Life Cycle Strategies for Higher Education Emergency Notification Systems

A white paper by Rave Mobile Safety

Rave
MOBILE SAFETY

Table of Contents

Introduction

Picture this scenario: One afternoon in a quiet campus lab a crisis erupts when containers of an abrasive chemical begin leaking. The toxic fumes create an environmental hazard requiring an immediate evacuation and lockdown.

Suddenly the facility needs to be evacuated, and the campus community needs to be steered away from the location. Communication and coordination among campus police, fire and safety teams needs to be swift and effective, and local municipal agencies need to be called in for support as well.

Media management is also critical; in a matter of minutes TV and radio stations will begin sending trucks and helicopters. As administrators deal with crisis response, camera crews will descend on campus hoping to catch students running from the labratory covering their faces.

Thankfully your emergency notification preparedness plans are fully engaged! The multi-modal emergency notification successfully fires off the critical messages - evacuation directions, locations to avoid, status updates.

First responders get the critical alert, along with a request to confirm their response capability - each responder replies signifying readiness and position. The administration quickly huddles to clarify both response and responsibilities; bridging into an ad hoc conference call from a voice notification. Hazmat teams are deployed and already at work containing the toxic spill.

Students hear about the issue from sources all around them:

- All 12,000 students and faculty receive a text message and email notification.
- Students logged into Facebook and Twitter see an urgent message on those sites as well.
- Computers around campus all display a noticeable warning on screen, brightly blinking.
- Alarms go off within the affected facility requiring immediate evacuation.
- PA systems call out instructions at key locations around campus.
- LCD displays in the Student Center and other key buildings display warnings.
- Safety beacons in the classroom switch to full notification mode.
- Cisco IP phone systems broadcast a voice, text and alarm sound to each campus display.
- The campus homepage automatically switches to “emergency communications mode,” providing clear and obvious instructions to viewers based on RSS alerts, and reassuring the community as well as parents and concerned citizens in the surrounding community – and providing a common place for the community to turn for up-to-the-minute instructions.

Within two minutes, 98% of the campus is effectively notified!

Once the situation is under control, the all-clear is sent; commuting students turn their cars around and return to campus for afternoon classes. No one has been seriously hurt, though several individuals are treated for inhalation at a nearby hospital. The response from all emergency staff and the administration was rapid, comprehensive, and praiseworthy.

As the media reports praise the university’s response and planning, the emergency staff are already looking at the rich data with careful scrutiny as they begin the post-crisis reporting and assessment process. *What was effective in the response? What could have been better coordinated?* Intelligent emergency preparedness learns from experience; this incident - properly analysed - better prepares the campus for efficient response in the future.

Preparing for the Unknown

All emergency plans and preparations take time to coordinate and take resources to coordinate and maintain. Your preparedness plans build on the tools and resources you have available, sensibly over time, prioritized against your risk assessments, active localized threats, and common best practices for preparedness.

This paper will look at the **life cycle** of your emergency notification systems, and the ways that your own institution's plans can be prioritized, planned, and executed for continuous improvement to build a system and a process to address a real crisis.

Products and services that technically qualify as *emergency notification services* are diverse, encompassing numerous software and hardware products —Emergency Notification Systems (ENS) spanning text, voice, email, and RSS/web communications, public address, siren and bluelight systems, safety beacons, IP telephony warning systems, specialized emergency systems (e.g., fire alarms, radiation warning systems in a hospital or laboratory, etc.), personal safety applications and systems, and more—have converged on preparedness planners in higher education as institutions seek to deploy a comprehensive systems strategy for managing campus safety and security communications.

High profile campus violence and other disasters have raised awareness of the need for these tools for crisis management and response. Institutions and government agencies are racing to comply with legislation *mandating* preparedness. Parents and student groups are more vocal than ever in support of these initiatives.

