

The Role of IT in Campus Security and Emergency Management

An EDUCAUSE White Paper

October 2008





EDUCAUSE is a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology. Membership is open to institutions of higher education, corporations serving the higher education information technology market, and other related associations and organizations. Resources include professional development activities; print and electronic publications, including books, monographs, and the magazines *EDUCAUSE Quarterly* and *EDUCAUSE Review*; strategic policy advocacy; teaching and learning initiatives; applied research; special interest collaborative communities; awards for leadership and exemplary practices; and extensive online information services. The current membership comprises more than 2,200 colleges, universities, and educational organizations, including 250 corporations, with 17,000 active members. EDUCAUSE has offices in Boulder, Colorado, and Washington, D.C.; www.educause.edu, e-mail info@educause.edu.

© 2008 EDUCAUSE

This work is licensed under a Creative Commons Attribution-NonCommercial-Share Alike 3.0 License.
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

The Role of IT in Campus Security and Emergency Management

Table of Contents

Abstract.....	3
Contributors	3
Introduction	5
Definitions.....	6
Hallmarks of Effective Emergency Management	8
Challenges	8
Emerging Opportunities.....	9
Emergency Communication Systems	9
Geospatial Mapping Tools	10
GPS Technology	10
Business Continuity Planning Tools.....	10
Learning Management Systems and Virtual Worlds	11
Social Networking Tools	11
Virtual Emergency Operations Centers	12
Intelligent Monitoring.....	12
Data Mining and Database Tracking	12
Information Sharing	12
Action Agenda	13
Conclusions.....	15
Endnotes.....	16
Summit Attendees	17

Abstract

Vulnerabilities on the campuses of our nation's colleges and universities have come into sharp focus in recent years, dominating headlines with what seems like increasing frequency and greater consequence. In August 2008, campus leaders in safety, security, emergency management, and information technology met in Washington, D.C., to put emergency management firmly at the top of the agenda during an EDUCAUSE Summit on "The Role of IT in Campus Security and Emergency Management." Brought together by a common purpose to explore proactive approaches to emergency management and a desire to learn about emerging technologies on the horizon, the group spent two days dissecting the state of emergency management at our nation's colleges and universities and sharing resources from their own institutions. This white paper outlines the results of the initial summit and presents key findings from two days of group brainstorming and collaboration.

Contributors

- ◆ William Badertscher, Georgetown University
- ◆ Mark Bruhn, Indiana University
- ◆ Steven Healy, Princeton University
- ◆ Norma Holland, EDUCAUSE
- ◆ James Hyatt, NACUBO
- ◆ David Lindstrom, The Pennsylvania State University
- ◆ Valerie Lucus, University of California, Davis
- ◆ Rodney Petersen, EDUCAUSE

Special thanks to Carie Page of EDUCAUSE, who served as the primary author of this paper.

Introduction

In the days and weeks that followed the April 16, 2007, shootings at Virginia Tech, the nation's colleges and universities responded with messages of solidarity and grief, pledging to mourn alongside their peers. In athletic stadiums and across university balconies, homemade banners read "Today...We are all Hokies."

In the hallways of the nation's higher education institutions, the slogan had particular significance for emergency managers, campus police, and leaders in information technology. While the national media dissected the campus response in Blacksburg—probing what might or might not have prevented the tragedy—college and university administrators were looking inward, suddenly rethinking their own emergency management plans and reevaluating their procedures for disaster response and recovery. If we are all Hokies, the slogan seemed to suggest that we are all vulnerable. The notion that higher education might be immune to the violence that had previously shaken the country's high school corridors was suddenly irrelevant. Although the threat posed by an active shooter on a college or university campus has refocused the attention of higher education institutions on crisis management, institutional leaders are increasingly aware of the need to develop comprehensive emergency preparedness plans that anticipate and address all hazards—from man-made events to natural disasters.

