Within an incredibly short period—perhaps less than twenty-four months—the need for emergency preparedness has risen to a higher level of urgency than at any other time in the history of academe. Large or small, public or private, higher education institutions are seriously considering the dual problems of notification and communications management when potentially life-threatening events confront a campus environment.

E. Michael Staman is the Peyton Anderson Professor for Information Technology at Macon State College. Mark Katsouros is Director of Telecommunication & Network Services at the University of Iowa; Richard Hach is Associate Director of Network Administration, Special Projects and Initiatives, at Virginia Tech.
Emergency preparedness is certainly not a new agenda item. Communications about and procedures for responding to fires or natural disasters have been in place for decades. Most institutions have some sort of campus hotline that students can use in the event of an assault or other violent crime and also some sort of calling tree that will communicate decisions such as a campus closing because of an impending snowstorm or similar situation. But the problems associated with—and the opportunities for dealing with—emergency preparedness have evolved significantly in recent years, possibly catalyzed by the April 2007 shooting incident at Virginia Tech. On the one hand, there seems to be a growing tendency toward violence; on the other hand, an increasingly rich collection of notification, communications, and management tools can assist in mitigating the impact of these situations.

These tools range from something as simple as external sirens to solutions involving combinations of various technologies: a campus website, e-mail, landline phones, cell phones, text messaging, paging, external loudspeakers, digital signage, a campus CATV system, network pop-ups, RSS feeds, instant messaging (IM), fire panel alarms with voice enunciation, and/or social networking websites.

This rich variety of tools and solutions leads to two important questions for colleges and universities to consider. First, how can these technologies be best leveraged to benefit emergency notification services? And second, what are the implications of all of these options on emergency communications management policies and operational procedures? We define an emergency notification system (ENS) as a specific technical service designed to achieve mass notification in the event of an incident demanding such an action. Emergency communications management (ECM) refers to the policies, procedures, and operations acting in concert with an ENS.

To help institutions answer these two questions and also to provide insight into the basic parameters of emergency communications in higher education today, the Steering Committee of the EDUCAUSE Net@EDU Converged Communications Working Group (CCWG)\(^1\) (http://www.educause.edu/ConvergedCommunicationsWorkingGroup/13524) recently sent a short survey to a group of carefully selected colleges and universities.\(^2\) The objective was to discover the nature of the work being accomplished at these institutions. The responses to this survey also helped to inform two case studies, prepared by the CCWG Steering Committee, on ENS and ECM solutions at Virginia Tech and the University of Iowa.

**Basic Parameters**

Of the survey respondents, 84 percent reported that they have “implemented significant features” of the ENS/ECM solution currently designed for their institution. But almost all also note that their efforts are a work in progress, with 88 percent reporting that they will be adding elements to their solution in the future. Examples include deploying additional infrastructure, expanding in-house capabilities to better track contacts, and integrating with “other technologies, such as digital signage, PA systems, alarms, and television.”

**The Driving Issues**

The shock of violent incidents such as those at Virginia Tech and Northern Illinois University has clearly accelerated the deployment of ENS solutions. The two predominant issues that respondents noted for driving ENS implementation were “recent incidents on other campuses” and “general public safety” (see Figure 1).

**Participation**

Despite the current visibility of the emergency preparedness problem, subscription rates to notification services are not uniformly high. Only 40 percent of respondents reported high participation rates (with “high” defined as over...
three-quarters of the population); 48 percent report participation rates at half or less (see Figure 2). It appears that the most significant factor driving these statistics is an institution's policy on the question of whether specific action is required from users to include or remove their contact information from notification databases.

(The “opt-out” vs. “opt-in” policy implications are discussed in more detail below.)

A number of institutions reported that people who are not directly part of the campus community can also receive notification in the event of an incident, with approximately one-third of respondents reporting that such information can go to students’ parents (see Figure 3). We anticipate that this figure will grow as ENS awareness and system maturity evolve.

