

The Challenge of Mass Notification on American Campuses

By William Sako



Through the proper application of proven mass notification technology, the frequency and severity of incidents that take lives and cause injuries on a campus can and will be mitigated.

For most of our history, Americans in general have felt relatively safe and isolated from violence as they went about their daily work and leisure activities. Certainly there were inner city areas where higher crime rates produced headlines in daily newspapers and isolated events throughout the country often focused national attention on horrific violence for a few days. But fortunately, most Americans took the position that “it can’t happen here, or to me” and continued on with their lives.

Then came the 1999 shooting spree at Columbine High School in Colorado and in a matter of hours, our illusions about personal safety and security were shattered. If the unthinkable could occur on a high school campus in heartland America, it could happen anywhere, anytime to anyone. When the terrible events of Sept. 11, 2001 confirmed America’s vulnerability to terror and violence, the entire country began an immediate transformation to a much higher state of security awareness.

Nowhere has the concern for personal protection hit home more than on the campuses of our colleges and universities. As security breaches became almost commonplace in virtually every area of the country, officials of public educational institutions, especially those located in gang-infested inner cities, were quick

to add security measures ranging from metal detectors in their lobbies and in-school security forces to police-manned perimeters.

However, the very essence of a college/university campus devoted to higher learning or a bustling corporate business campus is openness. A reality, for better or worse, is that America is an “open society” and the personal freedoms that we enjoy as a society are afforded by that openness. So naturally, there is a resistance to encircling entire widespread,

multi-building campuses with barbed wire fences and armed guards, or forcing people on campus to enter buildings through metal detectors. In the security design profession, we understand that we cannot always prevent incidents from occurring, but it is essential that we possess the capability to respond quickly to mitigate and limit the damage. It is easy to understand why the focus and emphasis is being placed on responding to the mass notification challenge: how to best communicate with all campus occupants in the event of an emergency situation.



The Purpose of Mass Notification

What situations could occur that would require campus officials to be able to communicate with all the people on campus? According to a recent Public Safety Survey conducted over a sampling of public safety officials, the top concern was a natural disaster. Judging from recent hurricanes in the South, tornadoes in the North and East and fires in the West, this concern is well-founded.

The Challenge of Mass Notification on American Campuses

Aside from weather-related emergencies, the threat could involve a security breach, an act of terrorism, a chemical release, a fire, a utility outage or any other type of disruptive event. The purpose of a campus-wide mass notification system is to provide a reliable method for officials to notify people on campus of an emergency event and explain what is happening, what to do, where to go and when it's safe to resume normal activities.

"...in a matter of hours, our illusions about personal safety and security were shattered."

The mass notification system must have the capability to send instructions to people in specific spaces, floors, buildings and facilities throughout the campus, or in some instances, to an entire regional or global network of people. These instructions can be transmitted via loudspeakers, voice-equipped fire alarms systems, public radio/television networks, computers, telephones and cell phones, PDAs, visual display signage and two-way radios.

The Risk and Reward of Technology

The leading-edge technology of mass notification has always resided in the government sector where the risk of security breaches are the highest and the consequences can be the most devastating. Following 9/11, it became apparent that in order to protect ordinary citizens from terrorism and violence, the government's advanced technology needed to be shared with system developers, manufacturers and integrators in the private sector. Under the guidance of the Department of Homeland Security, the government is still the leader in the pioneering and testing of new technology. However, under a presidential order, the government is sharing its lessons learned and technology applications with the private sector. This enables us to be in a much better position to apply leading edge technology to our security and mass notification challenges.

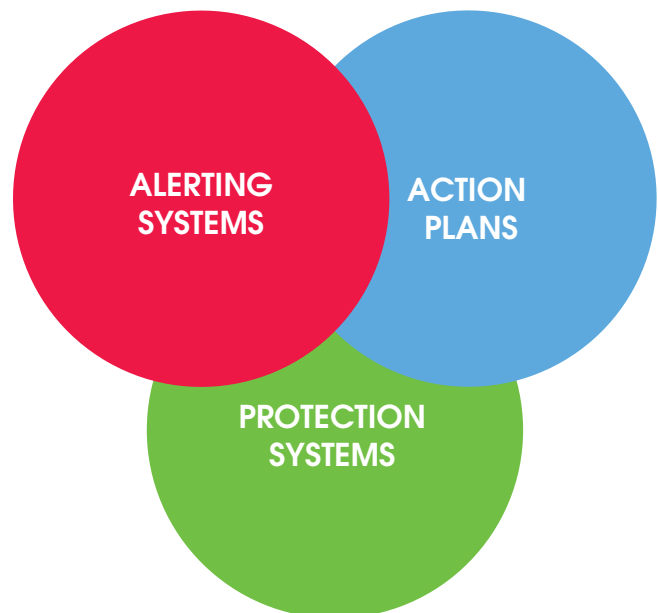
The flood of new security technology into the marketplace has raised the capabilities of mass notification exponentially. New products and systems are hitting the market every day. They're smarter, faster, smaller and less expensive than ever before and thanks to our mass media sophistication, more people know about this never-ending wave of new technology in a shorter period of time.

