Best Practices
in Emergency Alerting

A white paper by Rave Mobile Safety

Rave
MOBILE SAFETY

Table of Contents

Overview

On today's campuses, it is an unfortunate reality that emergency incidents can and do regularly occur. Institutions must be prepared to respond quickly to a broad range of events that interrupt daily operations – everything from acts of nature to acts of individuals. The headlines of newspapers are filled with stories of institutions caught unable to respond in an effective manner, underscoring the high costs of being unprepared.

The United Kingdom's Department for Business, Enterprise and Regulatory Reform (2008), describes a crisis as "an abnormal situation, or even perception, which is beyond the scope of everyday business and which threatens the operation, safety and reputation of an organization." A 2007 document further defines how a crisis should be considered in the framework of daily operations:

> "... The crisis should be dealt with as an operational management issue that is simply being undertaken in extreme circumstances. The crisis management framework for response is normally based on existing management structures and responsibilities. It must also reflect (or improve upon) existing lines of communication, both within the company, and with other organizations which may be affected. This approach, when developed in conjunction with the operational managers, will confirm ownership of plans and prepare the proposed framework for practical implementation."
>
> *- "Crisis management." United Kingdom, Department of Business Enterprise and Regulatory Reform. October 2007.*

The purpose of this paper is to provide institutions with a framework for creating an effective emergency communications response plan that easily fits into their normal management structures and responsibilities. It is not intended to be all encompassing but the basis for identifying areas of improvement and practical steps for enhancing an institution's ability to respond effectively. While much of the focus of the paper is on emergency and mass notification communications best practices, the importance of the procedural aspects of emergency management are stressed in equal measure.

Emergency Management Phases

An Educause White Paper, “The Role of IT in Campus Security and Emergency Management”, published in October 2008, identifies a widely accepted four phase approach to emergency management:

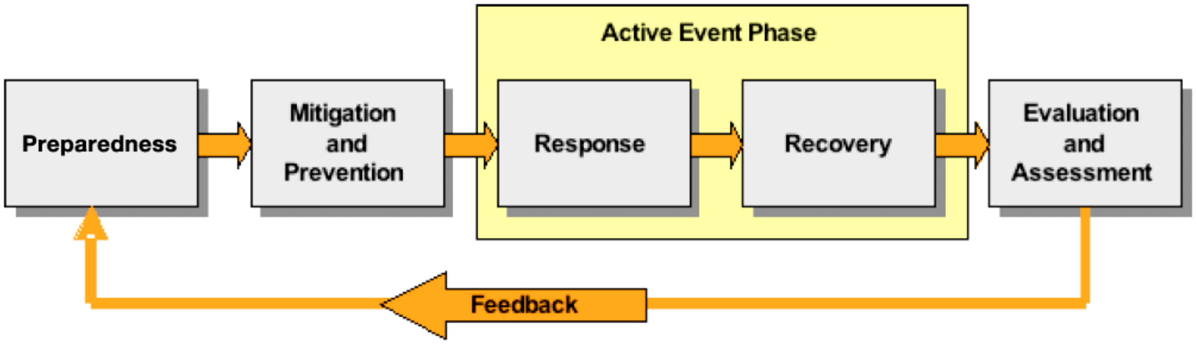
1. **Preparedness:** Mobilizing and preparing the campus response to emergencies, from the development of emergency response plans and the procurement of supplies to educating the campus community about procedures for disaster response.

2. **Mitigation and prevention:** Taking steps to reduce or prevent the possibility of disaster on campus, from identifying and assessing risk, to preventative measures that reduce the risk occurrence.

3. **Response:** Controlling how the campus reacts to disaster, including crisis communication and the treatment and protection of key assets, managing and protecting university students and personnel as well as critical information systems and university infrastructure.

4. **Recovery:** The timely resumption of standard operating procedures on campus, moving from “disaster” mode to “normal” mode through treatment, rebuilding, reorganization, and recovery.

A further recommended phase, post any actual event, is a continuous process of evaluation and assessment. Figure 1 below shows a typical process flow.



The value of mitigation and preparation should not be underestimated, and is perhaps the most valuable phase of the entire process; however, this topic remains outside the scope of this paper and has been well covered in a number of other sources. Let’s take a look at some best practices in the preparedness, response and recovery phases, especially as they relate to effective emergency communications.