Institutions are finding it necessary to focus systematically on campus safety both strategically and tactically. The possibilities and risk scenarios can be local, regional, statewide, or national — but each institution is expected to be able to provide comprehensive time-critical, authoritative communication of information, coordinated deployment of resources, and sophisticated, reliable state-of-the-art technology to protect the campus in the event of a crisis.

As institutions have reacted to the broadest requirements for preparing campuses for emergencies, it's also become clear that proper execution of emergency preparedness involves a ***life cycle*** approach— preparedness must be addressed in phases and stages, not as a one time implementation of a tool or plan. Preparedness means taking the time to assess, prioritize, and evaluate risk and response to the broadest variety of threats. It also signifies a commitment from the institution to re-evaluate continuously overall campus preparedness, assess newly documented threats, and integrate additional technologies.

In this paper, we will walk through a recommended life cycle that has been used effectively by dozens of institutions over the years, highlighting some of the key challenges to emergency preparedness; institutional policies, procedures and protocols; and assessment. Fundamentally, a campus is not transformed overnight into a safe environment; instead, institutions are best served by a systematic, project-oriented approach with prioritized risks, defined goals, and preparedness roadmap that can navigate measurable gains as well as respond to feedback with improvements, address legislative and campus imperatives, and incorporate improved and newly available technologies. All combine to improve communication and emergency response, and thus produce measurable benefits for campus safety.

Understanding the Landscape

One hurdle for emergency preparedness planning is that several aspects of technology stay constantly in motion while standards and regulations change rapidly.

1. **Networks are evolving**: Emerging technologies such as Cell Broadcast and expanded capabilities in IP telephony, for example, are likely to drive new standards for emergency notification for highly mobile populations in the coming years, but remember that many of these technologies are not yet mature enough for deployment, are not suitable for very narrow targeting of messages, or are at the very tip of a cost-benefit cycle that needs to come down-to-earth. Thus an emphasis on an extensible ***platform*** **-** preferably one optimized for network-based communications - is the right choice for changing times.

2. **Standards are evolving**: Just as FEMA itself is still discovering its role and authority within intra- and inter-agency emergency communications, various standards bodies are actively wrestling with technology standardization for emergency notification. For example, OASIS supports the Common Alerting Protocol (CAP) standard, as of this writing in review of version 1.2, and FEMA has declared ongoing support for the standard to enable a common language between a wide variety of notification systems — text based, voice based, and broadcast media-based.

The Emergency Interoperability Consortium (EIC) is a standards group devoted to developing common interoperable technologies for notification, and supports the Emergency Data Exchange Language (EDXL) standard in particular. Some time will pass before these standards become practical options for campus communications, but again, the direction for an institution's roadmap should be to embrace these standards when they become practical, tactical options for notification over the next five years. Eventually, these standards will lead to a more converged technology base for emergency notification — and your campus will benefit from notifications generated from presidential directives, state management offices, national weather service alerts, and county and municipal cooperation.

3. **Cost-benefits and priorities change,** sometimes subtly, sometimes quickly and in the extreme. Standards are well and good, but many universities and colleges are overwhelmed by the need to address such a wide range of technological needs. Many institutions have had to provision budgeting for these technologies in the wake of Virginia Tech and other newsworthy campus disasters. All while needing to develop a reasonable metric for cost-benefit analysis and prioritization given difficult economic conditions. On the other hand, technology advances are also making it possible for vendors to reduce pricing to produce quantifiable cost-savings. The return-on-investment on safety technology remains strong, and seems to be improving over time.

4. **Communications modes**: Subscriber habits around messaging change over time, and modes of communication change in popularity. Expect that over time the modes of communication with the highest usage rates and overall convenience to the subscriber will evolve as new technologies are adopted. Develop policies and select platforms that allow you to be responsive to these changes so that your messages reach the subscriber on today's, and tomorrow's, preferred platforms.