Summary of Deployed Solutions
The network is central to virtually every ENS strategy, as are also legacy voice and cellular solutions. All respondents reported that e-mail, texting, and the campus website are integral to the notification process (see Figure 4).

Speculating on future evolutions can be interesting. At any given time, for example, a large percentage of an entire campus community is logged on to one of many internal web-based services. What might happen if policies were developed to force pop-up permission for every one of these? Such a solution might drive additional dissemination of emergency information. Although word-of-mouth solutions are not addressed in this article, there is anecdotal evidence that human communication, though potentially not fully accurate, is not only rapid but also one of the most effective ways of quickly disseminating emergency information.

Case Studies
The Virginia Tech and the University of Iowa case studies are based on four incidents. Although all four demonstrate the need for emergency preparedness, their differing characteristics suggest that multiple strategies can and should be considered as higher education institutions prepare to respond to potentially life-threatening events. The two incidents at Virginia Tech were “instantaneous” in nature, both times involving someone with a gun. The first, in 2006, originated and was resolved completely off campus; the other was the now-infamous on-campus shooting that occurred in April 2007. In contrast, the two incidents at the University of Iowa evolved over time—over several hours in the case of a tornado in 2006 and over many days in the case of the floods of 2008.

Virginia Tech
On Sunday, August 20, 2006, the day before the start of a new semester at Virginia Tech, William Morva, a prisoner accused of armed robbery, was receiving medical treatment at Montgomery County Regional Hospital near the main campus of the university. At the hospital, Morva overpowered a law enforcement officer, killed a hospital security guard, and escaped from the facility, prompting a manhunt that would eventually include the Virginia Tech campus and the town of Blacksburg. Before being recaptured, Morva shot and killed a Montgomery County sheriff’s deputy and was falsely reported to be on the Virginia Tech campus. The incident prompted the closing of area roads and the cancellation of classes on the first day of the fall semester. Students, faculty, and staff received notifications—including emergency advisories, evacuation plans, emergency updates, road closures, and cancellations—via campus telephone, voicemail, e-mail, and the university’s web page.
Impact on Virginia Tech’s Emergency Notification Strategies

As early as March 2006, a Messaging Futures Working Group—composed of staff members from Communications Network Services, Systems Support, and the directory maintenance part of Secure Enterprise Technology Initiatives—had been meeting to look at the convergence of messaging technologies. Following the Morva incident later that year, the university reviewed its emergency notification strategy and formed another group to look at campus communication systems. In particular, this group investigated the idea of adding a hosted service capable of sending emergency alerts or other communications to cellular telephones and other wireless devices via short text messages known as SMS (Short Message Service). Potential vendors were identified, and the first meetings were conducted in March 2007. Working to evaluate the features and benefits of providers’ systems, the team identified a desirable feature: the ability to send a notification to multiple, concurrent platforms—that is, via landlines, facsimile messages, and e-mail, in addition to short text messages delivered via cellular networks.

An alerts system that could successfully provide the ability for “multi-modal communications,” including the use of true SMS protocol and IM, became one of the requirements. No less important was an alert system registration or “subscription” process that was flexible, including application program interfaces (APIs) and online methods that would allow the university to load existing directory information directly into the alert system of the provider.4

The April 16, 2007, Tragedy

An academic year that began with violence near Virginia Tech concluded with a tragedy on the campus itself. On April 16, 2007, in two related incidents, a gunman killed thirty-two students and faculty members and injured seventeen others, before killing himself. The second event, which followed a double homicide in a residence hall, occurred at Norris Hall, an academic and administration building. The Norris Hall incident was concluded in about eleven minutes. Approximately twenty-seven ambulances and fifteen hundred first responders, representing fourteen agencies and five hospitals, responded to the need at Virginia Tech.