Preparedness

Strategic Planning

Assess and rank the threat(s). The first step to improving your emergency response preparedness is to conduct a thorough assessment of the threat. Crisis communication expert Rene Henry describes five "generic" crises:

1. Terrorism;
2. Acts of nature including earthquakes, hurricanes and floods;
3. Sexual harassment and discrimination;
4. Violence in the workplace, and
5. Environmental pollution.

This taxonomy provides a useful starting point for identifying threats, but every campus has its own unique attributes that will greatly affect your planning process. What are the threats to your specific campus? Are you in an area vulnerable to a terrorist threat? Is their a chemical facility or risk of a train derailment in your immediate vicinity? Are you in an area particularly susceptible to hurricanes or other extreme weather conditions? Is your campus or a significant portion of your student body located in a high crime area? Do commuters regularly travel through an at-risk area? Are their any times of year when depression is particularly acute among students at your school? Does the institution itself have facilities that might be considered dangerous, such as a nuclear reactor, laboratory, or large store of chemicals?

To help prioritize planning, each threat should be ranked based on likelihood and severity. For example, the likelihood of an off-campus physical assault might be a very likely event but the severity in terms of its effect of spreading to the entire campus community and requiring mobilizing the emergency response team might be relatively small.

The University of Georgia preparedness web site provides an interesting example of assessing campus specific threats and prioritizing.

… 11 major structure fires have occurred on the UGA campus since 1993, and the Athens community has been hit by tornadoes in 1973, 1985 and 2003 (UGA Risk Management Services, 2007). On the Athens campus, accidental gas leaks from construction projects or chemical spills are far more likely than any of the above scenarios.

Identify prevention methods. While it is not the purpose of this document to cover the myriad of effective preventative and early warning processes, it is important not to underemphasize the importance of this step. From mental health screening programs to proper physical security measures, prevention must not be overlooked or under-funded. Prevention methods should be mapped out for each identified threat.

Define what constitutes an emergency. The next step is to identify what constitutes an emergency that requires a cross-functional response. Is an off-campus crime an emergency requiring a coordinated response on campus? Potentially, if the threat is severe enough and there is a risk of spillover onto the campus. It is important to clearly define for your campus the triggers that initiate an emergency management plan—and they should be defined unambiguously. These constitute the situations for which you will create a clearly documented preparedness plan. It is important to have generic procedures for unforeseen events, but data shows that over 80% of all situations experienced on a campus were envisioned prior to the event. One example of classifying emergencies is that used by the University of Chicago, where emergencies are classified into three basic types. They are:

- **Type One**. A Type One event or emergency is one that affects only one department or division of the University. It is assumed that Type One events can be handled by the affected department working in conjunction with the University Police and Safety Office. Typical of Type One events would be small, containable fires, or chemical spills.
- **Type Two**. Type Two events are those that affect multiple departments or divisions of the University. These events, at the discretion of the Emergency Director, may convene portions or all of the Policy Group and the Emergency Management Group. Typical of Type Two events would be major fires, significant electrical outages, severe snowstorms and/or major windstorms.
- **Type Three**. Events of this type are catastrophic in scale, affecting not only the University but the surrounding community as well. At the discretion of the Emergency Director, a full-scale response may be launched, utilizing the full extent of the University's capabilities, in conjunction with municipal emergency facilities. Substantial civil disturbances, tornadoes, or acts of war would be examples of this type.

Identify constituents and roles. A situation on campus can involve a broad spectrum of people. A best practice is to identify a broad working group that is involved in the planning process, appoint an emergency response manager, and then identify clear owners given the different types of situations. Here, a clear distinction should be drawn between a working group and planning effort from the response team. Often, the emergency response manager coordinates directly with the relevant “owner” of an incident. For example, the overall response to a fire in a residence hall would be managed by the emergency response manager but the situational “owner” might by the Residence Hall Director.

Clear lines of responsibility and communication must be identified ahead of time. The tendency during the chaos of responding to incident naturally pulls more people into the decision making process as they try to help, causing further confusion. Institutions that identify the constituents, their roles and a clear chain of authority ahead of time are much better prepared to respond effectively. Some key roles that should be included in an emergency preparedness council or working group include:

- Campus Safety
- Residence Hall
- Student Affairs
- Facilities
- PR/Communications
- Information Technology
- Local community law enforcement and emergency responders

Conduct an Assessment of your Situation and Assess Resource Gaps. What are the existing processes and policies in place? Where are the biggest gaps in planning and preparation? Institutions that have successfully stepped back and taken a cross-functional holistic look at existing procedures aimed at addressing identified threats often find than many threats have no easily identified or broadly understood procedures associated with them or at a minimum those plans and procedures are woefully inadequate. See the check list in Exhibit A for a good Situation Assessment checklist put forth by the International Campus Law Enforcement Association (IACLEA). Part of the situation assessment is to carefully identify available resources and identify the gaps. Every campus has different resources available. Based on the identified risks, their prioritization and the appropriate constituents, many institutions have found it helpful to identify the resources that could be used to address the situation. In many instances it is helpful to identify the ideal resources and then the reality of the situation. In addition to making it clear who and what resources are assigned to each type of risk response, this mapping will also help start to setting budget priorities. A partial list of resources that should be considered is included as Exhibit C.