In a 2008 survey of higher education institutions by the Midwestern Higher Education Compact, a staggering 87 percent of those polled said that their campus had conducted a comprehensive review of their policies, procedures, and institutional planning after the events at Virginia Tech. Nearly 9 out of 10 reported that those internal audits had already resulted in changes to their policies, procedures, or systems on campus.¹

Vulnerabilities on the campuses of our nation's colleges and universities have come into sharp focus in recent years, dominating headlines with what seems like increasing frequency and greater consequence. Storms like Hurricane Katrina have introduced the notion that returning to a physical campus might be an impossibility after a natural disaster, creating new emphasis on planning for long-term recovery and necessitating distance learning. An increased reliance on physical and virtual systems has created new concerns about widespread system failures and cyberterrorism. Words like *pandemic* and *bioterrorism* have entered the emergency manager's lexicon.

The greatest threat, however, may be an increasingly fickle spotlight, one that shines on a specific type of emergency response in the wake of a disaster but quickly shifts in the weeks that follow, pushing the conversation off the campus agenda and to the bottom of the university budget.

In August 2008, campus leaders in safety, security, emergency management, and information technology met in Washington, D.C., to put emergency management firmly at the top of the agenda during an EDUCAUSE summit on "The Role of IT in Campus Security and Emergency Management." Brought together by a common purpose to explore proactive approaches to emergency management and a desire to learn about emerging technologies on the horizon, the group spent two days

dissecting the state of emergency management at our nation's colleges and universities and sharing resources from their own institutions.

One of the pervasive themes was an agreement among attendees that campuses cannot expect to be proactive and innovative if they continue to work within departmental silos. Cross-campus communication and collaboration are critical. Attendees also agreed that the conversation surrounding emergency management cannot begin and end within the few weeks that follow a disaster. It must be part of an ongoing strategy as embodied in a comprehensive emergency-management plan.

In the closing session, the group assembled an Action Agenda rooted in a common desire to increase information sharing between one another and to put emergency management and campus security at the forefront of campus conversations and at the top of the research agenda, even after the national spotlight has dimmed.

This white paper is the first step toward that goal, outlining the results of the initial summit and presenting key findings from two days of group brainstorming and collaboration. The conversation will continue, in part thanks to the National Campus Safety and Security Project, a multi-association initiative launched in February by EDUCAUSE, NACUBO, and several higher education associations that will provide a comprehensive new assessment of the risks common to all institutions and guidance on preparing emergency management plans for prevention, response, and recovery.

Definitions

The International Association of Emergency Managers (IAEM) defines emergency management as “the managerial function charged with creating the framework within which communities reduce vulnerability to hazards and cope with disasters.”² For our nation's colleges and universities, emergency management serves as the first line of defense against man-made disasters, campus violence, domestic terrorism, computer security vulnerabilities, and an ever-increasing spectrum of emerging and existing threats.

Preparing campuses for the full spectrum of possibilities requires what summit participants adopted as an all-hazards approach, considering that campus emergencies may be isolated (a student death or suicide) or endemic (a spreading virus or pandemic). They may attack the physical components of a university, disrupt the network infrastructure, or impact human life. The incidents are both natural disasters and man-made events.

Although the vulnerabilities vary, most campuses accept a four-phased approach to emergency management:

- ◆ **Preparedness:** Mobilizing and preparing the campus response to emergencies, from the development of emergency response plans and the procurement of supplies to educating the campus community about procedures for disaster response
- ◆ **Mitigation and prevention:** Taking steps to reduce or prevent the possibility of disaster on campus, from identifying and assessing risk to putting preventative measures in place to reduce the risk occurrence

- ◆ **Response:** The way that a campus reacts to disaster, including crisis communication and the treatment and protection of key assets, from university students and personnel to critical information systems and university property
- ◆ **Recovery:** The timely resumption of standard operating procedures on campus, moving from “disaster” mode to “normal” mode through treatment, rebuilding, reorganization, and recovery³

Within this four-phased approach, all emergency management, as defined by IAEM, must be:

1. **Comprehensive:** Taking into account the full range of hazards and campus vulnerabilities while preparing a response that encompasses all assets (cyber, human, and physical) and members of the campus community (from students, faculty, and staff to visitors and adjacent neighborhoods)
2. **Progressive:** Anticipating new and emerging threats and securing the campus community against them
3. **Risk-driven:** Rooted in sound principles of risk and impact assessment and identification
4. **Integrated:** Considering all members of the college or university and surrounding communities, from federal response agencies and local law enforcement to campus police and IT
5. **Collaborative:** Cultivating a sense of trust, respect, and responsibility among all parties
6. **Coordinated:** Providing a safe, efficient, and well-maneuvered response to disaster and recovery
7. **Flexible:** Allowing for creativity and innovation when established responses may fail or fall short of needs and expectations
8. **Professional:** Relying on a knowledge-based approach to research and planning⁴

Within the larger framework for emergency management, summit participants agreed that a specific context for higher education must be set. Crisis planning at an institutional level often requires definitions and approaches broader than those used in the government or industry sectors. While a single business may develop plans for protecting financial assets, personnel, and production values, a college or university campus is almost a city unto itself, involving crisis planning that encompasses the total physical, virtual, and even cultural components of the institution.

University campuses can be sprawling physical and virtual entities, demanding planning consideration for locations as varied as green spaces, parking lots, athletic venues, research labs, dormitories, classroom spaces, and institutional communications networks. Crisis planning is often coordinated between disparate departments, involving personnel from information technology, facilities, environmental services, and campus police and requiring a multilayered approach that can often become tangled and mismanaged without a central emergency-planning team.

The very nature of academic institutions presents inherent challenges. Student populations come and go. The campus community oscillates between permanent staff and residents and outside visitors. The research enterprise often encourages data sharing on the one hand (which opens the network to risks and vulnerabilities) while fiercely shielding an individual researcher's autonomy and freedom. Within this unique context, it is the role and responsibility of emergency managers to mitigate and prevent disaster while providing comprehensive education, planning, and recovery.⁵

Hallmarks of Effective Emergency Management

If effective emergency management is comprehensive, collaborative, and flexible, what are the hallmarks of an effectively managed crisis on campus? Summit participants, drawing from their own reservoirs of experience and best practices, tried to visualize what a well-planned and well-executed disaster response plan might look like. At the core of their analysis were the following seven traits:

- ◆ Relevant players understand their roles in advance and execute accordingly.
- ◆ Crisis communications are clear, consistent, and well received.
- ◆ Life and property are preserved to the greatest extent possible.
- ◆ Response plans are easily accessible, appropriate, and updated.
- ◆ Critical technologies work without delay or interruption.
- ◆ Campus transitions from “crisis” to “normal” in a timely fashion.
- ◆ University image is maintained in the eyes of internal and external communities.

Implicit in their analysis was an understanding that effective emergency management is conducted without panic and with careful and calculated preparation, through drills and simulations, and with vigorous attention to policies and procedures. Participants also voiced concern that although pondering a worst-case scenario might make it easy to conceptualize how the average campus could be crippled by a major disaster, the reality is that those events are the exception—a typical institution deals with many smaller-scale emergencies on a regular basis.

A safe campus, therefore, is not merely a campus that responds to disaster but one that cultivates an institutional culture of safety and security⁶: where public safety is a shared responsibility among students, faculty, and staff; where training is delivered across all levels and maintained on a consistent basis; where colleges and universities have the research, technology, and budgetary support to closely monitor campus safety and assess areas of increased risk and vulnerability; and where people walk onto campus and simply feel “safe.”

Challenges

Although creating a “100 percent safe” campus is not realistic, attempting to do so is not as simple as eliminating threats and vulnerabilities and stockpiling plans for

emergency response. On many campuses, a persistent culture of “invincibility” makes it difficult to capture and sustain the interest of students, faculty, and administrators, making it impossible to isolate an institution from even the most basic risks. Emergency managers are constantly fighting a battle between deploying preventative measures, such as monitoring and risk profiling, and maintaining institutional values of privacy and academic freedom. Keeping the focus on disaster prevention and response becomes increasingly challenging when the threat of imminent disaster has faded, making it more difficult to fund and deploy simulation exercises, planning reviews, and technological assessments.