Complementing this proliferation of mass notification technology is a consumer base with real-world needs. The college/university president wants an immediate security solution that he/she can publicize to the parents of a student in the process of selecting a safe learning environment for their child. The CEO of a private company seeks the same quick fix solution to protect the people who work on a corporate campus whether it's a single building in one location, multiple buildings in a complex or facilities spread across the country or around the world.

It's the perfect storm so to speak, especially in light of recent events on campus. The consumer has a need, the industry has a solution. A typical question being asked by consumers is: "if I have a limited budget for mass notification, what's the one system I should spend it on?" Our answer is always the same: "Rather than investing in hardware, first find a good consultant capable of guiding you through the entire mass notification process and showing you how to assess and leverage the technology that you already have in place."

Unfortunately, in many cases, the top campus official is still intrigued with finding the "magic" system that will guarantee a horrific event will not occur on his/her campus.

An effective mass notification program must balance three design elements



In most cases, you'll find four different types of systems on a modern campus. They include life safety (fire, gas and smoke detection, alarm and sprinkler systems); security (surveillance, access control and intrusion monitoring systems); building automation (HVAC) and communications (voice and data systems). Typically, each of the four system categories falls under a separate jurisdiction.

"...it is essential that we possess the capability to respond quickly to mitigate and limit the damage."

For example, the campus police are responsible for providing a secure environment so the security command center is their turf and they oversee the selection and purchase of any type of security system hardware or software. They may also be responsible for the life safety function, or there could be a separate campus fire protection department in charge. Building automation is most often the domain of a facilities management group while information technology/information management falls under yet another autonomous group.



Each of the groups we mentioned tends to function as a separate "silo." Each has a separate chain of command, their own unique objectives, procedures and dedicated budgets. Ensuring that their systems are compatible with another group's systems is not high on anyone's priority list. They also tend to compete for dollars and human resources allocated in the annual budget.

This is not an ideal situation when the objective is to build a seamless campus-wide mass notification system. That's why this important investigation step

must be taken unilaterally. You'll need to know which systems can be used as part of your mass notification infrastructure, which must be upgraded or removed and what new technology you must add in order to have a fully integrated, enterprise-wide mass notification process.

In addition, you'll want to factor in the creation of a central command center dedicated to integrating all the incoming information and outgoing messages. The security command center, if it exists in proper form, can serve as the central command center for emergency event management. The key to effective management of any emergency situation is having situational awareness of the event. In other words, you need to have visual and informational knowledge of what's taking place in real-time terms. This is critical in a mass notification process where decisions involving people movement must be made in minutes or seconds, not hours.

Step 3: Design and implement your mass notification systems

Once you've completed the investigation step, you now know what improvements or additions must be made to your infrastructure and where these enhancements are most critically required in order to achieve total system integration and interoperability. Since very few campuses can afford to do everything at one time, you'll want to create a phased implementation plan, complete with budget estimates and detailed specifications for every system.

The implementation plan will enable you to compare and obtain competitive bids from leading hardware and software suppliers. Once the bids have been awarded and the construction begun, you'll no doubt require the services of a specialty consultant able to provide on-site project and construction management. The consultant should also be qualified to obtain the necessary code approvals and oversee the installation, testing and commissioning of the life safety, security, communications and IT systems.

The implementation phase also includes training on the systems. This not only involves the people who operate and maintain the systems, but also the people who populate the campus. The systems must respond properly in order to be safe. The system training should be a part of your overall emergency response training program.



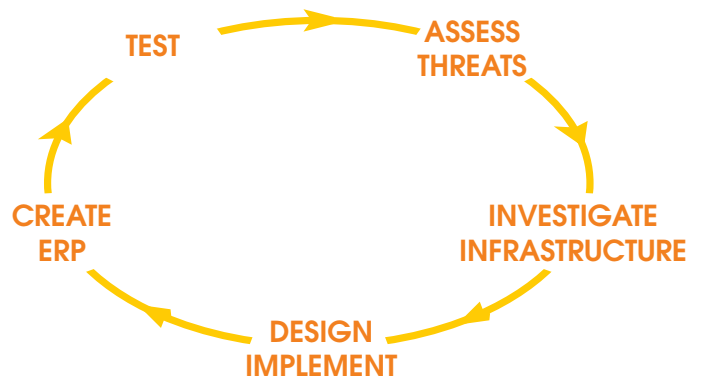
Step 5: Test your operational readiness

In the oil and gas processing industry, they call it keeping their processes “evergreen.” In other words, things change and so must your mass notification process. A campus is a growing, evolving community, from a structural, operational and human standpoint. Therefore, it is necessary to conduct regular periodic tests and evaluations of not only your mass notification process, but also your sub-systems, procedures, emergency response actions and any new threats that may have emerged.