Define scenarios and timelines for completing plans. Once a comprehensive situation assessment is complete, it’s time to put together a plan of action for each identified threat. At this point, clear scenarios will have emerged as top priorities for your institution. These are the situations where the threat ranking is highest and the level of current preparation and resourcing is the lowest. Establish a timeline for the emergency response manager and “owner” of an incident to create a plan for review. The timeline should be aggressive but attainable. Focus on working through the top priority plans first and then move to the next ones. Remember that this is a process of constant improvement, so the initial plan does not have to be perfect, but there needs to be one in place that you can call upon it when necessary. Safety is one of the top issues for parents and students, so make sure your discipline in completing the action plans is consistent with that level of emphasis! A helpful sample plan checklist is provided in Exhibit B below.

Implementing the Communication Plan

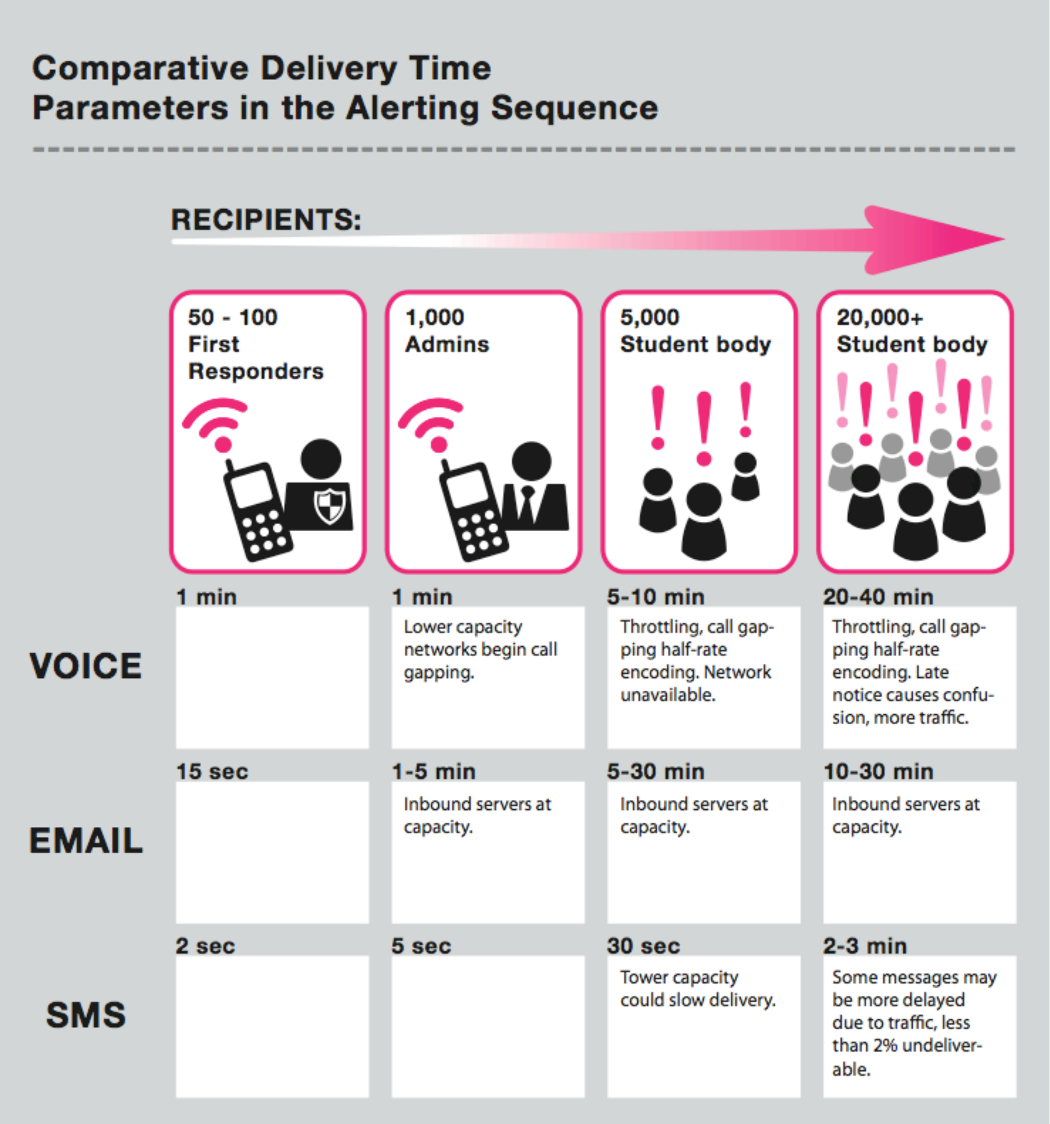
Implementing the plans defined in the Preparedness phase can be a daunting task, involving cross-functional cooperation across a wide spectrum of initiatives. This section provides a deeper look into the specifics of implementing the communication aspects of the plans.