Today’s Net Generation students bring their own share of challenges. The frequency with which they use and then abandon new technologies makes it difficult to provide comprehensive emergency notifications and communications. Solutions must bridge language, technology, and cultural gaps between students and the institution.

The sheer complexity of the campus organization can make it difficult to maintain clear and consistent response organizations. Communications must be managed between the central IT organization and support personnel, between the institution and its inhabitants, and between the institution’s emergency operations team and outside groups like emergency responders, government agencies, and the media. A culture of mistrust—often bred by “town versus gown” issues—may permeate the process, making it difficult to foster a truly cooperative and collaborative approach to disaster response with clear and respected lines of demarcation.

As institutional leaders struggle with the inherent challenges of their own campuses, they are also faced with a constantly evolving slate of technological solutions. Maintaining an inventory of new innovations, while carving out time to test, deploy, and assess their effectiveness, can prove an exhausting process, making it difficult to keep pace with current trends.

Emerging Opportunities

Despite the obstacles, the integration of information technology and emergency management presents significant opportunities for innovation in the way that we assess, manage, and respond to crises on campus. Today’s technologies are increasingly mobile, highly integrated, and inherently flexible. From social networking sites to geospatial imaging, campuses are already taking advantage of emerging tools to address critical needs.

Emergency Communication Systems

In the weeks that followed the shootings at Virginia Tech, “emergency notification systems” became the phrase du jour at the nation’s colleges and universities as administrators raced to fortify their institutions against the kind of criticism that had been leveled at Blacksburg officials—that they had been slow to notify students that shootings were taking place. Vendor applications offer a plethora of opt-in services that can push emergency messages to cell phones via text messages, e-mail accounts, instant message accounts, or college or university voicemail systems. But their success has often been impeded by student and parent apathy toward

participation, the time and effort involved to send messages across multiple channels and to maintain current contact information, and the difficulty in maintaining a consistent message across the spectrum.⁷

Sirens, digital signage in common spaces and classroom buildings, notification systems that include both e-mails and text messages, and automatic messaging to classroom projectors and alarm systems are among the most frequently cited technological answers to emergency notification.⁸ Brigham Young University (BYU) and Virginia Tech are among the campuses using customizable web-based systems that operate as a unified console for emergency messaging and notification. A user can log in, type or record a message, and then push information through multiple channels. The single-portal approach eliminates inconsistencies between messages and allows for fast and remote deployment.⁹

Geospatial Mapping Tools

In addition to more traditional tools for risk assessment, such as self-guided tutorials, calculators, and virtual assessment tools, campuses are taking advantage of geospatial mapping tools and location-based information to create visual representations of the campus landscape where officials can record and plot information about accidents or criminal incidents. By layering traffic accident reports with location data, for example, officials can gain a clearer image of key trouble spots on campus. Merely seeing the grid is not always enough, and the addition of complex layers of visual and geospatial information can allow a single administrator to identify a troubled area and then widen the perspective to look at key elements in the environment such as lighting, obstructions, or adjacent buildings.

At a broader level, geographic information systems are helping officials better predict and plot natural disasters, offering just-in-time data to assist in disaster recovery and evacuation efforts. Most recently, those systems helped coordinate response to Hurricanes Gustav and Ike in the Gulf region.¹⁰

GPS Technology

GPS-enabled devices are also helping students signal for help when emergency situations arise. Students toting cell phones with Rave Guardian software, for instance, can activate a timer on their device when they would like surveillance from campus police. A student stepping outside the library at night, for example, might activate the system while crossing campus. If the timer is not deactivated within a given time frame, authorities can use GPS technology to track the student's location. Students can also press a panic button, alerting officials that they may be in trouble and broadcasting the specific coordinates of their position. Using similar technology, students at BYU and Columbia University are among those who can tote a small, panic-button device on a keychain to alert authorities of emergency situations. The technology relies on radio waves to isolate a student's location.¹¹

Business Continuity Planning Tools

Summit participants agreed that disaster response plans must be easily accessible, consistently scrutinized, and up-to-date. Online databases and business continuity

planning tools offer new opportunities for the creation, storage, and sharing of plans in a virtual environment. Using university authentication, an individual campus department can log in to the campus planning tool, input specific plans to address its assets and responsibilities, and later access the plans for implementation or revisions. Tools such as the Berkeley Business Continuity Planning Tool (open source) allow users to print and share their plans while giving administrators the opportunity to quickly observe which campus departments have and have not submitted continuity plans.

