MARSH

MARSH MERCER KROLL
GUY CARPENTER OLIVER WYMAN

January 2009

Emergency Notification Systems

Compiled by:
Fiona Raymond-Cox
Senior Vice President
Fiona.Raymond-Cox@marsh.com
(415) 743-8644

Robyn Giannotta
Associate Consultant
Robyn.Giannotta@marsh.com
(212) 345-5598

Contents

White Paper Abstract

Recent human-caused and natural disasters have demonstrated the need for comprehensive communications procedures as a part of any emergency response, crisis management, and business continuity planning initiative. Emergency notification systems have proven to be effective tools for crisis communications. With many vendors in the marketplace, choosing the right system for your organization can be a daunting task. This paper identifies the considerations fundamental to selecting the best system to fit your organization's needs, and explains how emergency notification systems work.

1. Introduction

One of the most critical elements of any disaster recovery or business continuity plan is an effective crisis communications procedure. Reliable communications during a crisis can save lives and help facilitate the successful recovery of business functions. More and more, organizations are turning to automated messaging or emergency notification systems to facilitate crisis communications.

In the aftermath of events such as Hurricane Katrina and the Virginia Tech massacre, organizations are searching for effective tools to assist during a crisis or high stress situation. In addition, many industries are experiencing increased standards[1] that mandate the use of an emergency notification or similar system. These systems can yield immense benefit for an organization, though it is imperative to select the right vendor to address your specific needs.

> “Emergency notification systems are effective tools to assist during a crisis. Moreover, there are increased regulations mandating these or similar systems.”

There are many system providers in the marketplace and many more are emerging. Features and configurations for each product vary and should be examined against the priorities and needs of the organization before selecting a vendor. This report provides an overview of emergency notification systems and their features.

The report is divided into the following sections:

- Basics of Emergency Notification Systems
- Features
- Trends
- Lessons Learned

We also provide information on how Marsh Risk Consulting’s Business Continuity Risk Management Practice works with clients in assessing their needs for and implementation of emergency notification systems.

1 These standards include:
- NPFA 1600 - Standard on Disaster/Emergency Management and Business Continuity Programs 2007 edition (See Section 5.10 Communications and Warnings);
- Public Law 110-53 - Title IX: Private Sector Preparedness, August 3, 2007;
- Sloan Foundation - Framework for Voluntary Preparedness: Briefing Regarding Private Sector Approaches to Title IX of H.R. 1 and Public Law 110-53 “Implementing Recommendations of the 9/11 Commission Act of 2007”;
- Standard & Poor’s - S&P Extends Comment Period on Enterprise Risk Management Analysis for Nonfinancial Corporation Ratings - January 14, 2008; and
- Standard & Poor’s - Enterprise Risk Management for Ratings of Nonfinancial Corporations, June 5, 2008.

2. Basics of Emergency Notification Systems

Uses

Numerous academic, public, and private sector organizations are turning to emergency notification systems as a tool to facilitate crisis communications and disseminate routine notifications. These systems can be utilized to streamline communications. For an academic institution, this may include communicating with students during an incident through to surveying parents. For a public or private organization it may be used to execute a phone tree, solicit donations for a charity, or manage communications during a crisis. The concept of these systems can be applied to achieve many different goals.

Terminology

When researching vendors of emergency notification systems, it is important to note the different language used in the industry. Vendors often refer to aspects of their process using different terminology than their competitors. Set out below are terms used interchangeably.

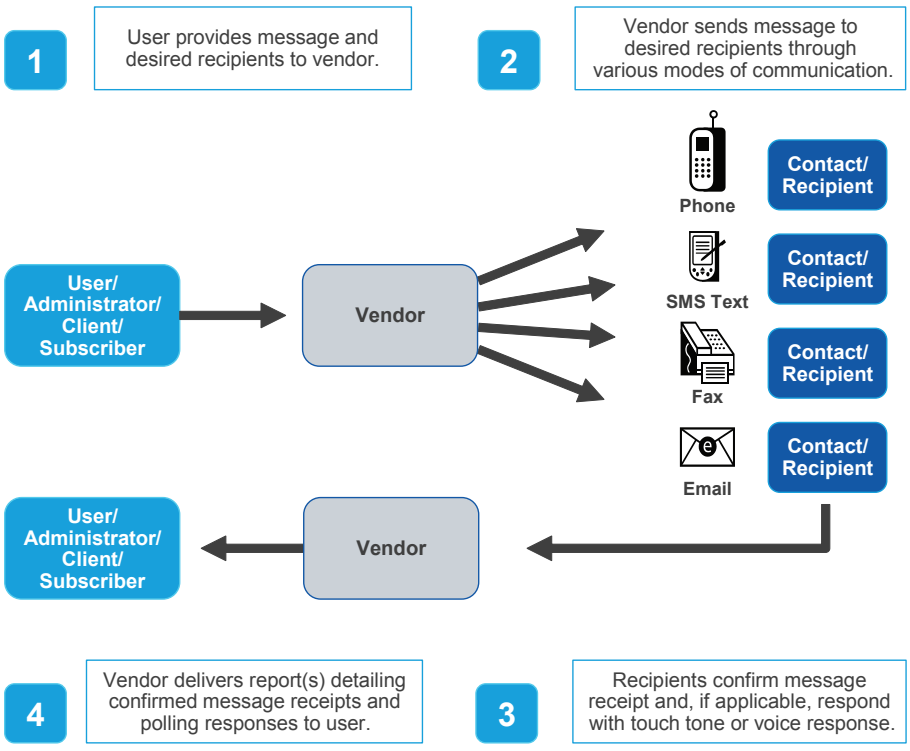
- **User/Administrator/Client/Subscriber** – All these terms refer to the individual at an organization utilizing an emergency notification system who initiates the messages. In a hosted system model (see below), this person communicates with the vendor via the phone or on the vendor's web interface in order to initiate a message.
- **Message/Notification/Broadcast/Call-out** – All these terms refer to the communications sent via the emergency notification system to pre-defined contacts. In a hosted system model, it is the message the user/administrator/client/subscriber creates and instructs the vendor to send on its behalf.
- **Contacts/Recipients** – The people who would receive the message distributed from an emergency notification system. At the start of a relationship with a vendor, an organization will provide the vendor with its 'contact lists' including the names and phone numbers, email addresses, and fax numbers of those people whom it wants to be able