How Priorities Change Over Time

The life cycle of your emergency notification strategy should clearly reflect your priorities for campus notification. First priority is usually multi-modal notification that reaches the largest amount of your campus population as quickly and efficiently as possible. Once that critical goal is met, you can start to consider optional integrations, alternative uses of your tools, new feature requests and delivery modes that can extend the value you derive from your systems.

To address the life cycle of next-generation emergency notification services, five phases should be analyzed:

1. Determine your policies for messaging and data collection (opt in vs. out out, etc.)
2. Get up and running quickly with a hosted notification system used by a targeted group of admins
3. Expand the modes of messaging managed through your single interface (e.g. signage, sirens, etc.)
4. Leverage your messaging system into other business processes (LMS, fin aid reminders, recruiting - non-emergency messaging)
5. Leverage contact database and expand safety capabilities with Rave Guardian

Phase 1: Determine your vision

Institutions face many choices and implementation options when configuring a messaging system — indeed, so many options that many institutions balk at the formidable effort involved. As with any complex, cross-functional project, however, it's important to remember that, broken into steps and smaller blocks of effort, these tasks are quite manageable. In fact, more often than not, the *policy* decisions and direction are more difficult to align than the technologies and resources that support them.

That's why a high-level **roadmap,** consistent **planning,** and dedicated **project management** are the foundation of a emergency preparedness strategy on your campus.

The *roadmap* outlines the final state that your various preparedness teams aspire to — whether from emergency management offices, campus security, student affairs or other campus departments and organizations. To build your roadmap, consider some of the following questions:

- How much of your campus population should be reachable by your notification tools?
- What are all the ways you want to be able to notify your community?
- What are the *highest impact* notification modes for our community? Prioritize the modes that reach the largest groups of subscribers the most rapidly and effectively (e.g., text/SMS delivery, email, web presence, etc.).
- Are there "related sub-communities" to consider (e.g., a campus hospital, off-campus residences, surrounding communities)?
- Are there specific or unique risks to your campus that suggest a specialized notification mechanism?
- Are there specific technological hurdles to resolve to enable broader coverage for communications and incident response?
- Are there local, municipal, or county government resources that you need to interface with?
- Who will be the primary user(s)? Are there approval policies or procedures for different types of users?

You might set a goal, for example, to be able to reach at least 95% of your campus community in under 5 minutes, or determine that you'd like to integrate LCD displays or your institutional web presence into the communications toolset. Once you get started, you are likely to generate a long list of potential integration points that implement your strategy. Sort through them and prioritize them to create your roadmap, and then use your roadmap to generate a realistic plan and project milestones that implement your strategy.

This is the phase where coordinators start to feel overwhelmed, but again remember that not every aspect of the plan is required to happen at once. Build slowly and steadily, using your priorities to guide the sequence of steps you take to reach your campus safety objectives.

Several issues are consistently highlighted as challenges as administrators think through their emergency notification vision, namely: organizational structure and policies, opt in or opt out strategy and its effect on data management, integration of different types of notification tools including hardware based, and the role of social networking tools.

Organizational Structure and Policies

Policy in general drives both your planning and execution. At some point, an institution assigns priority, budget, and resourcing to its emergency planning, and these features vary from institution to institution. Every campus has its own unique characteristics and associated risks and priorities. California-based schools, for example, might prioritize earthquake planning over other risk scenarios. In Kansas, tornadoes might be higher on the list.

Certain communication characteristics are common among all high priority scenarios — reaching the majority of your population, ensuring communications to remote users or commuter populations when appropriate, prioritizing individuals and groups most at risk from specific scenarios, enforcing lockdown procedures, establishing chain of command in incident response, to name just a few.

Finally, consider resources, budgets, and other required tools of planning. Many institutions have very large ambitions for emergency planning, but unless adequate human and financial resources are available to support these plans, it may be necessary to scale back your plans, address the project in more distinct phases over time, or find non-traditional resources to achieve institutional goals. Emergency planning has a small tolerance for error, so in most cases, it is better to accomplish your plan fully than to attempt too much and under-deliver.

