their classmates.

Awareness on the part of students can be a powerful tool. Often shooters tell someone their plans ahead of time, "even if only 20 minutes before," says Charles Burdick, a security consultant at iXP who was incident commander at Columbine High School in Littleton, Colorado, at the time of the 1999 shooting.

For example, tragedy was averted at a high school in upstate New York in 2001 when students tipped off teachers that senior Jeremy Getman was carrying weapons. When Getman was searched, police found an arsenal in his gym bag consisting of "14 pipe bombs, three smaller bombs, a propane tank, a sawed-off shotgun, a .22-caliber pistol, and a book bag full of ammunition." Getman had threatened a girl earlier that day.

Privacy. As the Virginia Tech incident shows, even when a student is identified as a threat, privacy laws erect legal barriers to accessing and sharing personal information that can be pivotal in making the correct behavioral threat assessment. During a congressional hearing a week after the Virginia Tech massacre, witnesses discussed two laws that preclude notification of disturbed behavior to relevant parties.

The Federal Educational Rights and Privacy Act of 1974 (FERPA) protects student records from the prying eyes of parents. The only time the university can allow parents to access student records is "in connection with an emergency ... if the knowledge of such information is necessary to protect the health or safety of the student or other persons."

Colleges and universities complain that FERPA doesn't explain what constitutes an emergency adequately enough, so they play it safe to avoid liability. Moreover, any divulgence of a student's mental health information by a university counseling center violates mental health ethics and licensing codes.

Another piece of legislation protects students' privacy as well. The Health Insurance Portability and Accountability Act (HIPAA) prevents mental health facilities from sharing patient information with the educational institution a patient attends. Regardless of whether a mental institution deems a student a threat, it can't provide that information to the university. HIPAA also bans sharing mental health data with parents unless the student signs a waiver.

Dr. Russ Federman, director of counseling and psychological services at the University of Virginia, testified that "conflicts between FERPA, HIPAA, and mental health licensing codes need to be lessened." The Report to the President on Issues Raised by the Virginia Tech Tragedy has since weighed in, noting "there is significant misunderstanding about the scope and application of these laws."

And Pennsylvania Congressman Tim Murphy (R-PA) has sponsored legislation to clarify FERPA and make it easier for schools and universities to notify parents if their child is suicidal or has shown homicidal tendencies.

Response Capabilities

Because prevention can never be 100 percent, campuses must also be prepared to respond to an incident. Though at this writing the formal reviews of the Virginia Tech incident have yet to be concluded, the tragedy will likely be remembered for highlighting two critical response issues:

- * The importance of campus security and police readiness to respond to active shooter situations
- * The value of coordination and cooperation for first responders at the campus level.

It also appears to be sparking a revolution in public safety technology at U.S. colleges and universities.

Active-shooter. Before the 1999 Columbine High School massacre, the response to a gunman on campus was similar to that of a plane hijacking. Authorities would surround the building, deny access or exit, and then try to negotiate an end to the situation. Everything changed once Eric Harris and Dylan Klebold made their high school a killing zone before shooting themselves.

In 1999, Burdick was not prepared for Harris and Klebold's behavior at Columbine. He likened them, and now Cho, to suicide bombers. "What we're dealing with is a very strange mentality that is so difficult for the normal person to comprehend."

This realization triggered a reevaluation. Standard operating procedure for active-shooter situations is now for officers on the scene to make entry as soon as possible and try to neutralize the threat.

In an active-shooter situation, officers are trained to respond to gunfire, bypassing everything else, even the wounded, to get to the shooter and stop him before he kills another person, says John Gnagey, executive director of the National Tactical Officers Association.

An active shooter response ideally takes four officers to enter a building so as to have a 360-degree circle protecting all sides. The decision of when to enter is situational and dependent on intelligence.

But the Virginia Tech massacre--in which more than two hours passed between incidents--revealed a problem: How do you know whether a potential active shooter is still loose unless

gunshots are heard? Should the discovery of even a single person shot dead on campus be treated as an active-shooter situation that could cascade into a larger incident?

Cho had taken a two-and-a-half hour break to mail his multimedia manifesto before resuming his rampage at Norris Hall. The police officers investigating the Virginia Tech case, as noted earlier, treated the first two bodies as "an isolated incident, domestic in nature."

If that was standard operating procedure at the time, should it be going forward? The university and college community is grappling with that issue now and examining options for alternative responses to single shootings where the shooter remains at large.

Coordination. The most important part of any response happens before the incident even begins. It's what Burdick calls governance or "defining and documenting relationships between responders before an incident occurs." As Columbine made clear--and what 9-11, Hurricane Katrina, and Virginia Tech have reinforced--an emergency event may need a large emergency response.

"We used to be able to handle most incidents with local neighbors--one or two communities away--and suddenly we're getting into these larger responses and units are coming in from hundreds of miles away," he says.

To ensure a seamless integration of all responders within a clear chain of command during such events, all universities should integrate into the National Incident Management System (NIMS) and adhere to the Incident Command System (ICS) within it.