Create communication processes, templates and approval procedures. During the chaos of an emergency event, communication processes that were once thought to be easy can become confusing and difficult. Even the use of an emergency notification tool that seemed so simple during training several months ago can become daunting and fraught with the risk of mis-communicating simple information and thus compounding a situation. A few simple best practices can make a significant difference.

- ***Define acceptable terms for emergency mass communications*** – What are the right terms for you to use that will be unambiguous and not cause confusion? Is there more than one library? Is the word “gunman” appropriate for a female assailant? How will people respond to a directive to “stay in your residence hall”? Do you expect them to return there if they are currently in a classroom or library? Are there abbreviations for text messages that might be particularly clear or unclear? Many institutions have created lexicons for emergency situations, leverage what others have created and modify them for your own use. Make sure you test any terms that are unique to your campus with some actual potential recipients of the message. Things that seem clear to a group of administrators might be interpreted completely different by a group of 19 year old students. Many institutions will choose to review emergency messaging language with appropriate legal and security staff as well.

- ***Determine target audience(s) specifics*** -- Each audience will have different appropriate priorities and content. Different communication content and modes are relevant to different audiences. The first job of the crisis communications team is to contact the list of need-to-knows – security, key administrators, and first responders. The individuals on this list may depend on the specific situation. When will these key individuals be contacted and what will they be told? Let’s look at the simple example of a chemical spill on campus. First responders would be notified first and told all appropriate details, including the expected material, resources in route, which roads are to be closed, what to communicate to civilians, and where to report. Students would be told to avoid the area in question, and to look to the web site for more information. Parents and media might be notified that there are no injuries and no immediate danger to any students or faculty and that more updates will follow. The important planning step is *to identify the different steps and procedures for communicating with each audience*.

- ***Identify the appropriate mode of communication for each audience*** -- Different modes of alerting may be better suited to specific audiences. For a mass audience where the highest performance and throughput is required, SMS alerts are an ideal solution. On the other hand, delivery notification to first responders may require a more interactive alert media that has better capability to convey a richer level of content and interactivity through a conference call. The number of first responders, and the corresponding network capacity used in communicating with them, is also a much smaller number than an entire student body. In this case, a voice alert may be ideal. The ideal notification media for faculty, admin, and staff may fall somewhere in between. Interested parties who are not directly part of the school community (e.g. parents, local community) may be effectively supported with a higher latency, lower touch alert such as email. Institutions should consider their different potential audiences when developing their mass notification procedures and determine appropriate media accordingly. Figure 1 shows an example of typical production delivery performance and selection of modes by audience observed over many notification events by a highly robust notification system. Note that the actual environment into which messages are being delivered is the single biggest determiner of performance, but the figure details some of the different technical limits seen in the different modes:



Comparative Delivery Time Parameters in the Alerting Sequence

RECIPIENTS:	50 - 100 First Responders	1,000 Admins	5,000 Student body	20,000+ Student body
VOICE	1 min	1 min Lower capacity networks begin call gapping.	5-10 min Throttling, call gapping half-rate encoding. Network unavailable.	20-40 min Throttling, call gapping half-rate encoding. Late notice causes confusion, more traffic.
EMAIL	15 sec	1-5 min Inbound servers at capacity.	5-30 min Inbound servers at capacity.	10-30 min Inbound servers at capacity.
SMS	2 sec	5 sec	30 sec Tower capacity could slow delivery.	2-3 min Some messages may be more delayed due to traffic, less than 2% undeliverable.