Evaluate and Assess

Just as threats and risks change over time, institutional policies need to evolve based on changes that are both internal and external to your situation. Risk management needs to be dynamic, and assessment helps to ensure that preparedness plans are staying up to date.

Internal feedback might come from the process of testing your preparedness plans, actual incidents leading to deployment of your systems, new threats identified by your internal safety personnel, and awareness of new technology options. Learning from deployment experiences is critical, and it is a best practice to report on events and make an honest assessment of the strengths and weaknesses of the emergency plan and its supporting technologies.

Communications modes are likely to change over time as well. Your campus may have added new technologies such as LCD displays that are now available for emergency notification, or your campus hospital staff may have moved from numeric pagers to smartphones. You may have identified an under-served population that requires a specialized form of communication, or your emergency management team may have spawned a new model for managing first responders.

Expect to revisit and revise plans to keep pace with organizational change, technology refresh, administrative directives, and legal mandates as part of the institution's standard overall discipline around emergency management and disaster planning.

Safety First: Opt-in to Opt-out

One transition that many institutions are making is to an “opt-out” default to replace an “opt-in” system for emergency notification. Young adults tend to underestimate their exposure to risks and thus many campuses find that a strictly “opt-in” system — where students are urged to self-register to receive messages from emergency notification — will meet with lower than desired compliance. Despite the best marketing campaigns, some significant percentage of students and staff are likely not to take the time to sign up for alert notifications.

Notification vendors have responded to this issue by supporting increasingly efficient tools to integrate with ERP and Student Information Systems such as SunGard Banner and PowerCampus, Datatel Colleague, Oracle/ PeopleSoft, to load the campus population’s contact data into the system — moving the campus from an optional participation model to a model where all members are opted-in to notifications, and then freely permitted to remove themselves should the individual choose not to participate. This model means that a very large majority of your campus is ready for notification on the first day of classes.

Again, a phased approach might start with an opt-in model, where subscribers to notifications voluntarily register to receive alerts and self-manage their own data, but then move later to an opt-out model, where faculty, staff, and students are entered into the system via automation when the resources are available to support this model. Again, look for a vendor with flexible configuration options that can support self-managed, fully automated, and hybrid models of subscriber management — and make sure that your IT resources concur with your selection since they are ultimately responsible for the integrity of this integration path.

An opt-out policy demonstrates that the institution takes emergency communications very seriously, and has set policy to ensure that the maximum number of community members receive an alert during a crisis. It is, effectively, a “better safe than sorry” approach to notification, and increasingly a best practice when provisioning notification tools with subscriber data.

Are Social Networks Ready for Emergency Notification?

Social networks, “Web 2.0” sites such as Facebook, MySpace, and Twitter, are valuable communication tools, and many schools have realized that student spent a lot of time connected to these sites and read them more avidly than email for example. There are several pros and cons to using these sites *specifically for emergency alerting* and some emerging best practices that derive from them.

PROS	CONS
Ubiquity; many subscribers spent a great deal of time connected to these sites.	**Placement**; your message must often via for attention with a large stream of messages, and some sites provide very limited control of message placement, contention with advertising spaces, etc.
Currency; your institution demonstrates its participation in the online community by including notifications to the “real” campus community.	**Opt-in**; subscribers must find the correct accounts where alerts are posted, and add it to their own account (e.g., “friending” or becoming a fan on Facebook, “following” the account on Twitter).
Integration; works well within a multi-modal communications strategy as “additional delivery point” and uses resources located off-campus.	**Reliability**; social networks are not yet mature platforms and are subject to outages and slowdowns.
Audience; reaches a broad community of active users.	**Politics**; many universities use their social networking sites for recruiting, and are concerned that mixing in tactical emergency communications might impact the institution’s recruiting and public relations efforts.