A key area of emphasis following the Morva incident was the provision of mass notifications during an emergency, along with subsequent instructions. In responding to the April 2007 tragedy at Virginia Tech, emergency notification was provided using multiple outlets: e-mails broadcast to the Tech community mailing list; voicemail sent to campus phones in offices and residence halls; recorded messages on the university WeatherLine/Hotline; the Virginia Tech home page (http://www.vt.edu); the Virginia Tech News website (http://www.vtnews.vt.edu); the university switchboard; the campus warning siren system; and public media outlets.

Following the April tragedy, an additional mass notification solution was deployed on the campus of Virginia Tech. As discussed above, a short list of providers for this service had been identified before April 16, 2007, and the vendor review process was expedited following the tragedy. 3n (National Notification Network) of Glendale, California, was selected to provide hosted services for sending emergency messages via cell phones, landlines, e-mails, and PDAs and other wireless devices.

Summary of Virginia Tech’s Current Strategy

Virginia Tech’s strategy regarding emergency notification and emergency communication systems is to utilize multiple methods of contact and more than one type of alert system to increase the probability of a successful contact. Although no single notification mechanism will reach everyone, and although “near real-time” notification is very difficult to achieve in a large campus environment, the overall strategy is to find solutions that focus on mechanisms in which the campus has control of most or all of the technical elements. In addition, the strategy aims to provide flexibility in adding subscribers, to integrate with existing systems, and to protect personally identifiable information. This ability to (a) initiate a notification, (b) verify notification delivery, and (c) gain accurate reporting in connection with an event is highly desirable.

Future Considerations

A project to develop a single, common interface for users of emergency communications systems began in May 2008. The goal of the project was to devise a web-based application for use by University Relations and the Virginia Tech Police Department to make the underlying complexity of the notification technologies less apparent. Another goal was to ensure that, even though the user may be under duress due to an incident demanding action, the emergency notification message could be issued quickly and correctly. This application was provisionally known as the “VT Alerts Notification Console,” and individuals from many
different areas of the Information Technology department were part of the team responsible for the project development and system integration. The first phase of this project was made available for use by University Relations and the Police Department before classes started on August 25, 2008. The initial Notification Console product resulting from this project integrates notification message delivery for VT Alerts via mobile, web, and e-mail delivery, collectively known as “VT Alerts: Online,” and also via classroom message boards, known as “VT Alerts: Classroom” (see below). With future funding, additional notification channels—such as the university’s WeatherLine, CATV system, outdoor loudspeaker system, and voice-mail system—will be integrated.

“VT Alerts: Classroom,” consisting of electronic message boards installed in each of the 165 general-assignment classrooms on the Blacksburg campus, was initiated in May 2008. The message boards communicate information about campus emergencies or other significant events directly into the classrooms. Stakeholders for this effort include the Office of the Provost, University Facilities (under the Vice President for Administration), University Relations, and the Virginia Tech Police Department. Communications Network Services provided the staff for the physical installation of the sign equipment and the related network facilities. The system was fully operational by August 15, 2008.

An important element of any emergency management strategy is continual testing and appraisal. On Thursday, November 13, 2008, Virginia Tech used its ENS for a situation other than a test. Unfortunately, not all of these systems functioned properly. The systems that are managed and maintained by Virginia Tech—the university home page alert, campus-wide e-mail, and the electronic message boards in classrooms—worked well. The 3n mass notification system failed to work as expected. Of the three emergency notifications sent that day, only some of the VT Alerts subscribers received the first emergency message. The second and third messages were not delivered by the vendor. 3n confirmed a system failure on its part, but as of this writing had not determined the cause of that failure. A subsequent test of the Virginia Tech emergency notification system conducted on December 8, 2008, indicated that all four communications channels performed as expected.