- ***Consider coverage and capacity limitations of your available communication modes*** -- Each mode of communication has its own strengths and weaknesses. Sirens are extremely effective for communicating to an on-campus audience, but are not easily targetable (i.e. any intruder gets the same message as everyone else) and do not cover off-campus users. Landlines provide a great way to deliver messages, but are subject to becoming overloaded during high volume emergency use and many users are not normally within easy reach of a landline phone. The ability of the existing coverage and capacity of cell towers covering a campus can be a limiting factor in delivering text and voice alerts quickly and effectively to mobile phones. Due to these constraints, attempting to simultaneously alert an entire school for multiple devices per user and multiple modes per device (text and voice) can be a bad idea. A better strategy is often to select optimum media to reach certain audiences (described above) and prioritize among audiences accordingly. Figure 1 above details some of the typical uses of the different modalities and constraints seen in production environments.

- ***Consider implementation of an inbound notification infrastructure*** -- An effective mass notification system should enable inbound responses and provide a simple mechanism for reporting on and responding to those messages. Additionally, institutions should plan for a large number of inbound information requests. Often, on premise telephony systems can be saturated with inquiries from press and parents. Coupled with even a small percentage of students calling in response to a notification they received, the call capacity of even the most robust telecomm infrastructure can be brought to its knees. In addition to a well-maintained informational web site, many institutions utilize off-campus toll-free information lines to steer call volume off site and effectively answer most of the typical questions.

- ***Define coordination around the approval process in detail*** -- Different situations may require different constituencies to take responsibility for sending an alert. For example, an alert canceling class due to a weather emergency might require a different sender and a different approval process than an alert notifying the campus of a dangerous security threat. On the other hand, some institutions may choose to centralize ownership and privileges for sending alerts within one campus organization. It is critical that ownership and processes for issuing alerts be explicitly defined at both an organizational and individual level in the emergency response plan. At a minimum, identify principal alert senders who are privileged to send alerts without internal approval. These individuals might be VP-level administrators from university relations and/or campus security. Identifying and training individuals who have complete decision making authority can dramatically cut the time it takes to decide to send an alert, create the alert, and deliver it.

- ***Establish policies for the frequency and level of communication*** -- In many cases you will not have a clear picture of information during a crisis, yet your audiences will expect it. In your planning clearly identify rules around the frequency and level of communication you will provide. For example, will you provide updates every 30 minutes even if there is no new information or will you update your audience(s) only when new information becomes available? Set expectations both with the communication team and the audience in advance of the event.

- ***Create message templates*** – Most institutions report that upwards of 75-80% of situations they encountered were ones they foresaw as possible threats. Pre-created messaging templates can take much of the "fog of war" out of an incident. By creating and using simple templates with fill-in-the-blank dates, locations and key details messages can be quickly edited and sent. It is important that the content created be appropriate for each mode of communication. For example, an email can and should contain much more descriptive content than the 160 available characters of a text message. A useful list of emergency message templates is available online from Margolis-Healy Consulting (www.margolis-healy.com).

Identify alternates and back up plans. The only thing that can be completely counted on in any plan is that things will not go as you expected. That is not to say a plan isn't invaluable, but you must be prepared to handle the unanticipated. If your internet service is down, can you still send an emergency notification? Where do you direct people for more information if your web site is down? If your landlines and cellular communications are spotty, are there established face-to- face coordination procedures? If the person responsible for sending emergency notifications is stuck in traffic in a snow storm with a dead cell phone battery or on vacation, is there a back-up? The most important step in preparing for the unexpected is ensuring lines of authority and communication are clear. When chaos strikes, many teams revert back to the habits of a team of 6-year old soccer players with every player running to the ball while leaving the goal unattended. Ensure that your team understands when they need to chase the ball and when they need to mind the goal.

Document and make plans easily accessible. Make sure emergency planning binders include instruction materials, necessary passwords/login information, contact information and are distributed to and accessible by those responsible for implementing emergency plans. Hard copy availability is important in case internet access is unavailable. We also recommend that this binder also contain a short, one-page school specific “cheat sheet” that describes the tactical process for sending an alert.

Communicate the plan to the campus and local community. From ensuring students know to give their contact information to ensuring the patrol officer on duty knows to unlock the motor pool gate, communicating the emergency plan is critical to its success. While there are normally effective and well established procedures for communicating with first responders and administrators, getting the word to students and faculty normally requires a more comprehensive marketing effort. A sample of marketing best practices for getting enrollment is included as Exhibit D.