If your institution does determine that social networking sites are a proper place to deliver emergency notifications, several best practices seem obvious:

1. Use social networks as an *additional* delivery point for notifications, not as the sole source of notification to the community. These networks are not yet mature and reliable enough to ensure ubiquitous messaging.

2. Consider publishing a dedicated emergency account on these networks that is used only for emergency notifications and critical announcements from your institution. This keeps the current messages clearly in focus in the context of the site, and also mitigates concerns about mixing tactical notifications with recruiting outreach and public relations efforts (admittedly at the expense of having to socialize a new address to the campus community).

3. Coordinate with your marketing, recruiting, communications, and public relations staff to ensure that your institution’s mission is correctly represented on social networking sites.

Hardware Integration Paths

Hardware notification systems typically represent a large investment for campus emergency preparedness, and figure in many emergency preparedness plans — but they do present some unique challenges to your strategy and roadmap. Hardware projects move fairly slowly given lengthier installation requirements, the need for power and connectivity across widely distributed locations, and the variety of needs met by broad technologies. Older installed hardware systems may not have the rich connectivity options that more current systems can feature. Thus, hardware installations and integrations typically require longer term vision — more time to set up the network of devices, configure each device, test those connections, and integrate these devices into your campus safety protocols.

Your long term goal should be to leverage your software platform as the centralized notification console for all notifications. But it's important to be aware that due to the longer timetables, physical complexity, and other factors involved in hardware system, it will often make sense to phase in your integrations with hardware systems. Software notification is typically easier to acquire and to configure, with the majority of vendors supporting a Software-as-a-Service (SaaS) or hosted option to provide coverage for voice, text, and email based notification.

Priority one is to maximize modes of communication to reach the entire campus as efficiently as possible during a crisis. Given that the complete mix of technologies on campus are likely to be heterogeneous, a realistic timetable and project plan for hardware integrations is sensible.

Phase 2: Get up and running

Your project plan should optimize around deployment of the furthest reaching emergency notification channels first. This is the phase where you get your system up and running, and these phases involve more than simply signing a contract and turning on a notification tool. The implementation should also reflect your high level goals for notification and communication.

Major areas to consider:

- **General configuration and deployment** – System setup and core configuration, including branding, setup, buildout of notification templates, integration with authentication systems and identity management tools.

- **Loading subscriber data** into the system from student information systems -- Issues include managing change in subscriber data (adds/drops/updates); data validation steps and resolutions; keeping contact information up to date; procedures for managing undeliverable addresses; graduated or withdrawn students; managing faculty and staff usage of the system; automation of data management. Work with a vendor that supports higher-education friendly integration, is partnered with your vendors of choice, and that can provide references to other institutions who have used their automation toolset.

- **Identifying and training system administrators** – Typical institutions will appoint numerous administrators who are authorized to send emergency messages. For example, this list might include the President or Provost's office, campus security staff, IT and Telecom staff, student affairs, and designated emergency managers. Identify all users of the system, and ensure that each user is properly trained in both systems usage and campus emergency protocols. You should also ensure system availability and socialize contacts for vendor support in the event that a user has difficulty sending an alert. Premium vendors should provide 24x7x365 support for emergency notification.

- **System testing** (initial and ongoing) – Initial system confirms that all aspects of the implementation are properly configured and functioning. Full system testing typically requires a plan that pre-announces to the campus community that a test will be conducted, careful presentation of the test alert as a test, and a follow up report to report back to the community on the success of the alert. An after-action analysis should be conducted to review both the planning for the test and its execution and provide recommendations for future usage.

- **Marketing the availability of the notification systems and educating the community** – A notification tool impacts the entire campus community, so some level of program communication is required to inform subscribers of your institution's programs, how they will be used to communicate emergency information, and any further information required by the user about program operations. Again, your vendor may provide you with tools and templates to assist the marketing of your notification programs to the campus community.