University of Iowa
On April 13, 2006, Iowa City was struck by a severe storm: large hail and tornados left a path of destruction three and one-half miles long and one-third of a mile wide. This was the first time a tornado had ever hit Iowa City directly—two had actually touched down inside Iowa City. Miraculously, there were no serious injuries or deaths in the Iowa City area, but the cost to repair all of the buildings damaged by the storm has been estimated at $12 million.6

Impact on Iowa’s Emergency Notification Strategies
This incident, combined with the availability of suitable emergency notification products, prompted the University of Iowa to embark on an ENS exploration project. The university’s solution included both a multimodal ENS and a separate siren tower system. The ENS is built on Blackboard Connect’s ConnectED system, and the sirens were manufactured by Whelen Engineering. At this time, however, these systems are not integrated. The sirens are generally utilized to disseminate serious tornado alerts provided by the National Weather Service. The ENS, branded as “Hawk Alert,” is the heart of the university’s emergency notification strategy.

The Flood of 2008
The flood of 2008 involved most of the rivers in eastern Iowa. It began sometime around June 8 and ended on about July 1—though flooding continued on the upper Mississippi River in the southeastern portion of the state for several more days. The phrase “Iowa’s Katrina” was often heard in descriptions of these events.7

By June 14, the Iowa River had risen dramatically. Warnings were issued for people to prepare to evacuate from the “500-year floodplain.” The university had time to get ready, and with the help of volunteers, it moved important library collections out of harm’s way. The bookstore

An electronic message board in a Virginia Tech classroom

Some of the worst damage from the April 2006 tornado, east of Governor Street on Iowa Avenue

The University of Iowa arts campus on the west side of the Iowa River
in the student union moved its contents to higher ground.\(^9\) The university’s electrical power plant was shut down on June 14 as sections of the plant began to take on water.\(^9\)

The good news was that the situation developed slowly, and water levels rose relatively slowly, giving the university time to plan. A new template was developed for evacuating buildings during a flood emergency: “EMERGENCY HAWK ALERT, [DELIVERY_DATE], (time): (building name) is under immediate flood threat. If you can safely do so, evacuate at once and immediately seek higher ground. Call 911 for emergency help. Tune into mass media outlets for further details.” This message could be quickly sent to the occupants of any specific building(s) on campus. Fortunately, it has not been used, but the university is prepared if a similar situation arises again.

**Summary of the University of Iowa Strategy**

The goal of the University of Iowa, like Virginia Tech, is to be able to reach as many people as possible, as quickly as possible, in the event of an emergency on campus. Given the general mobility and the broad range of diverse communication preferences of its community, one of the main priorities is to provide a solution that is as “multimodal” (voice, text, e-mail, etc.) as possible. The idea is to eliminate the dependency on any single communications medium and to distribute and lessen the impact on the various infrastructures involved.

Another important strategic goal of the Iowa planners is to make the process of initiating an emergency notification as easy and straightforward as possible while still keeping the process secure. Having to wordsmith and record a concise, calm, articulate message in the midst of a crisis, especially with the likely distractions of phones ringing and other commotion in the background, will be problematic, if not impossible. To combat these problems, the planners incorporated two ideas: (1) templates for a broad variety of emergency scenarios have been created and preapproved, and (2) those templates use text-to-speech (TTS) enunciation in order to announce dynamic (such as incident location) data without the need to “record” the messages. To add credibility, the TTS-enunciated messages follow a prerecorded message in the police chief’s voice: “This is UI Police Chief Chuck Green. Please listen to this important Hawk Alert.” Such a strategy is possible only if the system/vendor supports “blended” messages to include both recorded speech and TTS enunciations.

Finally, a communication campaign is being waged continuously, including everything from branding the service, so that it’s easily recognized/referenced, to frequently advertising the service, its portal, and the annual campus-wide tests via mass e-mails, the course management portal, and the other elements of the ENS infrastructure.

**Future Considerations**

The Hawk Alert ENS will continue to be refined as experiential best practices emerge. Additional communication modes will be explored as well. One such mode is social networking sites—particularly Facebook, which appears to be where college/university students “hang out” and thus is likely to be an effective communications channel. (In addition, messaging across Facebook has minimal impact to local communications infrastructure.)

The future promises to bring better integration of these various products/modes as standards for interoperability, such as CAP (Common Alerting Protocol) and EDXL (Emergency Data Exchange Language), emerge. In the meantime, the university hopes to develop a “dashboard” front-end application to provide a single interface into multiple back-end message-delivery systems.