Learning Management Systems and Virtual Worlds

When institutions affected by Hurricane Katrina were faced with either canceling their semesters or returning to storm-ravaged campuses, they began to focus on long-term business continuity planning. If the physical institution was no longer accessible—either damaged or vulnerable to pandemic—how would classes continue?

In the wake of Katrina, colleges and universities—particularly those in disaster-prone areas like the Southeast—began moving critical servers out of state or reevaluating how existing tools for distance education, like learning management systems, could be used to conduct classes when the physical campus is unreachable. But administrators are also looking at the emerging arena of Second Life, a virtual world where a number of campuses—including the University of New Orleans—have purchased virtual land to build entirely online campuses. If a disaster were to strike, students and faculty could log in from disparate locations and participate in an online lecture in virtual classrooms and buildings that resemble the physical institution. Students can create avatars that represent their physical presence, and faculty can use voice technologies to speak to students in the virtual room.¹²

Improvements in multimedia tools and sharing platforms has made it possible for faculty members to capture their lectures on a handheld device and upload them to university-specific channels on iTunes or YouTube. Together, these tools create a multilayered approach to academic continuity in a virtual context.

Social Networking Tools

To reach students who are constantly connected to the Web and actively creating and sharing content in their own time, emergency management teams are turning to familiar social networking tools to share news and strategies for campus safety and security. Social networking sites like Facebook and MySpace allow campus departments to create pages that store information about campus plans, emergency procedures, and university events. The widespread popularity of networks like YouTube and iTunes have created opportunities for officials to educate through quick, entertaining videos and podcasts that can be easily stored and shared.

By encouraging students to become “friends” with emergency management groups on Facebook and MySpace, administrators can create an alternate pathway for pushing information to the wider community. Unlike common emergency notification systems, however, Facebook and MySpace allow students to add their own commentary through “on the scene” reporting, sharing messages with friends, or

posting their own photos and videos. The university-developed groups offer a layer of authenticity, helping debunk misinformation provided by the students themselves.¹³

Virtual Emergency Operations Centers

Physical emergency-operation centers (EOCs) have often been the hub of campus response in times of emergency. Increasingly, however, campuses are considering replacing or supplementing those physical locations with virtual EOCs that can coordinate response teams across geographic areas. A virtual EOC dashboard can store and integrate unit response plans, incident reports, and operational reports from a variety of campus and community agencies. A single user can access the virtual EOC to send communications through various channels to relevant players. In cases when the physical campus is unreachable or unsafe, the virtual EOC provides a safe and accessible alternative to coordinate groups across campus and the wider community.

Intelligent Monitoring

College campuses are increasingly transient places, playing constant host to new students, sporting fans, community members, visiting lecturers, and outside groups. Striking a balance between security and openness often relies on community monitoring that provides critical knowledge while preserving personal freedoms and reasonable expectations of privacy. For these, campuses are turning to new advances in intelligent monitoring, from biometrics and speech-recognition software to intelligent video and swipe-card access to university buildings.