NIMS ICS is the federal government's emergency response framework. It ensures that all responding agencies, from the local level up, can work together and communicate in a domestic crisis. Whether it is a tornado, a terrorist attack, or an active shooter on campus, NIMS ICS is a standardized, framework for ensuring interoperability between responders so that they can deal with anything.

As a part of NIMS ICS, campuses should execute memorandums of understanding (MOU), which are cooperative agreements for mutual help, with other agencies from the local to the federal level. These agreements outline the roles and responsibilities of each responding agency in an emergency.

For instance, some campuses are patrolled by contract security officers, while others are protected by sworn or non-sworn police officers or both. At some campuses, police officers carry guns; at others, they don't. Some campuses are philosophically opposed to having an armed police presence, says John Matthews, executive director of the Community Safety Institute. Nationwide, only 20 universities have SWAT teams, according to Gnagey.

The VT incident, which shows the need for a quick response, may lead to a reevaluation of that approach as well. Meanwhile, if an active shooter situation arises at a campus with contract security or unarmed police officers, that campus will want MOUs with local police and other

jurisdictions to ensure that they can get immediate assistance from personnel with the firepower they lack.

Daniel Pascale, commander of security operations at Rutgers University, says smaller institutions like community colleges can also use MOUs to work out arrangements for temporary housing of students off campus. Through a MOU, "A small community college that has 750 to 1,500 students may actually be able to relocate their students to another facility that's in close proximity, but unaffected by an emergency."

NIMS ICS is also valuable because it establishes a unified command system rather than a single command system. That means that if an incident occurs on campus, a representative from the university will have input into all decisions made by the unified command. With this team approach, campus security remains a part of the decision making process. Before, the local police department or another jurisdiction could swoop in and take complete control of the incident, says Bernard Gollotti, senior associate vice president of public safety at Drexel University and vice chairman of ASIS International's Council on Educational Institutions.

After the institution has developed its plans and worked out MOUs with appropriate parties, it should test how everything and everyone will work together. A tabletop exercise is a good option for testing the plan. This dry run helps responders rehearse what is expected of them.

As a part of the practice, the institution and its MOU partners can ensure that everyone will be using the same terminology, speaking a common language to avoid confusion in an actual incident. The interoperability of equipment should also be tested.

Technology

In responding to an emergency at a university, the exchange of information among responders is critical, as is the ability to notify students, faculty, and staff of an imminent danger regardless of where they may be at the time. Technological advances in communications are making both types of responses much more feasible than in the past.

At Drexel University in Philadelphia, Pennsylvania, Gollotti's campus security team has been beta testing a new PDA-like device, produced in collaboration with Drakontas--a company composed of former Drexel researchers. Gollotti described the communications system as the technology of the popular counterterrorist show "24" made real.

The device is for use by the security team; it allows team members to track each other using GPS; they could also exchange text messages, photos, videos, and floor plans between handheld devices, enhancing the team's ability to maintain situational awareness. The most innovative element would be the ability to use white board video technology, the same used by sportscasters to write on-screen during game telecasts.

The tactical implications of this technology are endless. Gollotti explains: "So if you're going to breach a door on the north side [of a building], you can draw that out on the handheld and send it to everyone else. And if we want to concentrate on another particular area [of a building], you

can send a photo or a line drawing or a floor plan and say these are the areas you need to look at."

He says Drexel and Drakontas are working on technology that speaks directly to Columbine and Virginia Tech. By strategically placing cameras inside a building at critical surveillance locations viewable by remote monitors and directly on a handheld device, campus security could gather intelligence and make an informed decision about what strategy would be best for the situation.

That type of intelligence, if it had been in place at Virginia Tech, might have alerted police to the fact that the doors were chained, and it would have helped them to see where exactly Cho was--a significant advantage when planning tactical deployment.

Johns Hopkins University in Baltimore already employs a smart CCTV system to monitor the campus; computer software conducts behavioral recognition scans that can identify 20 different characteristics, such as whether someone left a suspicious package behind. Any such events cause an alarm to alert security.

Mass notification. Virginia Tech has spurred a flurry of interest in mass notification systems that would help institutions get out the word about an imminent threat. Most attention has been paid specifically to short message service (SMS) text messaging capabilities via cell phones because of the ubiquity of those devices. "[T]here's one statistic that says 90 percent of all college students now have cell phones," says Pascale.

Interestingly enough, some campuses already had SMS text messaging capability, but students hadn't opted in because they didn't feel the need or because they were unaware that the program existed.

But that was before Virginia Tech. Now, campuses are adapting fast to the voracious demand from students and parents for text messaging services.

Drexel University has expanded its mobile communications system to include SMS text messaging and is now doing a "big push" to let students know it's available, says Gollotti.

Drexel and Drakontas are also working on two-way text messaging between their dispatch command center and students. This would allow a student caught in a dangerous situation to text message campus security without a sound. "In light of the Virginia Tech incident, we believe that two-way text messaging could provide vital information related to student safety during a crisis," says Gollotti.