Step 4: Create an emergency response plan

The emergency response plan is the single most important part of the mass notification process. You’ve identified the threats to your campus; created worst-case scenarios; evaluated your systems; and identified the hardware and software issues you need to address. Now it’s time to create a blueprint for how the mass notification process will function in an actual emergency.

The emergency response plan (ERP) identifies your mass notification response team and assigns responsibilities. It determines what messages will be sent in specific situations; where you will instruct people to go; by what routes; to which safe areas. It details evacuation plans and provides for signage to guide your campus occupants to safety.



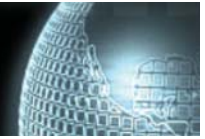
Keeping America’s campuses secure and their occupants safe is a monumental task, not without setbacks. No matter how prepared a campus is, regardless of how well-trained and vigilant the members of the emergency response team are, incidents can and will happen that take lives and cause injuries. But the frequency and severity of these events can and will be mitigated through proper application of proven mass notification technology.

"Effective mass notification is not a single system. It is a process."

The ERP further explains how your ER team will be trained and lays out methods for implementing training activities with different simulated emergency scenarios. It also focuses on the cooperation and synergy required from local government, fire, police, medical and disaster recovery personnel and provides a methodology for accomplishing a total response to any type of crisis.

Following the incidents at Virginia Tech and Northern Illinois University, many states are in the process of enacting laws requiring that higher learning institutions develop an emergency response plan, with annual reviews by a qualified third party auditor.

William Sako is a Senior Vice-President of Rolf Jensen & Associates, a leading global provider of life safety consulting solutions. Based in Chicago, Sako is a pioneer in the field of security and mass notification. He can be reached at +1-312-879-7230 or via e-mail at usako@rjagroup.com.



The most popular approach to this type of “instant solution mentality” on campuses today is the digital text messaging system. The well-founded theory behind it is that all students are mobile and they carry cell phones. So, in the event of an emergency, campus officials simply send mass notification instructions as text messages to the students’ cell phones. While this sounds great in theory and we would certainly advocate the use of cellular communications in an emergency, in actual practice, there are a few flaws. For example, a major natural disaster might knock the digital system or the electrical power necessary to run it offline. Or the college/university may only be successful in signing up 20-30% of the students for the text messaging service. What about the other 70-80% of the students? Or what if the message recipients are in locations where their cell phones must be turned off... a lecture hall for example?

The truth of the matter is that effective mass notification is not a single system; it is a process that involves leveraging many, if not all, of the monitoring, communications and control systems in your building or on your campus.

The Process of Mass Notification

Achieving an effective, efficient mass notification capability on a campus requires comprehensive preparation and precise execution. We’ve broken the process down into five key steps:

"In a mass notification process, decisions involving people movement must be made in minutes or seconds, not hours."

Step 1: Assess the threats to your campus

Every campus situation is different. A rural campus in Kansas might be more vulnerable to violent tornadoes than a campus located in downtown Chicago where the major threat could be drug-related security breaches from surrounding neighborhoods. Both campuses will need to take precautions against disturbed or disgruntled students or staff members.

Campus officials won’t be in a position to design intelligent mass notification responses until they analyze the vulnerabilities and threats unique to their campuses, and to the faculties, students and visitors

(or employees, in the case of corporate campuses). This analysis must take into consideration what events could possibly happen and how they rank in probability of occurrence from most likely to least likely.

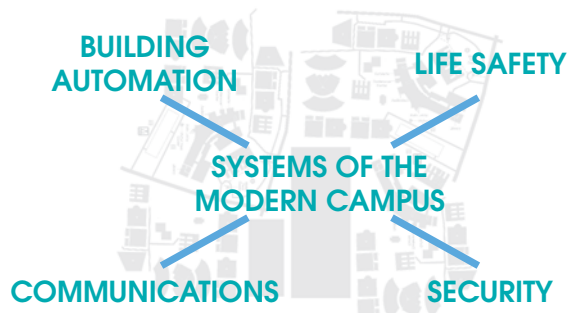
According to a recent public safety survey, this chart shows the major identified threats and the percentage of public safety officials who ranked each one as the top threat.

Natural disasters	65%
Drug trafficking or drug possession	11%
Non-drug related crimes	10%
Terrorist attacks	7%
Fires	2%

In addition to identifying what threats are most likely to strike the campus, you need to assess when (time of day, time of year, special dates) and where (specific office, building or facility) the event could take place. Creating worst case scenarios for each threat is a good way to begin getting a handle on the mass notification challenges your campus is facing. Since no one has a crystal ball, this exercise is highly subjective yet very necessary in the mass notification process.

Step 2: Investigate your infrastructure

Most campus officials assume they need to start from scratch when it comes to the system hardware and software necessary for mass notification. That’s not true. In point of fact, many of the systemic pieces are already in place. What is generally missing is an overview of how the campus operates on a daily basis. Are these critical systems interoperable? How can they be integrated and re-tasked during an emergency to serve a single command and control function for mass notification?





World Headquarters
600 West Fulton Street
Suite 500
Chicago, IL 60661

For more information, please visit rjainc.com