Mass Notification for Higher Education

National Clearinghouse for Educational Facilities

Tod Schneider
October 2009

Due to rapid changes in security technology, this publication is updated quarterly. See the related NCEF publications, School Security Technologies *and* Selecting Security Technology Providers*.*

Mass notification is a high priority in educational institutions. But as the number of electronic communication devices has diversified, so has the complexity of designing an effective mass notification system. Picking the right system, with the right features, support services and price, can be daunting.

Overview

Emergency notification systems (ENS) have become essential security features in higher education since the 2007 Virginia Tech shooting. In that incident, some believe the two-hour gap between the dorm killing and the classroom massacre provided a missed opportunity to warn the entire campus. At the time, the school was reviewing the 3n Instacom™ emergency notification system, which they quickly implemented thereafter (this system was used successfully after a stabbing death at Virginia Tech this January). Biola University used the same system to successfully alert students when police were pursing armed subjects near off-campus student housing. Northern Illinois University used its own in-house emergency notification system immediately after a major shooting in February 2008, posting alerts on their website, sending email notifications, and making automated phone calls (but their efforts were of little consequence; although police were on scene in 90 seconds, the killing was over and the shooter committed suicide before they arrived). Northern Illinois has now added text messaging to its system as well.

Most emergency notification systems communicate via multiple electronic devices, such as phone, email, instant messaging, text messaging, fax, BlackBerry®, PDAs, and pagers — the list continues to grow — with the order of delivery to specified groups and devices customized to fit the user's priority list. Similar products come from Intelligent Wireless Solutions, MIR3 (inCampusAlert™ Intelligent Notification™ system), Wide Area Rapid Notification (WARN), and ParentLink. These systems promise to reach thousands of recipients very quickly, often in less than a minute. Vasonatech's Priority Alert Software System (PASS) adds advanced graphics and text messaging capabilities to the usual bevy of devices, displaying emergency guidelines, photos, diagrams, evacuation maps, voice directives and updates on dedicated monitors or reader boards placed throughout campus. Orsus displays an automated security plan at a central monitoring station to walk staff through required actions. Zylaya Emergency Notification System (ZENS) adds radio frequency-based devices to serve as repeaters that track real-time locations of anyone who triggers a portable panic button — including security guards. The end result is similar to what GPS devices offer in outdoor environments. ZENS works indoors equally well, but is applied to a much smaller geographic area—usually one campus. IWSAlertis is a commercial, off-the-shelf (COTS) software solution that uses a schools' existing IP network to tie multiple devices (for example, PA communication, sirens, telephony and text-messaging, desktop computers) into a comprehensive emergency notification system managed through a single, unified console (ATHOC.com).

Prices for these products are steep but are likely to drop with competition. They can quickly send an extraordinary number of customized messages to a multitude of devices. In many cases, the number of devices used can effect costs, so carefully determine the specific devices you most want to send messages to, then compare costs, products, and vendors.

Essential Considerations

Plan for Incoming messages. Before sending an alert, you need to know an emergency is occurring. Verify that your emergency communication center is easily reached 24/7 via redundant systems, starting with phones, email, and radio, and that it can handle the sudden crush of communication that occurs in a crisis. Also integrate duress alarms (both fixed and portable), fire alarms, or in some circumstances chemical, biological, radiological and nuclear (CBRN) and other detection systems. Whoever staffs the center needs to know how to respond when any of these are triggered and how to get help. An emergency response manual should be readily

accessible, both in hard copy and online. An ideal system pulls up instructions on-screen when an alarm is triggered or a call is received.

Plan for power outages. Many disasters come with power disruption. Build in power redundancy and independence. When the grid goes down, the emergency systems are needed more than ever.
Plan to reach everyone. Ultimately, the goal is to get the **right message** to the **right people** at the **right time and place**—which could mean before, after, or during classes, while en route to campus or while on campus, indoors or outdoors.

Send the right message at the right time. Communication needs to be clear, concise and timely. Bells or alarms don't spell out the nature of the threat or fine tune the response. Does everyone know what the second blast of the siren means? Take cover, remain in place, evacuate, or the crisis has passed? Some systems can integrate pre-recorded messages into the existing system, making the instructions clearer. But even with a speaker system, garbled communication can be a problem, rendering messages indecipherable. In addition to making sure the equipment is up to the task, attend to the content. Create templates or boiler-plate messages ahead of time. Messages written on the fly risk basic errors, over-heated rhetoric, or inadvertent omissions.