Many other campuses are looking at outside solutions.

Services such as e2Campus and Connect-ED provide a Web-based, fully hosted system that allows students, faculty, and staff to provide multiple points of contacts using in either voice or text message form. The system uses landlines, cellular phones, e-mail, PDAs, RSS, or TTY/TTD.

These vendors maintain the contact information in their database and use multiple servers across the nation to push out the information to ensure that a designated administrator can send thousands of messages and have them received in minutes regardless of whether certain servers are down in the area. (See sidebar, page 56, for the six characteristics of a highly effective mass notification system.)

In situations such as Virginia Tech where the assailant is in a certain place, these systems can also send targeted messages to individuals in a particular location to warn of danger.

Other solutions include public alert systems that use sirens or recorded voice messages to alert the campus community. At the University of Iowa, sirens were installed to warn students of tornadoes.

Some colleges face additional communication challenges, but technology is helping there as well. For example, Gallaudet University, in Washington, D.C., is the preeminent college for deaf and hearing-impaired students in the nation. The university needed alternatives to the traditional voice messages and audible alerts.

Gallaudet uses text messaging services, e-mails, and regular Web updates. But it has also purchased 30 rolling electronic signs that will be placed strategically throughout the campus to warn students of emergencies.

Perspective

Tragedies such as Virginia Tech elicit increased public attention to campus safety and security, but it's important to step back and make sure that any policy and procedural changes are well-thought-out.

For example, because Cho chained the doors to Norris Hall shut, Gollotti now expects campuses to look into and develop policies and procedures regarding alternative points of entry to buildings in case major access points are denied. That's not a bad idea, according to Gollotti, but it's also important to look more holistically. Security changes should not only be made piecemeal in reaction to each new event.

And for all the talk of what campuses can do to provide for the safety and security of their students in emergencies, it's important for students to realize that staying safe is mostly in their own hands.

Murders on campus are rare, averaging 16 per year, according to the Department of Education. Students are much more likely to die from alcohol-related injuries than at the hands of a fellow student.

Matt Harwood is a staff editor at Security Management.

RELATED ARTICLE: [Six Tips for Evaluating Mass Notification Systems](#)

Institutions that plan to buy new systems that would make it easier to notify students, faculty, and staff of a threat or emergency situation should consider these six tips, provided by Chief Steven Healy, director of public safety for Princeton University and President of the International Association of Campus Law Enforcement Administrators.

1. Capacity. The vendor you choose must have the demonstrated capacity to send out thousands of messages, voice or text or both quickly.
2. Security. Students, faculty, and staff are entrusting the university with their personal contact information; therefore, the vendor must have policies and procedures to ensure data security.
3. Customer Service. Is customer service 24/7, 7 days a week, 356 days a year? If not, don't bother.
4. Experience. What type of experience and track record does the company have sending messages or providing mass notification to customers? How long has it been in the market? Talk with other directors of campus security and see which company they've contracted with and whether they would endorse their current provider.
5. Assessment. This may be the most critical criterion. Can you check which messages reached their destination and which didn't? Does the system make multiple attempts to reach people when the initial attempt fails? Do you get a report back? What is the depth of the reporting function? Can you identify the people not reached so that you can get up-to-date contact information from them?
6. Market specialization. The education market poses unique challenges, such as the need to comply with applicable federal laws and regulations compliant, so stick with those companies proven reliable by other educational institutions.

RELATED ARTICLE: SYNOPSIS

The massacre at Virginia Tech has once again brought campus security under intense scrutiny. Though it is still early to draw specific lessons from how VT handled the incident, it is useful to look generally at policies and procedures in place at other universities that may reduce the threat of such an incident or improve the response if one does occur.

One approach that merits greater consideration is the use of behavioral threat assessment teams, like the one at the University of Maryland, which can help campuses identify students that may pose a threat to themselves or others.

On the response side, training in active shooter responses is expected to get more attention. Colleges and universities are also advised to integrate their own plans into the National Incident Management System and the Incident Command System. Doing so helps to ensure that everyone responding is using the same terminology and coordinating their actions.

Technology also has a role to play. A revolution in public-safety technology is making it easier for security and police to alert the campus community through mass notification systems when there is an emergency or potential danger on campus. These tools are also facilitating first-responder communications.

While these efforts are all important, it also helps to keep the threat of a shooter in perspective. On-campus shootings are extremely rare; students are far more likely to die from drinking too much than at the hands of a fellow student.

COPYRIGHT 2007 American Society for Industrial Security Reproduced with permission of the copyright holder. Further reproduction or distribution is prohibited without permission.

Copyright 2007, Gale Group. All rights reserved. Gale Group is a Thomson Corporation Company.

NOTE: All illustrations and photos have been removed from this article.

Copyright © Entrepreneur.com, Inc. All rights reserved. [Privacy Policy](#)