Internalize via Practice, Practice, Practice. A plan is only as good as its execution. Ultimately the success or failure of any emergency response plan is based on how well the different constituents execute on their responsibilities. Periodically test systems, processes and people. Where possible, involve as many constituents as possible and have different levels of practice – just first responders, broader constituents, campus wide, etc. Campus wide scenario based tests should be conducted at least semi-annually. An effective test should start with the triggering conditions, go through the first responder and mass notification, and finish with an after action review to identify and address any gaps.

Response

Communicate truthfully and promptly, and communicate succinctly. The communication goal is to be transparent without causing panic and chaos in the community. This means getting the word out quickly, communicating effectively without undue complexity, and monitoring both the situation itself as well as the coordinated strategies and tactical execution of your safety plans and protocols.

- **Be comfortable not over communicating.** Too much information can confuse things during a crisis, and when the community requires clear messages that demonstrate leadership and promote safety, be succinct.

- **Expect to be forced to make decisions based on incomplete information.** As with all other aspects of your emergency planning, plan our your chain of command, and your tactical response. What are the decision-making processes involved in your tactical response? Do constituents across all functional areas understand the bounds of their authority and a clear chain of decision making – within your safety responder community, the administration, security and police, and the campus at large?

- **Organize your first responders.** Some emergencies have a clear tactical protocol, others may be more ad hoc. Build appropriate networks of first responders and have lists that can reach these teams prebuilt and ready to access in an emergency deployment. Use features such as conference call bridging to organize tactical execution during an emergency – get your appropriate responders on a call to coordinate tactics, share up-to-the-minute information, and organize assignments and action plans.

- **Plan to utilize response features in your alert solution.** Be sure that the administrators of your alert solution are fully trained to manage responses from individuals during the alerting process. This includes checking responses, validating delivery of emergency messages in a timely fashion, dispatching help to individuals in crisis who request assistance, and communicating with strategic players in your emergency management team.

Recovery

Recovery should not be overlooked as part of the emergency alerting communication plan. This is the final phase of emergency management – returning the campus to its normal state.

- **Again, determine the decision makers.** Who on the team has the authority to recall a lockdown? Who determines if the crisis is complete? Again this takes some planning according to your risk predictions. As you know, in some events, staff on the ground may lack complete visibility of a threat. Most schools recognize that distressed communication of a still-active threat is a high risk issue. Your emergency preparedness scenarios must include a process to declare a threat fully mitigated, and assign responsibility to those who make that final determination.

- **Provide a smooth transition from Crisis to Normal mode.** Many customers structure an "all-clear" message that communicates the end of an event. Once your decision-makers have called a situation clear, send a concise alert to the community announcing this fact referencing any available information resources that are available to explain the situation that has occurred.

Evaluation and Assessment

Finally, ensure you institutionalize a process of continual improvement by critically evaluating the incident and assessing areas for improvement. Make sure the results are fed back into your planning process and assigned owners and deadlines.

- **Post-mortem analysis and continual improvement.** Your emergency management plan is a great starting point, and each event will demonstrate the strengths and weaknesses of your response protocols. Be sure to establish a discipline around reviewing events with all affected constituents, and follow up with a formal analysis.

  - Establish a process of continual review and improvement. Review plans at least yearly and immediately following any event. Some institutions go so far as to establish a number of days after an event by which a written analysis should be completed

  - Participate in sharing best practices with peers and among constituents of safety, security, and emergency planning across campus.

  - Did you overcommunicate, undercommunicate, or get it just right during the crisis? Look at the big picture to understand the efficacy of your response to the event.

  - Stay in touch with the issues affecting higher education via participation in key organizations such as EDUCAUSE, IACLEA, and other campus safety organizations.

- **In your notification management tool itself, utilize available reporting features.** Standard practice following any alert event should be for the primary emergency administrator to review all reports and data that are collected during the alert. A summary report of the alert might be produced interpreting these data and distributed to constituents. Important statistics include:

  - Description of the alert event and its outcomes.

  - Log of events in the execution of the safety protocol, including timings on alert sending and distribution. Break down alert distribution statistics by mode of delivery to show how each mode of delivery compares in terms of efficiency, rapidity of communication, and overall deliverability.

  - Capture any interesting responses to messages, ad hoc comments by community members, and/or relevant press coverage of the event to provide the flavor of how the event was perceived by the campus community.

