

Mass Notification Systems in Higher Education

Introduction

A fire erupts in the Student Union cafeteria. A water main breaks, forcing an institute of higher education to shut down the campus and cancel classes. A crime suspect on the loose on school grounds puts everybody on campus in danger.

Recent history shows these emergencies can and do happen. And they require swift action by administrators at higher education institutions to protect students, faculty and staff from immediate threats to their safety. Every second is critical. Administrators must alert the campus population with real-time information and instructions on what they should do, as well as provide off-campus first responders with the information that they need to help ensure a safe resolution.

Technology plays a pivotal role. A mass notification system, which links an institution's communications and technology infrastructure with a comprehensive emergency response strategy, can save lives. When an emergency strikes, these systems allow officials to immediately notify everyone on campus through phone calls, e-mails, text messages, instant messages, loudspeakers or flat-panel displays. If students are off campus but on their way to school, notifications can warn them to stay away.

The need for mass notification systems was made apparent after the attacks of Sept. 11, 2001, when the communications system failed in New York, hampering the ability of firefighters and police officers to save lives. In response, the Department of Defense directed all of its facilities to install mass notification systems. Today, much of the public and private sector are following suit. According to a study by research firm Gartner, 75 percent of Global 2,000 companies in the world will deploy mass notification systems by the end of 2007.



"We need to reach everyone we can as fast as we can and give them enough information to keep them out of harm's way," says William Sako, chairman of security consulting firm Sako & Associates and senior vice president of Rolf Jensen & Associates.

Many higher education institutions have been evaluating, purchasing or installing mass notification systems while others have recently reviewed their security strategies and explored improvements to their emergency notification procedures.

In this white paper, security consultants, industry analysts and mass notification system vendors discuss how best to choose, install and manage a mass notification system.

Specifically, this white paper will explain:

1. What is a mass notification system? A look at how the technology works, its benefits, a federal law that requires timely notifications, and return on investment (ROI);
2. How to purchase the right system. A look at choosing in-house versus hosted (outsourced) solutions, the key features to seek and the right questions to ask while evaluating systems;
3. Details of mass notification systems available from CDW•G;
4. Strategies for deploying a successful mass notification system.

What is a Mass Notification System?

Effective communication during emergencies is essential. Mass notification systems typically use existing data and voice networks to deliver pre-recorded or live messages that alert students, faculty and employees of emergencies and provide them with instructions, such as evacuating a building or going to pre-assigned rooms that serve as shelters.

A comprehensive mass notification system typically allows administrators and campus fire and police to immediately contact every faculty

member, staff member and student through phone calls, text messages (also known as short message services, or SMS), instant messages, e-mails and other alerts on the following devices:

- Internet Protocol-based phones
- Traditional analog and digital phones
- Desktop and notebook computers
- Mobile phones, personal digital assistants and BlackBerry devices
- Fax machines and pagers

In addition, mass notification systems can broadcast messages throughout campus, indoors and outdoors through:

- Loudspeakers or paging systems
- Digital signage, such as LCD or plasma screens in buildings and throughout campus (This is an important form of communication particularly for the deaf and hard of hearing)
- Sirens or alarms

Institutions may also want to install video surveillance cameras to augment a mass notification system. "You need to see and hear what's going on and evaluate the situation before you make a decision to evacuate people or tell people to duck and cover," Sako explains.

Video cameras can work as a standalone system separate from a mass notification system. But linking the video cameras to a mass notification system has its benefits. For example, some camera systems offer add-on technology that analyzes sounds and video, and notifies campus police if it detects gunshots or other dangerous activity.

The Law Requires Timely Notifications

Today, a federal law requires higher education institutions to provide timely information about crimes on campus, and new legislation requiring timely information about all campus emergencies could soon be on its way.

The Clery Act, enacted in 1990, requires that institutions receiving federal Title IV student financial aid funds to provide the campus population with timely warnings of crimes that are threats to students and employees.

In late April, Sen. Dick Durbin (D-Ill.) introduced legislation, called the Campus Law Enforcement Emergency Response Act of 2007, which would require all institutions to develop and distribute policies for law enforcement emergencies, including procedures for notifying students and employees. The proposal would require administrators to notify the campus community of an emergency within 30 minutes of its discovery and for campuses to test their emergency response procedures annually. It would also provide the Department of Education an initial \$5 million allocation to provide grants to fund security initiatives.

