MARGOLIS HEALY
& ASSOCIATES
SOLUTIONS FOR SAFE CAMPUSES

How to Develop the Right Alert Notification Strategy to Keep Your Campus Safe and Informed

by
Dr. Gary J. Margolis & Steven J. Healy

There is little debate that mass notification is the area most influenced by the loss of life at Virginia Tech in April 2007. Not since the installation of emergency "blue light" phones on campuses has there been such a push in security technology, due to campuses being criticized for not having such tools readily available in short order.

While high technology security and safety solutions have many benefits, institutions of higher education should use an array of methods to disseminate information to the campus community during urgent situations. Universities and colleges should not depend solely on high tech solutions (i.e., multi-modal communication through personal digital assistants, e-mail, voicemail, etc.), but instead strike a balance between these systems and low-tech solutions, such as flyers, loudspeakers, etc., when appropriate. In order to maintain consistent communication, there must be multiple ways to share information that meet the following criteria.

First, an urgent communication service should enable a campus to notify its entire university community via multiple channels. It should be capable of reaching students, staff and faculty through multiple points of contact, including voice messages, e-mail, Short Message Service (SMS) communications, public address systems, and more. However, when selecting and implementing an alert notification platform, it is important to keep in mind the limitations of high technology solutions. For example, SMS–a communications protocol allowing the interchange of short text messages between mobile telephone devices–was intended as a one-to-one communication strategy, not one-to-many. This creates challenges when the technology is taxed beyond its design. Likewise, without an acoustic engineering study the installation of a public address system may result in inefficient coverage and penetration.

Systems must also have the capacity to deliver messages in a timely manner. For instance, the backend infrastructure that requires aggregators and other transmission support protocols must be examined to ensure that the service providers have eliminated choke points. The service provider may have done what was needed to ensure that adequate servers can send parallel messages through enough phone lines, however, none of this will matter if the university has only one pathway through which the phone company can communicate to the desired geographic area. When telephone lines are destroyed, delivery is thwarted. Having a system that can send 20,000 text messages during a critical event is only effective if it can do so in seconds, not hours. If the service provider does not have the capacity via its own hardware or service level agreements (SLAs) with contracted support, then the system could fail. An alert notification platform should be tested at least twice a year, or more, depending on the campus community's unique demographics.

Since institutions tap into affiliate records, appropriate security and redundancy should be implemented. Colleges and universities that use a third-party vendor must ensure that access to private student and employee data is limited only to authorized personnel. Some institutions will arrange for nightly, secure data file-uploads to the vendor. These files contain the daily changes to personnel and student records, to ensure the institution has the right contact information on file properly notify recipients. Simply, it is not effective to have the right message delivered at the right time to the wrong number or the wrong person. Additionally, a notification system must have redundant capabilities in all power interconnects. Much like institutional computer systems that have multiple clean power sources and required backups, vendors must ensure their mass notification servers are similarly equipped whether it be their own hardware or infrastructure accessed through a service level agreement (SLA). For those institutions that choose to host their own servers, the same principles apply.

It is vital that a selected vendor provide an institution with 24/7 client care. The support relationship between the institution and the vendor should be constructed contractually to include training, customer service and technical assistance. It should not be assumed that users can operate the system properly without instruction. While the interface should be straight-forward and user-friendly, various means and methods for support for the systems' users should exist, especially for the initiators of the message and those responsible for managing data file uploads.

After the Virginia Tech tragedy, the number of mass notification vendors seemed to grow exponentially in a matter of hours. Those looking for a system that is a good fit for their campus should select vendors that have significant experience disseminating timely alerts at institutions of various sizes across the country. A reputable vendor will be able to demonstrate its experience and provide the necessary references.

An alert notification service should also have an assessment tool that reports on the system's effectiveness. A university should be able to see how many messages were delivered, in what time, and to what devices. Two-way messaging is also an important aspect of an alert system, enabling students, staff and teachers to receive messages and respond, letting emergency personnel know if they need assistance.

Lastly, campus public safety officials and other appropriate administrators should have the authority and capability to send emergency messages from on and off campus, or from any location around the world. In today's technologically-advanced environment, communication should not be hampered because the appropriate person is not physically on campus to initiate a message. Campus administrators should consider the following criteria before sending emergency messages: (1) the message should alert and be timely; (2) the information must inform and direct; and (3) the notice must reassure. Recipients of emergency messages should be urged to inform others.

When establishing a campus urgent notification strategy it is important to consider the capabilities outlined above. Having the right system in place will keep students, staff and faculty aware of important information in a quick and efficient manner.

Dr. Gary J. Margolis is the former Chief of Police at the University of Vermont, and a noted campus security expert. Steven J. Healy is the former Director of Public Safety at Princeton University and a noted campus security expert. Together, through Margolis, Healy & Associates, LLC they work with universities and colleges around the country on a wide range of security and safety related issues unique to educational environments. Margolis can be reached at Gary@Margolis-Healy.com and Healy can be reached Steven@Margolis-Healy.com. Their website is http://www.Margolis-Healy.com.