Data Mining and Database Tracking

In the weeks that followed the shootings at Virginia Tech, campus administrators were criticized for failing to heed potential warning signs during Seung-Hui Cho's time at the university, particularly a history of mental illness and a faculty member's request that Cho seek counseling. Since the shootings, colleges and universities have questioned whether predictive modeling, aided through data mining software and other actuarial tools, offers some promise for preventing campus violence or suicide. The problem, experts say, is that predicting violence is a nebulous process, sending up false positives and missing potential offenders.¹⁴ Still, colleges and universities have turned to databases to encourage information-sharing between institutions. After two separate incidents in 2004 at the University of North Carolina Wilmington in which students were murdered by other students, officials at the UNC system's 16 campuses began feeding suspension and expulsion data into a shared database, allowing schools to check to see if a potential applicant had a violent history at another university. The 2004 murders were not connected, but both assailants concealed past offenses from school officials.¹⁵

Information Sharing

Summit participants continually noted that one of the most frequent barriers to effective emergency management is a lack of communication between campuses. Greater communication might include sharing case studies that showcase best practices or offering open solutions to campus needs. The University of Oregon

hosts the Disaster Resilient University (DRU) listserv to encourage information sharing and open dialogue between emergency management practitioners on campus. Users must have a dot-edu e-mail address to join.

Action Agenda

Summit participants agreed that technology alone cannot be the answer. Rather, a comprehensive new agenda for emergency management must leverage both the possibilities of new technologies and the critical components of institutional collaboration, planning, and research.

The goal of the summit was not to create a concrete plan for campus response but to begin assembling the pieces of a comprehensive action agenda that would facilitate information sharing between campuses, foster collaboration among institutions, surface key issues in emergency management, and build solutions for a higher education approach to disaster preparedness. As they looked to the horizon, participants agreed on the following tenets of an action agenda and, under each item, proactive steps that they—or the higher education community at large—might take to move forward:

- ◆ Information sharing is a critical and often neglected cornerstone of a national approach to emergency management.
 - ❖ A multicampus information-sharing mechanism should be at the hub, providing anytime, anywhere access to just-in-time threats and resources.
 - ❖ Campuses may need to explore the establishment of a central organization, similar to the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC),¹⁶ for monitoring, collecting, sharing, and analyzing information related to current and emerging threats.
- ◆ Emergency management must stay at the top of the institution's agenda, in terms of strategic discussions, budget allocations, and administration priorities.
 - ❖ Individual campuses must work to discover and cultivate a “champion” within their administration to keep emergency management at the forefront.
 - ❖ Leading higher education associations should produce simple, easy-to-understand policy documents that outline the importance of emergency management and key items for college and university administrators to know. These documents should be used to align emergency management with funding priorities.
- ◆ Campuses must take an all-hazards approach, focusing on emergencies and disasters across the spectrum.
- ◆ Risk management is a critical component of campus preparedness.
 - ❖ Institutions of higher education should continue to sponsor and support research into emerging threats and risk assessment.
 - ❖ Results from individual risk assessments should be shared across campus and the greater higher education community.

Campus Security and Emergency Management

- ❖ Campuses should consider the development of geospatial mapping tools to plot and share risk assessment data.
- ❖ Risk assessment planning and hazard analysis should be part of the standard operating procedure, not an occasional exercise.
- ◆ Campuses must begin to think proactively, not reactively, about common threats and vulnerabilities.
 - ❖ Colleges and universities must constantly monitor information systems to search for specific points of weakness and vulnerability.
 - ❖ Emergency response plans should be consistently updated and accessible, with physical copies and digital repositories.
 - ❖ Students and faculty should know how and where to access information in case of an emergency.
- ◆ Preparation and response require collaboration across departments, throughout the community, and between campuses.
 - ❖ Campuses should begin to build partnerships with outside units, sponsoring community symposia with local emergency response teams or inviting community responders to have an active role in campus planning.
 - ❖ The community should carefully examine the roles and responsibilities of local emergency operations centers, seeking opportunities to collaborate on central command or share resources.
- ◆ Evaluation of disaster plans and planning tools must be a critical component of the approach.
 - ❖ Developing criteria for evaluation and tools for information sharing could fall to a multicampus association or professional working group.
 - ❖ Campuses should consider open access to institutional tools for planning and evaluation.
 - ❖ The research enterprise should develop tools for simulating and evaluating emergency response.
- ◆ Higher education institutions must strike a balance between the open, research-driven nature of their enterprise and the need to foster a safe campus environment.
 - ❖ Individual campuses should begin a dialogue between critical campus units and researchers, fostering an understanding of the needs, fears, and responsibilities of each group.
 - ❖ Institutional procedures should be created for alerting students, faculty, and staff to emerging cyberthreats, offering useful tips for managing risk.
- ◆ Higher education must keep an eye on emerging technologies, constantly seeking new opportunities to leverage technology for emergency management and to evaluate existing and emerging tools.