Other Benefits

In addition to crime alerts, mass notification systems can warn people of severe weather, such as tornados or hurricanes; class cancellations because of a power failure, a gas line or water main break, or other utility problems; and biological and radiological accidents, or other hazardous spills.

While mass notification systems are geared toward emergencies, they can also be used as a communication tool for non-emergency situations that can improve employee productivity and simplify everyday tasks. Some uses include:

- Allowing individuals on campus, such as department chairs, to notify faculty members of a change in a meeting place or time;
- Professors can tell students via e-mail or through text messages that class will be held at the quad instead of the classroom;
- Administrators can warn students that they are late in paying their tuition.

Calculating ROI

ROI is hard to quantify because you can't place a value on saving lives. If institutions deploy the systems for non-emergencies, such as reminding staff members of meetings, then they can get a bigger ROI, says analyst Michael Osterman of Osterman Research.

"You don't want to bombard people with messages, but if you use it the right way, such as reminding students of tuition payments or anything that makes the college run more

efficiently, then you can have real benefits," Osterman says.

Implementing one mass notification system can also save money to implement, upgrade and manage rather than using a series of standalone systems.

Purchasing the Right System

With dozens of vendors to choose from, it's a daunting task to know where to start. During the request for proposal and evaluation process, higher education officials and information technology administrators must examine two key factors — system architecture and the features available — and ask the right questions to determine the best fit.

Architecture: In-house Versus Hosted Solutions

Mass notification systems come in two varieties: in-house systems that institutions install and manage themselves, and hosted Web-based solutions.

An in-house system is typically server-based software that ties into an institution's PBX or IP telephony phone systems, allowing them to broadcast messages over a phone system or Web page. Some systems require IP-based phones, while others support analog and digital phones.

An in-house system offers IT departments more control, including the ability to more easily customize features and tightly integrate with the rest of the institution's technology infrastructure. But it also requires institutions to have the IT staff, expertise and budget to install and maintain the system. Such a project could require the purchase of new servers and a network upgrade to ensure reliability, uptime and good performance.

A hosted solution requires fewer upfront costs and leaves the headache of managing a mass notification system to the vendor. But in doing so, IT departments have less control.

Hosted systems typically offer several pricing options, including monthly or yearly subscriptions

The Role of TV and Radio

Institutional TV or radio stations can be part of a mass notification system, but don't assume everyone on campus is tuned into those channels, says Joe St. Sauver, a professional active in the higher education security community at the University of Oregon.

However, a voice message or SMS can instruct recipients to turn on a campus TV or radio station for more detailed information as an incident unfolds.

based on the number of users or how often the system is used.

“The architecture should really be determined by institutional requirements, and the choices you’ve made about things like how you want to notify users, what you need to tell them, and how quickly they need to be told,” says Joe St. Sauver, a professional active in the higher education security community at the University of Oregon.

St. Sauver notes that institutions need to examine three issues when deciding between in-house and hosted solutions: the cost of developing the capabilities in house versus the cost of subscribing to an outsourced solution; the expertise of the institution’s staff and whether other projects would compete for their time; and the fit between an institution’s requirements with off-the-shelf hosted offerings.

A hosted service is good if institutions have a small IT staff. But institutions with large IT departments that can handle the workload are better off installing and managing it themselves because they can more easily customize a solution to their needs, Sako says.

Institutions that choose hosted solutions may face limitations if they want to interface the hosted service with their campus technology because the vendor may not have the expertise to do the integration, Sako warns. Those that choose the hosted route need to ensure that their vendors offer good customer and technical support and ensure uptime 24 x 7, 365 days a year.

“Do what you can afford,” Sako advises.

Features to Consider

Here are some key features that mass notification systems should offer:

- Flexibility in activating the system and sending a notification. Mass notification systems should allow administrators to use different devices, such as a campus phone or password-protected Web page, to activate the system and send a message. Some systems even allow administrators to activate the system through their PDAs or cell phones.

- Support for multiple forms of communication. For major emergencies, campus administrators need the ability to blast a message using all forms of communication, including phone calls, e-mails and text messages, to multiple communications devices simultaneously. However, St. Sauver warns that overloading critical emergency communication systems at a key time is a possibility.

“If you can identify failures as they occur, you may be able to selectively employ redundant communication channels, particularly for high priority notification targets, thereby ensuring your message makes it through, but in a way that does not contribute to overloading communication systems,” he says.