  - Analyze deliverability statistics to determine the freshness of your contact database. Did you messages reach well over 95% of the community (or whatever number your planning has targeted for maintenance of up-to-date contact information)? If not, consider a renewed user registration effort or troubleshoot the issues. One Rave customer who had a high-profile campus threat the first week using Rave Alert was able to leverage the publicity of the event to spur a large voluntary registration drive.

    If deliverability and freshness were well aligned with your goals, be sure to share this success factor with the community in your report.

Conclusions

Unfortunately, the risks facing our institutions and the people in them have grown complex, and seem to increase in complexity over time. New approaches to emergency preparedness and emergency management are required to protect our students, our faculty, and our staff from an increasingly frightening network of threats. However, as we have seen, many if not most threats can be elaborated, predicted and prioritized in our preparedness scenarios. While it’s obviously impossible to predict all events that might occur in our midst, it is entirely possible to build a practice that protects and prepares us for many of the trials that await us.

Exhibit A - Situation Assessment Checklist

Source: American Council on Education, http://www.acenet.edu, May 3, 2007.

Although no single template will adequately meet the emergency planning needs of all institutions, the key questions that Presidents, CIOs, security/safety and emergency management teams should consider include:

- Has our institution conducted a comprehensive assessment of the potentially catastrophic risks it faces? Has our institution made plans to address those risks?
- Does our institution have an appropriate emergency team in place? Is the team headed by a senior administrator? Do key team members regularly participate in emergency preparedness exercises? Are team member responsibilities well-articulated, well-understood, and effectively coordinated for efficient crisis management?
- Does our institution have a plan for continuous operation in the event of an emergency (i.e., a continuity plan)? Is that plan applicable to all types of emergencies?
- Does our institution have multiple means to communicate with students, faculty, staff and visitors in the event of an immediate, ongoing emergency situation that demonstrate that all possible means are invoked to communicate during a crisis?
- What role does our campus information technology leadership play in our emergency planning? How are technology experts brought into the day-to-day planning process for campus communications, emergency response, and the ability to maintain campus services during a short- or long-term disruption?
- What communication and coordination networks exist among our campus security leadership, local law enforcement, political officials, first responders and health officials, both on an ongoing basis and in case of emergency? For example, does our institution's campus safety department have mutual aid agreements or memoranda of understanding with local emergency response agencies?
- What kinds of processes or programs does our institution utilize to inventory campus security resources, including the ability to retain experienced, trained staff?
- Is the training of campus security personnel appropriately responsive to catastrophic risks?
- Are the policies and procedures used at our institution appropriate with respect to persons who are believed to pose significant danger to themselves or others?
- Are the policies and procedures used at our institution demonstrative of our commitment to emergency preparedness, well-aligned with accepted standards, and demonstrative of our institution's reputation and leadership in higher education?

Exhibit B - Seven Crisis Management Essentials

Source: "A primer for crisis management." Risk Management. Oiver, Barbara B. January 1, 2002.

1. Reach out to key public safety agencies in your community when designing your facility evacuation plan. Determine where the fire or police department is likely to place its staging area and designate that location as the site where staff will congregate after evacuating your building. Many communities also have an office of emergency preparedness that may be able to provide advice about evacuation strategies.

2. Establish a network of community institutions that you can call on during a crisis. Consider a wide range of organizations that might be key partners during specific types of crises.

3. Keep a comprehensive directory of personnel up-to-date, with copies maintained off-site. Be diligent in maintaining emergency contact information for all staff; every time an employee leaves or joins the organization or undergoes an annual review by a supervisor, update current home addresses and phone, fax, wireless and beeper numbers. With security and privacy issues in mind, consider an online directory that enables each staff member to update personal information without requiring a visit to your personnel department.

4. Carefully inventory the physical assets needed to continue mission-critical operations, even at vastly reduced levels. Update these databases or spreadsheets during the annual audit or property insurance renewal process, but record major acquisitions as they occur.

5. Maintain a backup of your computer file server and key databases and financial files. Update the backup at least every week and store a copy off-site or in a fireproof safe. Schedule drills every thirty to sixty days to test the procedure and to determine if you can restore systems from the backup tapes.

6. Store a copy of all insurance policies, vehicle and property titles, vehicle registrations and bank account numbers in a safe deposit box or fireproof safe.

7. Review emergency and crisis management procedures at least once a year with key personnel. Make it a top priority to create procedures indicating who does what in the event of an emergency with alternates to replace them.