- ❖ Campuses need an up-to-date database of existing technologies, with resources for discovering what the tool does, who is using it, and best practices for deployment.
 - ❖ Within existing and future associations, emergency management professionals should form partnerships and working groups to develop community solutions, moving away from individual point solutions.
 - ❖ Colleges and universities should keep a keen eye on industry, watching outside trends in emergency management and adopting those trends to the higher education context.
 - ❖ The emergency management community should develop tools and criteria for evaluating current technological tools.
- ◆ Emergency management is not merely a planning issue but a cultural one, requiring the commitment and dedication of students, faculty, and staff.
- ❖ Web 2.0 tools (such as Facebook and MySpace), university websites, and campus orientation sessions should be seen as opportunities to educate the campus community about their responsibilities as campus citizens and procedures for emergency response and recovery.
 - ❖ Members of the institution should receive ongoing education about their role in prevention and preparedness.

Conclusions

In the opening session of the summit, EDUCAUSE President Diana Oblinger posted a single quote from the International Association of Emergency Managers: “If we shake hands before a disaster, we won’t have to point fingers afterwards.” After ticking off many of the hazards that colleges and universities have faced in recent years and noting their unpredictability—and their apparent frequency—she suggested that the most powerful tool for moving forward might be the collaborations fostered by participants over the course of the two-day summit.

That theme—cooperation and collaboration—permeated every session, rising to the top of the list of challenges and also landing at the top of the group’s action agenda. While all agreed that a comprehensive approach to emergency management must include risk assessment, technological innovation, planning, and evaluation, breaking down the walls between departments—and institutions—seemed to be a central and consistent tenet of their common vision for moving forward.

Campuses need to share best practices and lessons learned, participants said. They argued for a national database of campus experts and innovative solutions—a way to connect people who can share ideas or lend expertise, a new model for continuing and building the conversation. Only when the dialogue is ongoing and evolving, they agreed, can a truly cooperative and innovative model for emergency management in higher education be established and maintained.