- Providing different administrative rights to users. Institutions can give their presidents and senior-level staff full access, allowing them to send notifications to everyone on campus. But institutions can limit access to others, for example, allowing department heads to send messages to people in their departments.
- Support for multiple contact lists. A mass notification system isn’t effective unless institutions can create and maintain updated contact lists. A good system will let administrators create an unlimited number of contact lists for every need. For a campuswide emergency, the contact list should include everyone at the school. For specific needs or isolated issues, contact lists can include just the IT department, people responsible for specific facilities or the school’s emergency response team.

- Reporting tools. The system can generate reports, tracking how many people the system contacted and on what devices. Some tools track successful transmission of the messages and the amount of time the notification process took from start to finish. Some tools also allow administrators to monitor the progress of a notification in real time.

Other Important Questions to Ask

It’s also helpful to ask the following questions:

- How long does it take to activate the system?
- Does it provide indoor and outdoor coverage?

- Is the system scalable and customizable?
- Is it compatible with your hardware, operating system and in-house phone system?
- How much does it cost to implement and maintain?
- How much technical expertise is needed to manage and maintain the hardware, software and network?
- Is it easy to integrate with other parts of your disaster recovery and business continuity strategy?
- How do you secure your list of contacts?
- Is it easy to update the contacts database and can you add contacts located outside the institution?

CDW•G's Offerings

CDW•G provides mass notification systems from CDW Berbee, Computer Instruments and Roam Secure. CDW Berbee offers the InformaCast system, which is tightly integrated with Cisco's Voice over Internet Protocol equipment, including IP phones. Computer Instruments' e-IVR software supports Avaya and ShoreTel's IP telephony equipment, as well as traditional analog connectivity to most PBX platforms. The Roam Secure Alert Network (RSAN) provides text-based emergency alerts.

Here's a closer look at the vendors' offerings:

CDW Berbee's InformaCast System

The InformaCast system, originally built for the Department of Commerce following the Sept. 11 attacks, is a highly scalable and customizable server-based software solution that allows institutions to simultaneously send audio and text messages to any combination of Cisco IP phones, computers or the company's own IP-based loudspeakers. CDW Berbee also recently added support for SMS text messages to cell phones and PDAs.

Users can send live, pre-recorded or scheduled broadcasts to one or more groups of contacts through a password-protected Web page or an IP phone's menu, says Ken Bywaters, CDW Berbee's director of voice products. School employees can receive the messages, either as an audio message on their PCs or IP phones, or as a text message

that pops up on their PC or the menu window of their IP phones.

The advantage of the InformaCast system is that it is IP-based. The audio and text messages travel on the local area network, allowing institutions to send critical emergency notifications to every campus location on the network, including satellite campus locations.

In addition, the InformaCast system's architecture takes up very little bandwidth and does not overwhelm the converged voice and data network. The audio messages are sent via multicast and are not actual phone calls on the public switched phone network. If administrators send one audio or text message to phones and PCs, that one message takes up the same amount of bandwidth, whether the message is sent to two devices or 2,000 devices.

In contrast, with other solutions that send actual phone calls, traditional phone lines can become overloaded and go down, Bywaters warns.

The InformaCast system encompasses three pieces:

- **InformaCast IP Broadcasting Solution.** Server software for mass notification. It requires at a minimum a Windows 2000 or Windows 2003 server running on a 2.5 gigahertz Pentium-class processor and 1 gigabyte of RAM. It also requires Cisco Unified Communications Manager, formerly called CallManager, an IP-PBX that routes and manages phone calls over the network. The software is compatible with most Cisco 7900 series IP phones. The InformaCast system automatically pulls phone information from the Cisco Unified Communications Manager to create paging zones, which are different groups of people to send messages to.
- **InformaCast Desktop Agent.** Software installed on users' computers to receive audio and text messages. The agent plays the audio on the computer, while text messages pop up on the screen — a communications tool that is more immediate than e-mail.
- **InformaCast Compliant IP Speaker.** Easy-to-install loudspeaker systems for indoors and outdoors. The speakers, manufactured by

Stay Up to Date

Contact lists should include people's e-mail addresses, all their phone numbers and location information, including class schedules, classroom locations and home and work addresses.

To get students to give their updated contact information, make it part of the class registration process or part of logging in when they want to go to faculty Web sites to download homework assignments, says William Sako, chairman of security consulting firm Sako & Associates and senior vice president of Rolf Jensen & Associates.