Automated, recorded or text messages should be time and date-stamped, since their delivery might be delayed for technical reasons, reaching recipients long after circumstances have changed. Some mass communication products include automated message receipt confirmation (confirming, for example, that the recipient has opened an email message).

Audible messages should be short and should be repeated, to account for noise, stress and confusion.

Plan for customized communication. You often will want to send different messages in different formats to different people, simultaneously. The system should be designed for sending by zones or other identifiers, such as emergency responders, staff, or students. Further specialized groups might include disabled students, foreign-language speakers, or campus visitors. To do this, most campuses will need to take a two-tiered approach:

- **Tier One:** The top priority for mass notification is to aggressively communicate without requiring recipients to take any active measures to hear your messages. Examples are sirens, messages over loudspeakers, or text on a large LCD display in a public space where it can't be missed. Options include bell systems, loudspeakers, intercoms, public address systems, bull horns, sirens, strobe lights, visual electronic displays, and broadcasting live or pre-recorded messages. Radio and television announcements are also included if these devices are normally turned on. These options may be split into indoor and outdoor devices.

- **Tier Two:** A parallel mass notification track communicates through personal devices that reach people selectively, one-on-one, such as telephones or e-mail accounts. They allow for a great deal of customization, with tailored messages going to different recipients. The crisis team might get one message while dorm residents get another. Pre-established electronic lists can make this an efficient process. Particular recipients, such as active shooters or other criminal suspects, can be blocked from receiving messages. One weakness with tier two devices is that they require recipients to actively receive messages, such as check their e-mail or answer the phone. A second weakness is that mass distribution of electronic messages can overload a distribution system. A formal agreement between the mass notification host and phone service providers is essential to make this work. For efficient delivery of messages, an aggregator, such as VeriSign or Sybase, can parcel out automated messages to multiple carriers simultaneously. Arranging for multiple aggregators provides backup in case one fails. Tier two devices include cell phones, conventional phones, email, fax machines, hotlines, network pop-ups, pagers, social networking sites, portable radios, text messaging, TTY phones for the hearing impaired, weather radios, and web pages.

If it works, don't fix it immediately. If you're satisfied with your existing system, there's no need to throw it out and start over. At the same time, you may want to augment what you've got. Keep an eye to the future. Will the existing system be able to keep up with changing needs for capacity, integration of new features, or new technology platforms? Will you be expecting more out of your mass notification system? Technological improvements are occurring at such a rapid pace that waiting often pays off, as better options become available. Areas that can only be reached with hard wiring, for example, are likely to be reachable in the future using wireless devices.

Ideal systems should be modular and scalable, meaning you can add new devices and expand capacity in the future, building on the same core equipment and software. Wireless transceivers can be attached to many

existing devices to tie them into new high-tech systems, saving on costs. Even if your existing system works, it may be highly vulnerable, dependent on fragile, aging or non-replaceable parts. Software and technology platforms can become obsolete, posing similar risks of system failure. If a particular part dies, does the entire system crash? If this sounds like your system, upgrade decisions should be made with some urgency.

If it doesn't work, do you repair or replace it? Diagnose before you treat. One university, for example, has an archaic phone system that's dysfunctional for the E911 location identification system. Research is needed in order to determine whether software or hardware solutions will be most cost-effective. Sometimes dysfunctions are due to poor installation and can be addressed with simple repairs or by refresher training on the proper use of equipment. In other cases, new technology may be able to overcome old hardware weaknesses.

Have a back-up plan. Any single component, regardless of its sophistication, is vulnerable to catastrophic failure. Hurricane Katrina disabled over three million phone lines. Murphy's Law says that if something can go wrong it will go wrong, and if there's ever a time that's likely to happen it's during a crisis. Or the crisis simply may occur in the midst of down time due to routine maintenance and repair. Plan for this by installing redundant, independent components or by including non-technological response options in your crisis plans. Mesh networks and similarly redundant arrangements are self-healing—if one path is disabled, the message will automatically be re-routed around it. Hopping between multiple frequencies similarly avoids disruption—if one frequency is jammed, another may work. IP-based systems can be designed to be accessible from multiple locations, including off-site, an advantage if the primary base station is incapacitated or inaccessible. Not only are backup data tapes good precautions, but backup servers need to be available in locations not likely to be hit by the same disaster, such as in other counties or even other states. Be prepared to physically remove servers and reconfigure them in new locations.