- **Ongoing support of subscriber information** – Subscriber data changes frequently, and keeping contact data up-to-date should be an important priority for your team. This means ensuring data feeds are current, that contact data in your SIS or ERP systems is also current, and that data is validated to the fullest extent when it enters the system, either from end user subscribers, or from an automated system. Reports and automation can assist. Certainly, once an alert is sent, undeliverable numbers should be reviewed to determine currency. Vendors should also endeavor to address contact integrity and data cleansing programmatically.

Rave Mobile Safety's "Best Practices in Emergency Notification" provides an excellent overview of the emergency preparedness practices that inform your system deployment and provide further support for this aspect of your roadmap. Please see that document for further detail covering the implementation and testing of your notification systems.

Phase 3: Expand Messaging Modes

Since you've already prioritized the highest impact messaging modes in your planning, once your system is deployed you can then begin working on enhanced capabilities. You might decide to tackle your voice system next; tie in to a safety beacon initiative that can project sound and text into each classroom via radio, Ethernet, or WiFi. Perhaps your campus hospital has requested some new precautions be enacted around pandemic alerting in response to the H1N1 or some other medical threat.

Again, safety is not a one-time occurrence. Threats and risks emerge or are re-prioritized within your campus community. New technology systems may be brought in by campus security, student affairs, or other groups on campus. Crime waves (of any size and severity) might lead to specific new crime prevention initiatives across the campus.

How do you prioritize delivery modes and determine which to pursue first as additional communication channels?

Again, consider under-served or exposed areas within your overall emergency plan. Are there areas or sub-populations on campus that have specific communication needs? For example, you may discover that notifying dormitory populations of water advisories or other public works issues has emerged as a shortfall. You may also have discovered that your LCD displays recently placed in key buildings around campus would be ideal to integrate into your messaging strategy.

Prioritize such needs via a plan that factors some measure of the complexity of implementation against the ability to reach sizable sub-populations on campus with the greatest exposure to critical risks, the greatest inconvenience factors in mass communication, and the least exposure to alternative means of receiving time-critical communications.

You may also decide to investigate any application programming interfaces (APIs) that allow IT staff to access your notification systems programmatically from institutional applications. Each vendor's tools are likely to differ substantially, but campus IT will typically identify potential applications that can derive benefit from integration with your notification tool. Many institutions take an experimental approach here, and allow a small team to attempt integrations in prototype applications. These are tested and deployed when they have proven their value. When the need exists, however, these integrations may provide a keen advantage to the campus community and allow institutions to customize aspects of the notification system to achieve very targeted and campus-specific application goals.

Once your priorities are set, revise your plans to include these newly prioritized phases of your plan.

Centralized Console

As you progress, it's valuable to organize all your systems around a single centralized console so that alerting is done from a single interface, a single location that can reach out among all the available methods of communication. This ensures that technology is working most efficiently, reduces the risk of operator error when alerting, and consolidates monitoring and reporting on an event within a single interface, allowing your staff to focus on the incident more than the software and hardware tools.

Again, it may take some time to reach a fully integrated state with all of your tools, but the value of having a central dashboard view of all your notification capabilities is worth the effort. Again, look for platform vendors who have the ability to support a broad range of alerting targets and a user interface that minimizes training and maximizes ease of use.

You should also provision tools to enhance your *response capability* for any given crisis. During a critical notification event, chances are the situation will change rapidly and your responders will need to mobilize decisively. A rich emergency plan will include special communication channels to empower responders. For example, use of conference bridging to get critical security personnel, campus administrators, or emergency management teams online quickly to discuss tactical response. Organizing your first responders, at large, or targeted for specific types of response, is a worthwhile effort.

Also, look for and exploit ways that automation can improve intra- and inter-agency communication as well. Don't overlook opportunities to use your tools to connect you with other jurisdictions, local law enforcement, state agencies and information, and other coordinated resources where that can produce genuine value.