Atlas Sound, support Power-over-Ethernet connections and require only a RJ-45 connector to connect to the data network. (The system also allows institutions to connect non-IP speakers using a connector called Zone Controller Hardware.)

CDW Berbee offers a PushToTalk application for Cisco's IP desktop and wireless phones, which allows two employees, or a large group of employees, to turn their phones into a virtual walkie-talkie. "You can hit a button to talk to everyone in the security department in multiple locations and say, 'Have you seen a person in a black windbreaker?' and you're not burdening the phone system," Bywaters says.

Another benefit is that users can receive an emergency notification, even if they're talking on an IP phone. The technology allows administrators the option of forcing users to hear the emergency audio notification, even while they're talking on the phone.

The InformaCast system is best suited for employees, but can also be used to alert students by having them install the InformaCast Desktop Agent, Bywaters says.

CDW Berbee can customize the InformaCast system to meet any requirement that institutions may have. For example, if an institution wants to include the ability to send text messages to students' cell phones, the CDW Berbee staff can customize that functionality into the solution. CDW Berbee also supports integration with Axis surveillance cameras. If administrators want to tie a video surveillance system with the InformaCast system, the CDW Berbee staff can write a custom application that tells all video cameras to point to the direction of an incident once the mass notification system is triggered.

"It's software, so we can offer a high level of flexibility to meet customers' needs," Bywaters says.

The InformaCast system, which can be installed quickly and easily, can scale to meet the requirements of higher education institutions of all sizes. A server with a minimum configuration of a 2.5GHz processor and 1GB of RAM can immediately send notifications to 10,000 devices. The speed of the notifications depends on the

speed of the network, but in typical cases, notifications to 10,000 devices will take less than one minute.

Computer Instruments' e-IVR Software

Computer Instruments' e-IVR Emergency Response system is customizable server-based software that allows school officials to make phone calls and send text messages and e-mails to faculty, staff and students through multiple devices, such as landline phones, cell phones, PDAs and PCs. The software can also send pop-up messages to premise-based PCs located throughout a campus wide area network.

Administrators can send notifications through a password-protected Web site, or through a PDA, or any landline phone or mobile phone. "You can just call in, put in your extension and password, and the e-IVR system authenticates you to access the system," says Brandon Herring, the company's director of sales.

The system, which runs on Windows, gives users the flexibility to send messages on the fly using "text to speech," or through pre-recorded voice messages or pre-written messages. With the text-to-speech feature, an administrator can type a message, and the e-IVR software, through a robotic voice, reads the message when people pick up their phones. The text-to-speech feature can support multiple languages, so administrators can type a message in Spanish, and the application will read the message in Spanish.

The e-IVR software is also programmable, allowing individual users to prioritize how they may be reached, whether it's through a phone call to their work phone or a text message to their cell phone first. But if it's a major emergency, administrators can simply dispatch an alert to every person's device using all forms of messaging, including phone calls, e-mails, text messages and numeric paging. Administrators can use e-IVR to send notifications to specific groups of people on campus.

If phone calls are unsuccessful because of a busy signal, the system will retry the phone number up to three times, or if voicemail picks up, the system will leave a message. In addition,

the system can ensure successful delivery of a phone call by asking people to press "1" to acknowledge that they received the message.

Contact lists, featuring people's phone numbers and e-mail addresses, can be easily created and updated. Institutions can direct everyone on campus to log onto a Web page to input their contact information, or they can send e-mails to everyone and have them respond with their contact information. Administrators can also add the contact information for people off campus, such as first responders.

A contact list can be housed on a spreadsheet and imported into the e-IVR software. Computer Instruments can also customize contact lists and store them in a secure SQL server database or in Active Directory, where people's e-mail addresses are already stored, Herring says.

The e-IVR system is highly scalable. As part of the mass notification system, Computer Instruments provides Intel-based servers that support up to 384 ports, meaning one server can make calls to up to 384 phones simultaneously. The server — powered by dual Intel Xeon processors — features dual power supplies and RAID 5 (redundant array of independent disks) hard drives to help ensure availability, reliability and redundancy.

If an institution sends a 10-second message through a 384-port server, the mass notification system will be able to make nearly 14,000 calls in 15 minutes or nearly 28,000 calls in 30 minutes, while the system is simultaneously sending text messages and e-mails. Institutions can also cluster several 384-port servers together, resulting in faster notifications.