Carnegie Mellon University has installed a mesh network that relies on wall-mounted units around the campus. These units include call buttons, text messaging, lights, sirens and voice capability, and can send messages to a variety of portable devices. Jackson State recently tested the "Transmission Alternatives Link Kit (TALK) box, a "Swiss Army knife" type device that can tie together all the surviving components after a major disaster knocks out towers or other equipment, and make them functional and interoperable, including across frequencies. The TALK box uses any remaining communication infrastructure for routing, ranging from networks to landlines to satellites, with a simple graphic user interface (www.teleusa.com).

Research your options before selecting an integrator and system. Visit and communicate with other campuses to see what they've done, who they've hired, and how satisfied they are with the end results. How reliable are various providers? What happens if components die? How quickly are they replaced? What if a manufacturer goes out of business? Will the integrator find an alternative? See the NCEF publication, *Selecting Security Technology Providers*.

Paying for the system. Mass notification systems represent major investments. To cover or defray costs, consider the following:

- Build costs into your core budget and look for support from private and public sources. Investigate grant funds available, such as those listed in the FEMA-funded Responder Knowledge Base, www.rkb.us, which tracks potential funding sources for emergency response groups. The U.S. House of Representatives passed a bill in the summer of 2008 requiring colleges to immediately notify students and employees about emergencies that occur on campus and establishing a federal grant program to improve emergency notification systems. It remains to be seen whether this will make it through the legislative process and be signed into law.

- Look into partnership opportunities. Colleges and universities with relevant academic programs may be able to partner with commercial enterprises to develop and test new technology on campus, a win-win arrangement that can potentially reduce costs. The caveat here is to make sure it works. If new equipment fails in a crisis, you don't want to be in the awkward position of explaining why you weren't using equipment that was tried and true.

- Look for ways to integrate existing equipment into a new, more comprehensive system. While starting with a clean slate is sometimes best, that's not always the most cost-efficient approach. Explore your options.

Registration. Opt-out systems will keep more people connected than will opt-in systems. With the opt-out approach, participation is normally required unless a student specifically chooses to opt out. Western Kentucky University asks students to enter emergency contact information as part of registration each

semester. Florida State University uses an opt-out approach, and has an 85% participation rate; UCLA's Bruin alert system encourages students to register their cell phones, with only a 35% success rate). All phone numbers, email addresses, etc., are captured as part of registration or hiring. Make it as easy as possible for students and staff to update information directly on-line, and consider providing incentives or rewards. Send reminders twice annually to update information. Flag cancelled contact information for timely follow-up. Establish a base-line for required devices and allow for additional devices if possible. Whether using an opt-in or opt-out system, be careful not to abuse it. If students sign up for emergency notifications and instead start receiving what they consider spam, participation may flag.

Testing. Once a system is in place, use it regularly enough to be comfortable with it, but don't go overboard. If it is over-used for non-emergencies, it may be ignored; if it is under-used, people may not remember to check it. Weather closures and severe weather warnings provide good opportunities to test systems. While testing a delivery system with a small sampling of recipients can serve some purposes, massive distribution is essential to test a system's capacity. One of the most common shortcomings has been system overload leading to a delay in message distribution. Vendors may provide a product that sends messages to carriers, but what happens next varies considerably. Some systems include a feedback function to determine whether a message has been received. Verify that your local service providers can handle the huge volume efficiently, and that messages won't be screened out as spam. In addition to testing the devices, it's important to practice crisis scenarios. Determine, for example, who has the authority to issue alerts, and practice scenarios where a major player is not available. A decision tree may be needed. The system must make it realistic to issue alerts in a timely manner, and too much bureaucracy will work against that.

Notification Devices: Pros and Cons

Bell system. *Pros:* Already installed in many cases. *Cons:* Very limited message, requires training for students and staff to know how to respond. If already in place, bells can be integrated into a more comprehensive system.

Call boxes with panic buttons. *Pros:* If already in place may be able to retrofit with strobes, cameras, speakers for outgoing messages, and electronic message boards. In-coming messages from the field can help keep security staff apprised of developments; one model even provides an option of including an on-board electronic defibrillator for treating heart attacks. *Cons*: Sound quality can be garbled. Call boxes on some campuses often generate nuisance prank calls that waste officer time, although cameras can help discourage this misbehavior and identify offenders.

Cell phones. *Pros:* Widespread use, can reach users quickly, can be broken into multiple carrier distribution lists to avoid overload. Some colleges have stopped installing land-line phones in dorms, and are instead establishing their own cell phone businesses in partnership with providers. The phones can include text message capabilities and be used for all kinds of information, from class schedules to weather warnings (see **Text Messaging**, below.) *Cons:* Can be turned off, some people don't have them, a data base is required for mass use. Wireless transmissions can be disrupted by steel structural components. Check the reception in all buildings, and consider installing repeaters to mitigate this weakness where it exists.

