ECAR

Emergency Notification Strategy

April 2014

Mark Katsouros
Director, Network Planning and Integration
The Pennsylvania State University
Co-chair, ECAR Communications Infrastructure and Applications Working Group

Introduction

In higher education, the IT department is often the service provider for the institution's emergency notification system (ENS) and, in that role, is tasked with ensuring that the institution is technically capable of complying with the "Timely Warning" requirement of the Clery Act, the federal statute that "requires all colleges and universities that participate in federal financial aid programs to keep and disclose information about crime on and near their respective campuses."[1] Perhaps more importantly, a notification system must support the institution's goal of keeping its community as safe as possible. For many institutions, the complexity of providing emergency notification to students, faculty, and staff makes using a local, on-premise solution unrealistic.

But finding the right commercially hosted technical solution to meet the institution's emergency notification requirements can be a difficult process, involving participation from numerous campus stakeholders, including university police, public relations, risk management, and general counsel. Indeed, figuring out the procedures and processes that make the system the most effective possible while balancing interests from different stakeholders may mean that working with the technology itself is one of the easier components of this undertaking.

With the public-safety stakes as high as they can be, the need for a complete solution is essential. Valuable lessons can be learned in the process, not only along the road toward the technical implementation, but also in terms of defining the actual policies, procedures, and roles surrounding this critical function. Learning from these lessons results in a robust, optimally effective emergency notification implementation and set of procedural best practices, keeping the institution's community informed of threats to public safety and thus as out of harm's way as possible.

The following are top ENS technology strategies to consider when determining the best notification system for your institution, along with recommendations that will help you make implementation and usage decisions.

EDUCAUSE

Single Mode vs. Multimodal

Some of the hosted (or SaaS, Software as a Service) emergency notification solutions focus solely on text messaging—in the form of mobile phone text messaging, or Short Message Service (SMS)—and e-mail. While SMS/text might be the most reliable, scalable modality, it should not be the only one upon which your institution relies. Given the broad range of messaging options and notification technologies available today, providing a multimodal solution dramatically increases the chances of reaching more people sooner, not only because of the diversity of individual communication preferences and capabilities but also because of the greater resiliency achieved in not relying on only one or two communication infrastructures. In addition to text, consider landline and cellular voice, indoor and outdoor loudspeakers/sirens, digital signage, websites, social media, and others. In addition, all of the modes should be controllable from a single console (or as few control points as possible) to reduce the time it takes to initiate a multimodal notification.

Emergency Only vs. Casual/Other Use

It's vitally important that the system that you deploy is dedicated exclusively to emergency communications so that these messages can be certain to get to the recipients without getting lost in an overfull inbox or, worse yet, a spam folder. Even if people opt in to receive non-emergency messages, "mixed messages" dilute the most important stuff. There are plenty of other mechanisms for non-emergency announcements, such as LISTSERVs and websites. Reserve your ENS for emergencies only, so people will treat those messages as having the utmost importance.

Templates vs. On-the-Fly Wordsmithing

There isn't sufficient time to create well-thought-out, well-crafted messages during an emergency. Preparing messages in advance and in the form of preapproved templates will ensure that you get your message out as quickly, clearly, and easily as possible. You will want to establish a broad collection of templates to account for all foreseeable emergency scenarios (active shooter, armed suspect, bomb threat, earthquake, flood, hazmat, hurricane, tornado, winter weather emergency, etc.) but also for the various modalities (e-mail, enunciated voice, text, tweet, etc.). By crafting template messages in advance, you also are afforded buy-in on the wording from all major stakeholders, from legal counsel to public relations to risk managers. Make sure that when you choose an ENS that it supports templates.

Text-to-Speech Enunciated vs. Recorded-Speech Notifications

Just as wordsmithing an appropriate message from scratch is difficult during an emergency, trying to record a calm, cohesive voice message during an emergency can be equally challenging. Variable specifics of an emergency, such as the location of the activity, can prevent you from recording in advance, limiting your ability to provide important messages during an emergency. Enter text-to-speech enunciation, which has come a long way since its early days of stilted computerized speech. Some ENSs will even support a preamble—a short statement that comes before any real alert—which can be recorded by a voice of authority, such as "This is University Police Chief John Doe; please listen to this important alert," adding credibility to the machine-generated message that follows.

Opt-Out vs. Opt-In

Do you want to make your ENS an opt-in (so that the default is to not receive the notifications) or opt-out? This is the difference between having a near-zero subscriber base and a near-100-percent subscriber base. By all means, default to having everyone signed up for all modalities, and allow them to opt-out where they want—your constituents are far less vulnerable having not opted out versus having not opted in.

Policies and Procedures vs. Just Technology

Again, the technology is the easy (or at least easier) part. Fully developing and documenting your emergency notification policies and procedures, including identifying who is authorized to initiate notifications and who is trained in the mechanics of sending them, is critically important. Well-documented communication and marketing plans, testing procedures, and overall notification policies are critical to ensure consistent on-boarding, a verifiably functional system, and a clear understanding of when and how the system will be used.

Consistent and Explicit vs. Irregular and "War of the Worlds" Testing

Notifiers should test at the start of every shift by sending a test message to themselves, and those messages should never mock a real emergency scenario, just in case they are distributed by accident. A good test message should look something like this: "This is test of the University Emergency Alert System. This is only a test." And, again, it should be sent by the notifier to him/herself. (You do not want to bombard the campus community at large, nor your communications infrastructure, nearly so regularly. Such broad testing should only occur once per semester at most.) This regular, individual testing ensures that notifiers have the access and the familiarity they need to competently and swiftly initiate a notification and that the system, with all of its complex integrations, continues to function as expected.

For more, in-depth information on emergency notification and the emergency communications realm in general, including the Clery Act, you can see the recording of and access the slides from a February 2013 *EDUCAUSE Live!* webinar on the subject: http://www.educause.edu/library/resources/emergency-communications-management-and-clery-act.

If you are interested in the broad topic of Communications Infrastructure and Applications (CIA), consider joining the ECAR-CIA Working Group: http://www.educause.edu/ecar/ecar-working-groups/communications-infrastructure-and-applications-working-group.

---

[1] "Clery Act," *Wikipedia*, *http://en.wikipedia.org/w/index.php?title=Clery_Act&oldid=593037565*.