**Lessons Learned and Policy Implications**

The ongoing use of an ENS (to include both testing and responses to actual incidents) will provide valuable information, as well as opportunities to make process improvements. Both case studies yield the following lessons:

- No single notification mechanism is going to reach everyone.
- The inherent fallibility of every notification mechanism mandates that a campus use an array of diverse approaches to increase the probability of making contact with everyone in its community.
- Near-real-time (i.e., instant) communication is very difficult to achieve in a large campus environment.
- Any solution should focus on mechanisms for which the campus can manage as many of the technical elements as possible.

Another significant lesson learned from both case studies is the need to simplify the process of sending an alert. Assume, as in the case of the University of Iowa, that the campus has prepared preapproved templates. This strategy becomes more efficient if the templates are optimized for speedy creation and delivery—for example, having a single message/template per scenario and sending one alert per incident to direct people to mass media outlets for additional information. Otherwise, “update” messages may be sent too soon and can
potentially compete for communications infrastructure resources, possibly delaying the delivery of the original message.

What Works?
Survey responses indicated that the one solution with the potential to work best is simple audio alerts with voice capabilities: outdoor or indoor sirens or paging systems. More generally, responses to the question “What worked?” included e-mail, calling trees, campus websites (occasionally linked to social websites), texting, and campus radio and television, along with voicemail and calling to legacy landline and cell phone systems—probably because these were commonly deployed solutions.

But with the exception of audio alerts, the same responses were given for the question “What did not work well?” The primary contributing factors were slow speed, congestion, network capacity, available size of text messages, and the difficulty of making contact as a result of subscribers’ mobility or the asynchronous nature of services such as e-mail or voicemail. Time was the common factor: time to “officially” conclude that there is an emergency, time to compose an alert, time to get the alert through a congested infrastructure, and time for recipients to see or hear the alert once it arrives at a given destination.

An important factor for institutions to fully consider is the “least common denominator” of each of the elements of a communications infrastructure. An analysis of peak capacities is probably in order. In the voice system, for example, a campus could make the mistake of considering inbound trunk capacity to be the most important constraining factor when the availability of voicemail ports may actually be more limiting. Depending on the way a specific voicemail system queues calls and on how a specific ENS retries and timeouts, overloading that voicemail system may be highly detrimental to delivery times.

Opting-in versus Opting-out
At the University of Iowa, a major concern expressed by both campus officials and customers was the potential for non-emergency communications (essentially, “spam”) to dilute the service and lessen the impact of emergency messages. The decision was therefore made to use the service only for “emergency” situations.

As a result, the entire enterprise directory, with all of the phone and e-mail contacts for each person, is loaded into the Hawk Alert database. The initial default is that all contact points will be used to send Hawk Alerts. Someone would have to explicitly opt-out of the service for each contact point, via the university’s homegrown portal, in order to not receive Hawk Alerts. The decision to make the overall receipt of emergency Hawk Alerts an opt-out vs. an opt-in process stems from the perception that the potential negative outcomes for those who intended to opt-out but never did are clearly less serious than the outcomes for those who intended to opt-in but never did.

Results from the survey reinforce the wisdom of this decision. Although there are minor variations from one service to another, when the default status is opt-out, subscribers do so less than 8 percent of the time, leaving approximately 92 percent participating in the ENS (see Figure 5). On the other hand, opt-in figures are low regardless of the service or the population. Not surprisingly, when the default action requires subscribers to opt-in, less than 40 percent participate in the ENS.