Endnotes

1. Midwestern Higher Education Compact, "The Ripple Effect of Virginia Tech," Minneapolis, MN , May 2008, http://www.mhec.org/policyresearch/052308mhecsafetyrpt_lr.pdf.
2. International Association of Emergency Managers, "Principles of Emergency Management," September 11, 2007, 4, <http://www.iaem.com/publications/documents/EMPrinciples091107.pdf>.
3. For definitions of the four phases of emergency management see National Fire Protection Association, "NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity Programs, 2007 Edition," <http://www.nfpa.org/assets/files/PDF/NFPA1600.pdf>.
4. NFPA, "Standard on Disaster/Emergency Management," 4.
5. Diana Oblinger, "Computer and Network Security and Higher Education's Core Values," (Research Bulletin, Issue 6) (Boulder, CO: EDUCAUSE Center for Applied Research, 2003), <http://connect.educause.edu/Library/ECAR/ComputerandNetworkSecurit/40063>
6. Security, as defined by the ASIS Foundation in *ASIS Standard for Organizational Resilience: Security, Preparedness and Continuity Management System*, is "the condition of being protected against hazards, risk, threats, or loss" http://www.asisonline.org/guidelines/inprogress_published.htm#org.
7. Andrea Foster, "After Va. Tech, Campuses Rush to Add Alert Systems," *Chronicle of Higher Education*, October 05, 2007, <http://chronicle.com/weekly/v54/i06/06a00103.htm>.
8. Virginia Tech is among the campuses using LED displays in the classroom to broadcast notifications to students. See Jeffrey R. Young, "Virginia Tech Adds LED Message Boards for Emergency Notification," *Chronicle of Higher Education*, September 3, 2008, <http://chronicle.com/wiredcampus/index.php?id=3288>
9. Mark Owczarski, "University Agreement to Significantly Expand Campus Emergency Alert Systems," *Virginia Tech News*, June 21, 2007, <http://www.vtnews.vt.edu/story.php?relyear=2007&itemno=363>.
10. "GIS Helps Bolster Hurricane Preparation and Response," *American Surveyer Online*, September 11, 2008, <http://www.amerisurv.com/content/view/5395/2/>.
11. Jeff Cox, "After Virginia Tech, Security Firms Ramp Up," *CNN.com*, April 26, 2007, http://money.cnn.com/2007/04/25/news/companies/campus_security/index.htm.
12. "Virtual Campus Could Aid In Emergency," *eSchool News Online*, June 17, 2007, <http://www.eschoolnews.com/news/top-news/index.cfm?i=46372&CFID=11812042&CFTOKEN=33421087>.
13. Jeffrey R. Young, "Emergency Alerts via Facebook and MySpace Are New Ways to Reach Students," *Chronicle of Higher Education*, August 22, 2008, <http://chronicle.com/free/2008/08/4317n.htm>.
14. Elizabeth Redden, "Predicting and Preventing Campus Violence," *InsideHigherEd.com*, April 7, 2008, <http://www.insidehighered.com/news/2008/04/07/violence>.
15. Mary Beth Marklein, "An Idea Whose Time Has Come?" *USA Today*, April 18, 2007, <http://www.usatoday.com/educate/college/arts/articles/20070415.htm>.
16. According to its website (<http://www.ren-isac.net>), the REN-ISAC is "an integral part of higher education's strategy to improve network security through information collection, analysis and dissemination, early warning, and response—specifically designed to support the unique environment and needs of organizations connected to served higher education and research networks; and supports efforts to protect the national cyber infrastructure by participating in the formal U.S. ISAC structure. The REN-ISAC receives, analyzes, and acts on operational, threat, warning, and actual attack information derived from network instrumentation and information sharing relationships.... Information sharing relationships are established with other ISACs, DHS/US-CERT, private network security collaborations, network and security engineers on national R&E network backbones, and the REN-ISAC members."

Summit Attendees

William Badertscher, Georgetown University

Earving Blythe, Virginia Tech

Art Botterell, Office of the Sheriff, Contra Costa County

Allen Bova, Cornell University

Mark Bruhn, Indiana University

Timothy Chester, Pepperdine University

Kenneth Fauerbach, New York University

Cynthia Golden, EDUCAUSE

Steve Goodman, Brigham Young University

Jay Gruber, University of Maryland

Betty Hawkins, University of South Carolina

Steven Healy, Princeton University

Norma Holland, EDUCAUSE

James Hyatt, NACUBO

James Jokl, University of Virginia

Mark Katsouros, University of Iowa

Richard Katz, EDUCAUSE

Laine Keneller, University of California, Davis

Joseph Lalley, Cornell University

Dave Lambert, Georgetown University

Timothy Lance, NYSERNet, Inc.

Kathy Lang, Marquette University

John Lawson, Western Washington University

Catherine Lewis, Xavier University of Louisiana

David Lindstrom, The Pennsylvania State University

Valerie Lucus, University of California, Davis

Mark Luker, EDUCAUSE

Walt Magnussen, Texas A&M University

Jenny Mehmedovic, University of Kansas

Diana Oblinger, EDUCAUSE

Carie Page, EDUCAUSE

Rodney Petersen, EDUCAUSE

Larry Rickard, Marquette University

Leslie Riester, Portland Community College

Martin Ringle, Reed College

Jeri Semer, ACUTA

David Sliman, Gulf Coast University of Southern Mississippi

Mike Sofield, Smithsonian Institution

Brenda van Gelder, Virginia Tech

Brian Voss, Louisiana State University

Wendy Wigen, EDUCAUSE

Kirk White, Indiana University

Owen Yardley, University of Nebraska–Lincoln