Conventional phones. *Pros:* May be already in place. Auto-dialers can reach large numbers quickly. Some software now on the market transforms campus phones into loud speakers and ties a variety of communication options into one platform.(Alcatel-Lucent OmniPCX Enterprise telephony network/Safe Campus). *Cons:* Can be unanswered or ignored. Can overload systems. Updated database required for mass distribution to individuals' phones. Students much more likely to use mobile devices.

Email. *Pros:* Potential for quick mass message distribution. Broad coverage with opt-out system or mandatory opt-in. Can be grouped by priority to mitigate overload. *Cons:* System can delay, overload, or screen out as spam. Requires timely viewing of email. Students often have multiple accounts, not just university-issued ones, so all accounts must be listed.

Fax and network printers. *Pros:* Can send to pre-programmed numbers. Minimal cost if already wired. *Cons*: Requires timely viewing, so it must be time and date stamped.

Hotlines and 800 numbers. *Pros:* Can use recorded, consistent message for callers or serve as clearinghouse for incoming information, or both. Can take some of the load off of other lines that need to be kept clear. *Cons:* Can overload.

Intercoms. *Pros:* May already be in place, and can be tied into a more sophisticated system with the use of transceivers.

Low technology. *Pros*: May serve you best when all else fails, and at minimal cost. Flashlights, glow sticks, glow strips for way-finding, flags, and hand signals have all proven worthwhile, *Cons:* Require charged flashlight batteries and training on visual codes for maximum effectiveness.

Portable loudspeakers and bull horns. *Pros:* Low tech. Location flexibility. Can be battery operated. *Cons:* Sound quality can be garbled. Someone needs to be in charge of keeping fresh batteries available.

Network pop-ups. *Pros:* Can reach all networked active monitors without throughput issues. *Cons:* May not reach non-networked, unattended or inactive monitors.

Pagers. *Pros:* Reach all users quickly. *Cons:* Limited messages, largely displaced by cell phones.

Posters. *Pros:* Very low tech, inexpensive. *Cons:* Labor intensive, logistically complicated distribution, weak on timeliness, very quickly out of date and counterproductive unless time-stamped.

Public address system. *Pros:* May already be in place and can be integrated into a more sophisticated system using transceivers. Systems are available with high clarity over long distances (1/4 mile per speaker). *Cons:* Often have poor sound quality.

Radios (handheld portables, for staff.) *Pros:* Great back-up devices when other systems collapse. *Cons:* Limited battery life requires supply of batteries, solar chargers, etc. Users require basic familiarity and training. Must test radio range ahead of time to identify any dead spots on campus and install repeaters to remedy them. Radios must be programmed to the same frequencies in order to talk to each other, and these frequencies must be coordinated with local emergency responders. Digital radios were initially adopted with great enthusiasm, only to run into "vocoder" intelligibility problems. Vocoder systems enhance the loudest sounds and cover the others, which has led to serious problems at fire scenes when sirens or emergency equipment noises drown out speech. As a result, many departments are staying with analog radios until the technological issues are sorted out.

Radio announcements. *Pros:* Uses existing public radio stations at no cost to institution. Saturates area; if people know there's a crisis, they'll often turn to radio news for updates. *Cons:* Relies on people listening. Cannot be limited to a select audience.

Satellite phones. *Pros:* Independent from terrestrial systems, such as cell towers or landlines. *Cons:* Expensive and require unblocked view of the sky.

Security staff and runners. *Pros:* When technology isn't an option, security staff and resident assistants running messages, knocking on and locking doors may be what's left to work with. *Cons:* Requires a system to alert security staff to report for duty. They must know how to communicate with flags or hand signals from a distance.

Sirens. *Pros:* Widespread, quick alarm. Can be integrated into a more sophisticated system. *Cons:* Sirens don't spell out the specific emergency or identify the recommended actions to take, which may confuse recipients (for example, do they evacuate or take shelter?).

Social networking websites. *Pros:* Used widely. Work for the hearing impaired. A strength of Facebook © is that it's University-based; if a University wants to send an emergency message to all of its students who subscribe to Facebook ©, it can readily do so. *Cons:* Students must have computers, have access to the Internet, and know to check the site. Other social network sites, such as My Space © or Bebo ©, are generally not University-based. In these cases, mass distribution would be overly problematic, requiring the school to establish a group within the network which the students would have to join. Wiki, Twiki, and Twitter are networking mechanisms taken in a more collaborative direction. All subscribers can contribute to and steer a conversation, usually around a common theme. A "tweet", or short query, is posted to a twitter group, and anyone subscribing can respond. A school security tweet might be "Does anybody have a suggestion for someone in California to install our cameras?", but it could just as easily be "Where's a great Chinese restaurant?"