The e-IVR system tracks message delivery with detailed reports, including whether people received the messages. It also allows users to monitor in real time the progress of a notification being broadcast, Herring says.

Computer Instruments also makes its e-IVR mass notification system available as an outsourced, managed service. The company charges a per-port monthly fee, as well as extra fees for add-on features, such as text-to-speech capability.

Both CDW Berbee and Computer Instruments offer different administrative rights, meaning senior staff can have full access to send notifications to everyone, while others are limited to smaller groups on campus.

Roam Secure's RSAN

RSAN is another software-based system that sends text alerts to many types of devices. It uses SMS to reach cell phones, e-mail accounts, PDAs, BlackBerrys, Treos, satellite phones and XM Satellite radios. Roam Secure says its network works with any SMS device and can send 18,000 messages per minute/per server running the software.

A designated RSAN administrator on campus can send alerts from a computer, cell phone or other wireless device to everyone registered on the network. Messages can be scripted or written ad-hoc.

Message recipients on the network can register multiple devices or e-mail accounts, with the limits set by the RSAN administrator. They register online by sending a text message.

RSAN also supports two-way communication. That means recipients can respond to messages, allowing them to provide vital information in case of an emergency. RSAN stores messages and responses in a Web-based application, creating a summary and audit trail.

Roam Secure can be deployed in-house or as a hosted solution in redundant geographically dispersed data centers. The vendor offers consulting services for implementation, maintenance, training and testing. It also offers a system tuneup for in-house systems, which includes a database integrity check, database scrub for invalid addresses, system performance testing and optimization.

Campuses using RSAN can also tie into the Roam Secure Information Exchange. RSIX lets institutions link to other RSAN systems off campus, even in other parts of the country. Security staffs can share information and resources via RSIX. The RSIX community includes local and state government first responders in several metropolitan regions.

Remember to Test

Institutions must also test their emergency warning system quarterly. "Test the whole campus, not just pieces of it. You need to find out if the stuff works and the only way to do that is to test everything," says William Sako, chairman of security consulting firm Sako & Associates and senior vice president of Rolf Jensen & Associates.

Digital Signage

CDW•G sells plasma and LCD screens that can be used as part of a mass notification system. Sony offers 32-inch to 50-inch displays. Administrators can use networking cards to connect the displays to the LAN, which allows them to centrally manage and broadcast messages onto the screens.

Samsung offers 40-inch and 46-inch displays with built-in mini computers running Windows XP Embedded. Administrators can link the displays to the LAN, and broadcast messages — including scrolling messages across the display — through Samsung's MagicNet software.

Video Surveillance Cameras

Axis Communications provides two dozen IP-based indoor and outdoor video surveillance cameras that institutions can easily install on their networks. Through a Web browser or software, campus administrators and off-campus law enforcement can track individuals moving throughout campus and react to situations more quickly and accurately.

Administrators can also print photos from the network cameras and use a mass notification system to send pictures of crime suspects for possible identification.

Features of Axis network cameras include motion detection sensors, wide-angle lenses and the ability to pan, tilt and zoom. PTZ dome cameras, which are good for parking lots, athletic fields and building perimeters, offer 360-degree views and up to a 35x optical zoom that allows users to see objects 500 feet away.

Several indoor camera models also support Power over Ethernet, which can save money in installation charges and can provide constant uptime when plugged into a switch that is running on an uninterruptible power supply. Axis also provides network video servers that allow campuses to integrate existing analog closed-circuit TV cameras into their new IP-based surveillance system.

Deployment Strategies

A mass notification system is about more than just technology. Institutions must create detailed emergency preparedness plans. High-level administrators, facilities managers and campus security staff must meet to discuss every possible scenario and how the campus should respond, Sako says. In the process, the institution should create a database of pre-written emergency notification messages, so campus leaders can quickly send notifications when situations arise.

Emergency notification systems need to be carefully engineered to provide a high level of survivability, St. Sauver adds. That means thinking about emergency power, redundant network connectivity and the use of multiple communication channels.

Conclusion

Institutions of higher education are a microcosm of the real world, where crime, disasters and other bad things can happen. Fortunately, advances in technology, particularly in new communications software and tools, allow institutions to build effective mass notification systems that make campuses safer. Today, a mass notification system at the ready can give everyone on campus peace of mind. Tomorrow, it can save lives.