Phase 4: Narrowcast Messaging

Many institutions wrestle with the idea of using emergency notification technology for “non-emergency” or narrowcast messaging. On one side is the idea that your institution can leverage the investment in systems to extend the value of the system into other realms. On the other side is the legitimate concern that if your messaging becomes too voluminous, users may grow fatigued with the system or opt-out of all messaging in order to reduce the volume of messages broadcast by your institution. It is a serious concern, worthy of discussion and open-minded consideration among your emergency management team.

What kinds of applications might be considered? On the short list, to name just a few, are:

- Financial aid or registrar’s office deadline alerts
- Campus events management
- Learning management system integration
- Student affairs messaging
- Sports program alerting
- Athletic facilities schedules
- Academic program or departmental communications
- Campus services alerts (e.g., dining hall menus, bookstore hours, etc.)
- Student government bulletins

Students, faculty and staff may find such group messaging applications highly valuable.

Protect Your Emergency Contacts

First and foremost, as you explore the idea of narrowcast messaging, consider some of the following questions:

- How can we implement narrowcast messaging so that our emergency messaging channels remain open and protected?
- Can we provide adequate levels of opt-in configuration so that the community can distinguish between emergency and non-emergency communication, *and* that each can be controlled individually?
- Can we implement narrowcast messaging so that the subscriber has complete control over message volume?
- If we are using our messaging tools for narrowcast messaging, is the usage consistent with our institutional goals and usage policies?
- Does the proposed narrowcast usage produce justifiable value to the subscriber?

Many institutions are hesitant to use ENS in particular for narrowcast messaging, but remember that if your narrowcast messages do indeed provide value to the subscriber, that subscriber is potentially more motivated to keep their contact information up to date and will be more engaged with the system. For example, if your system can deliver assignments or grades from your learning management system as narrowcast messages, these features can prove very appealing to students and raise awareness and acceptance of your notification system overall.

Also, you do not necessarily have to view the decision as all or none. You might decide to try out narrowcast group messaging on a limited basis to determine the viability and manageability of the idea, then assess and analyze further with some real-world experience as guidance.

Phase 5: Protect Individual Safety

One phase that sometimes gets overlooked within safety planning and provisioning is to assess personal safety on campus from the perspective of inbound notification. Personal safety applications might include any of the following:

- Usage of bluelight systems or call boxes
- Mobile safety applications
- Crime reporting hotline applications
- Transit safety and safe-ride programs
- Personal protection initiatives such as campus escort or safe-walk programs
- Sexual violence prevention
- Restraining order compliance enforcement
- Individual crisis management plans
- Property protection programs

Many of these initiatives become relevent due to unfortunate external events such as crime waves, and many of these initiatives are separate from the general cycle of notification, but there is clearly a communication aspect in common among all these programs that starts with communication of the availability of the program and can extend into more interactive applications.

The reason to factor personal safety into your overall roadmap is that, increasingly, inbound and outbound communication will converge around your safety programs, technologies, and applications. Clearly, your personal safety programs are a critical component of the overall safety provisioning that your campus presents to its community, so it makes sense to consider personal safety as part of your overall roadmap for notification and communication with the campus community.

Conclusion: Constant change, subscribers are in motion

Next-Generation notification starts with the keen awareness that change is the only constant: risks change, safety priorities re-prioritize, technologies and systems change, subscriber presence is fully mobilized, and subscriber data itself, as we all know, is in a permanent state of flux. From strategy to plan to execution and implementation, preparedness means adaptability — from your staff, your planning, and your software and hardware tools.

Flexibility and configurability have a certain cost — not the least of which is the time and effort spent in your own emergency preparedness planning, coordinating resources, provisioning technologies — but the *value* of preparedness warrants the effort. That value should extend as well from your notification tools, which should give you the freedom to reorganize your plans, add new modes of delivery, integrate with existing systems so that your notifications reach the largest majority of your community. On top of all that, your notification tools must demonstrate clearly superior reliability and performance in all phases of usage.