Opt-in systems such as Pacific University's e2Campus™ system empower the school to send messages to a wide variety of devices and services through a single source; an administrator can log in to the e2Campus™ web site and send one message that works as an email, text message, RSS feed, Facebook, and Twitter entry.

Strobe lights. *Pros:* Can be merged with many other devices to reach hearing-impaired. Can be integrated into a more sophisticated system. *Cons:* Like sirens, do not state the emergency or the actions to take.

Text messaging (SMS, or "short message service", to cell phones, PDA's, Blackberrys ©, etc.). *Pros:* Very effective for reaching college students. Can be broken into multiple carrier distribution lists to avoid overload. Can receive optional automated feeds, such as weather, traffic or news alerts. During major disasters, text messaging has worked when phones did not due to much smaller band width requirements. If Wi-fi enabled, cell phones can move more data effectively, making multi-media options more workable (www.wi-fi.org). Recent innovations include a free community information and emergency text messaging service (www.nixle.com) and tip411, a text messaging anonymous tip line application (www.citizenobserver.com) *Cons:* Ongoing database management is necessary. Systems can overload, towers can fall, service can be cost-prohibitive. Although generally very popular among students, texting can incur additional charges for both the sender and the recipient (see **Cell phones**, above).

TTY phones for hearing impaired. *Pros:* Provide means of communication for hearing impaired, should supplement hotlines. *Cons:* Require staffing.

TV announcements. *Pros:* Uses existing television stations at no cost to institution. Can be both visual and auditory. Saturates area; if people are aware of a crisis they'll often turn to TV news for information. *Cons:* Relies on people viewing the correct station. Cannot be limited to a select audience.

Visual (LCD) electronic displays in public spaces. *Pros*: Great for widespread use. No sign-up or data base required. No service charge. Can reach pre-determined locations with reasonable certainty. Can reach hearing impaired. Can be used for non-emergencies. Can be integrated into a more sophisticated system using transceivers. Newer LCD screens use LED backlights for major improvements in energy efficiency, longevity. and brightness. Loyola installed 30 screens in key indoor locations throughout campus — such as near elevators, entrances and lobbies (www.digisign.net). They are used for a variety of messages, but emergencies take priority. Services such as RoomView® remote help desk (www.crestron.com) allow users to send messages to any text type device on a campus network, including whiteboards, projectors and displays, customized for a single room or broadcast across campus.

Voice evacuation recordings. *Pros:* Often part of fire alarm systems and may be expanded for other emergency uses. Can be integrated into a more sophisticated system. *Cons:* Sound can be garbled.

Public alert (weather) radios. *Pros:* Reliable for public alert and weather-related information. Can be automated. *Cons:* May not offer sufficiently campus-specific guidance.

Web pages. *Pros:* Consistent message. Can be updated and time-stamped. Blogging features can provide a site to which multiple students can send updates during a crisis. This was a role played by the Napa Valley Register's site during a lockdown at Napa Valley College in April, 2009. *Cons:* Risk of overload in a crisis. Offenders can see site. Requires students to check the website.

Related Resources

U.S. Department of Education, Office of Safe and Drug-Free Schools:

- *Practical Information on Crisis Planning: A Guide for Schools and Communities*, http://www.ed.gov/admins/lead/safety/emergencyplan/crisisplanning.pdf

National Clearinghouse for Educational Facilities (NCEF):

- *Mitigating Hazards in School Facilities*. Includes assessment, planning, funding techniques, and links to 25 NCEF Assessment Guides, http://www.ncef.org/pubs/mitigating_hazards.pdf
- *School Security Technologies*, http://www.ncef.org/pubs/security_technologies.pdf
- *Selecting Security Technology Providers,* http://www.ncef.org/pubs/providers.pdf
- NCEF resource list, *Campus Safety and Security*, http://www.ncef.org/rl/safety_securityHE.cfm

Public Alert Radios. NOAA Weather Radio All Hazards is a nationwide network of radio stations broadcasting all-hazards information 24 hours a day, 7 days a week. Broadcasts include alerts and safety steps for a wide range of emergencies and natural hazards, http://www.crh.noaa.gov/Image/lot/nwr/NWR-FactSheet.pdf

Publication Notes

First published October 2008; updated January 2009, April 2009, July 2009, October 2009. William Brenner, editor.