Exhibit C – List of Resources to Consider

- Communication tools and infrastructure
    - Mass notification system(s) addressing multiple modes
        - Sirens
        - PA Systems
        - Text messaging
        - Email
        - Voice call messaging
        - Digital signage
        - “Blue Light” phones
        - Monitors
        - CCTV
        - Radio
    - Redundant/Highly available web site with easy access for rapid updates
    - Capacity and coverage of telephony
- Campus Safety
- Transportation resources
- Up to date contact database/directory with proper access
- Emergency collaboration and response management tools
- Local first responders
- PR and communications

Exhibit D – Marketing Best Practices for Rave Alert

- **Make emergency notification registration part of existing school “getting started” processes.**

    - *Admissions.* During the admissions process, capture key student data like preferred email address and mobile phone number and upload it to the Student Information System (SIS), which can then be uploaded to the school emergency notification system. Schools embed registration into admissions and other administrative processes see compliance rates up to or exceeding 95%, while those that rely solely on “marketing” typically see results in the 40-50% range.
    - *Orientation.* Register students for Rave Alert during student orientation sessions, when students are taking care of their campus IDs and getting access to campus systems. If there is a presentation or material on campus safety and security, make sure the Rave Alert service is featured prominently within it, along with instructions on how to register.
    - *Move In.* Encourage student registration so that students can receive channel information and narrowcast alerts pertaining to their residence halls. Instruct resident advisors to encourage registration and create Rave channels for their RA groups to use for communication during the school year.
    - *In Class.* Encourage faculty to set up a Rave channel for each class and ask or require students to register and opt in. (If you are using Rave’s optional Blackboard Building Block integration, Rave maps channels to Blackboard courses automatically, and this provides additional incentive for students to use alerting and keep their contact information up-to-date as well.)
    - *School fair and school activities.* If there is a school fair promoting school activities, have a physical presence there so that the Rave Alert service is recognized as a school resource.
    - *Get the word out to parents.* Publicize the availability of alerts to parents and advise parents to emphasize usage of the system.

- **Promote Rave Alert on campus on an ongoing basis.**

    - *Posters.* Promote the alert service by putting up posters describing the service in key locations on campus.
    - *Flyers.* Create flyers as handouts to be included in school informational packages.
    - *Direct mail.* If practical, stuff student mailboxes with postcards promoting the service.
    - *Email.* Use periodic mass email campaigns to remind students to register and/or keep their contact information up to date.
    - *School newspaper.* Run a story on the school’s purchase and/or adoption of Rave Alert as an addition to the school’s emergency response capability.
    - *Web presence.* Incorporate references to the school’s alert service key web pages that are accessed regularly by students, including potentially the school’s homepage, webmail login page, SIS or course management system homepage, etc.
    - *Text messaging***.** If student mobile contact information has been collected outside of Rave Alert and uploaded into the system, Rave Alert can be used to send these students a text message encouraging them to register and validate their phones.

    Rave’s Student Marketing Toolkit includes a number of communication templates that can assist you in crafting messages to the campus population.

Glossary

Campus Emergency – Onsite incident in which students, faculty, and staff are in potential danger

Email Alert – An alert transmitted via e-mail to a pre-defined database. Typically, transmitted through SMTP.

Emergency Notification – A means of quickly delivering time sensitive information, through a variety of modes, to a specific set of recipients.

Mass Notification – A means of delivering information, through a variety of modes, to a specific set of recipients.

Reverse 911 – Communication system that allows emergency services to quickly contact members of a community or organization with information

RSS Alert – Relaying both emergency and university information through a RSS feeds, such as signage, twitter, facebook, etc…

SMPP – Short message peer-to-peer

SMS – Short message service

SMTP – Simple mail transfer protocol

Text Messaging – Sending of "short" (160 characters or fewer, including spaces, newer phones can hold up to 20 pages of 160 characters) text messages from mobile phones using the Short Message Service (SMS)

Voice Alert – A recorded voice message transmitted to a pre-defined database of cellular & landline phones. Can be transmitted through either VoIP, or more reliably, through circuit-switched technology.

Resources

IACLEA – International Association of Campus Law Enforcement Administrators
www.iaclea.org

Security on Campus
www.securityoncampus.org

Margolis and Healy
www.margolis-healy.com

Educause Connect - Communication
connect.educause.edu/taxonomy/term/77/0/feed

Campus Safety Magazine
www.campussafetymagazine.com/

Rave Wireless
www.ravewireless.com