Most campuses have selected opt-in as their policy. When asked to comment on the rationale, almost all of the survey respondents provided a comment similar to the following: “E-mail is seen as the one method that guarantees we reach everyone, so it is automatically sent; text, cell, landlines use the same mechanism and since text has cost associated, it is opt-in.” But concern about low participation rates appears to be causing many to reconsider. The following comments were typical:

- “We plan to get incoming students to sign up—and are already seeing improvement there—parents want them to sign up.”
- “Student feedback indicated that opt-in was preferred to avoid spam. Having the subscription process integrated with [the] semester class registration process has greatly improved the subscription rate, however. A student must either opt-in or opt-out before completing the class registration process.”
- “We automatically pop up a screen to all employees and students at the beginning of each semester that requires them to review and update their emergency contact information. . . . Students were asked to provide a cell phone number; now they are required to do so in order to register.”

Communications Management
Most solutions include external emergency organizations in their ECM and ENS procedures. In fact, the emergency
preparedness question involves communications policy and planning as much as systems planning and operations. Good cooperation and agreements between campus and local police, fire, and EMS jurisdictions are required, including joint training exercises, a joint emergency preparedness response plan, and emergency communications systems that understand each other. From all sources, we observed the common threads of the requirements for an engaged campus leadership and the need for proactive and effective education of the college/university community.

Working with multiple agencies has become important. Here are two typical survey responses regarding communications management: (1) “Local emergency response services are used to coordinate and acquire accurate and credible information on the incident. This includes law enforcement, fire, hazardous material, Emergency Medical Services and the Regional Dispatch Center.” (2) “[We] have involved health authorities since pandemic planning—county and local, but also some ties to state level; city police department with University police—better coordination to meet Cleary requirements…and better coordination between the University hospital and campus—[are] not usually viewed internally as belonging under one ‘umbrella.’”

**Summary**

Several important success factors can be identified as a result of the analyses of the CCWG survey and the two case studies. Technical and operational considerations focus on

- implementing multimodal techniques (e.g., use many and diverse communications solutions);
- realizing the extent to which solutions and services can operate in converged networked environments; and
- understanding and, if necessary, improving infrastructure constraints (e.g., voicemail port vs. external trunk capacity).

Key policy and strategic considerations focus on making as many decisions as possible in advance. Important factors include

- prerecorded and predefined message templates for incident-specific emergencies;
- authorization alerts by (preapproved) proxy;
- policies that eliminate every level between the observation of an incident and the authority to send notification; and
- the ability to communicate the realities about system capabilities before an actual emergency.

Other important considerations concern campus decisions about

- whether the ENS will be used exclusively for emergencies,
- how the institution will deal with the opt-in/opt-out policy,
- the importance of branding to ensure
clear and focused identification of the sending authority,

- the need for sufficient testing to ensure that both the roles of individuals and the capacities and limitations of the system are well understood, and

- the requirement to ensure that all contact databases are updated on at least a daily basis.

Not surprisingly, the list of policy and strategic questions is longer and potentially more difficult to resolve than the list of technical and operational questions. In the final analysis, there are many dimensions to emergency preparedness: notification technologies, communications management, operational and strategic policies—all within the context of events that either can happen instantly or can evolve over time. Like virtually every other problem in which technology is an inherent element of the solution, the need for emergency preparedness—along with its policy questions, communications issues, and continually evolving solutions—will remain an issue for colleges and universities for the foreseeable future.

Notes
1. The EDUCAUSE Net@EDU Converged Communications Working Group (CCWG) was formed on July 1, 2007, from the merger of the Net@EDU Wireless Working Group and the Integrated Communications Strategies Working Group. For more information on the CCWG and how to become involved, please see the website or contact any of the members of the Steering Committee.

2. The Steering Committee selected and contacted 125 institutions with a short survey and received a 20 percent response. Readers should not consider the data in this article as representative of a random or national survey. Results from the survey are more representative of conversations that would occur at a meeting of colleges and universities that have completed significant work on ECM/ENS. Comments are reflective of the status and progress of those working on the problem and tend to be weighted in favor of large, R-1 universities.

3. All quoted comments in this article are taken from the questions and responses in the CCWG Steering Committee survey.


5. William Dougherty, Carl Harris, and Patricia Rodgers contributed to the Virginia Tech case study.