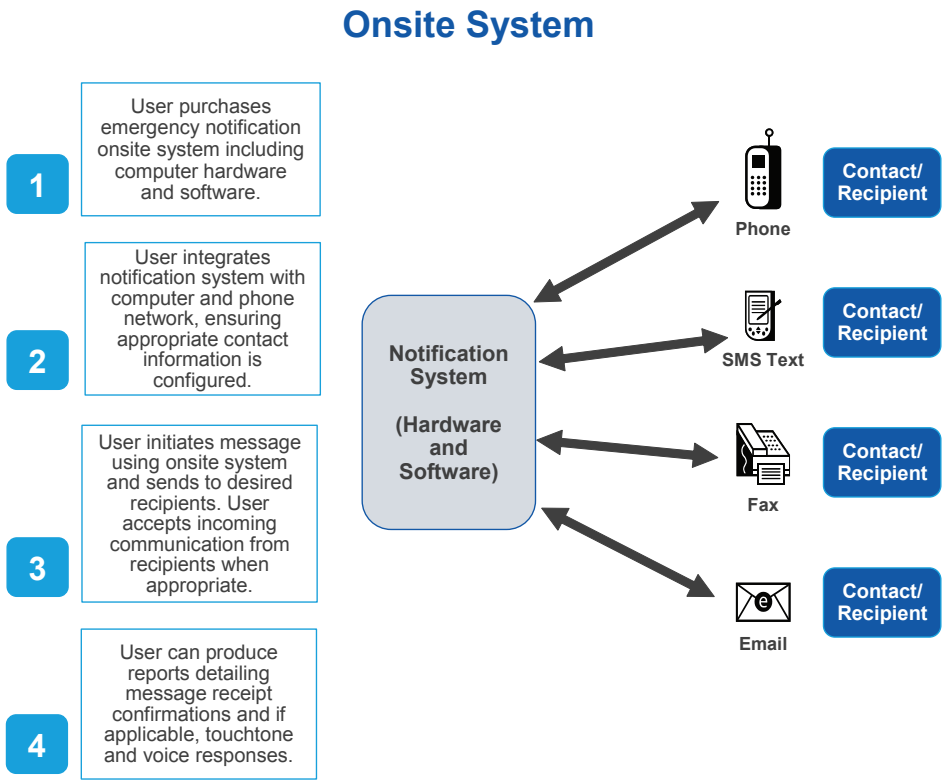
to message using the emergency notification system. When initiating a message, the contacts or recipients are chosen from the contact list provided to the vendor.

How It Works

Communications can be sent via phone, email, fax, or text to a large number of contacts in a short period of time. Depending on the vendor, they may offer a hosted system, onsite system or a hybrid of the two. Irrespective of the type of system chosen, all are capable of tracking and reporting (to varying degrees) on the response to the communication from those contacted.

Hosted System





Operating System

There are three types of operating systems used to administer an emergency notification system.

- **Hosted System** – A hosted system is housed and operated by the vendor. An organization pays a subscription fee for services and leaves the cost of purchasing the technology infrastructure and facilitating the sending of messages to the vendor. In this model, a subscribing company or organization (the user/administrator/client/subscriber) would provide the vendor with their contact lists, instructions for triggering a message, and the content of the message.
- **Onsite** – Emergency notification systems are also available for purchase to be operated by the subscribing organization. An onsite system requires the purchase or lease of the computer hardware and licensing software to run the notification system. These systems must be integrated into the organization's internal phone system and computer network. Once purchased, the subscribing company or organization has the ability to use the emergency notification system at its discretion.

- **Hybrid Solution** – With a hybrid solution, the subscribing company or organization purchases the hardware and software needed to operate the emergency notification system. In addition, the subscribing company or organization maintains an agreement with the vendor that allows the subscriber the opportunity to "borrow" additional call capacity if needed. A hybrid solution operates most similarly to an onsite system, but includes additional services from the vendor.

Hosted Versus Onsite

A company or organization should carefully weigh the pros and cons before making a final selection for a hosted or onsite operating system. The two operating systems yield a different set of benefits and challenges. Below is a comparison of some of the more significant differences between the operating systems.

	Hosted	Onsite
Pricing Structure	Requires annual subscription fee, usually based on the number of contacts and desired level of usage. Some vendors charge an initiation fee and flat fee for the anticipated number of messages to be sent per year.	Capital investment for system purchase and software leasing. Additional expenses incurred with training staff, system upgrades, maintenance, technical support, and maintaining phone lines.
Technical Expertise	Virtually no technical expertise is required. Free training and customer services often included in subscription.	Requires integration with company phone and computer network systems including any relevant applications containing contact information. Technical expertise needed to configure system with phone lines and ports. Technical expertise needed to operate system, install upgrades, and troubleshoot.
Risk of Unavailability	Hosted system vendors maintain redundancy of phone lines and ports to ensure the systems are rarely or never incapacitated. To access the services of a hosted emergency notification system, phone or internet access is needed.	Onsite systems are dependent on the reliability of local telephone lines and ports. An event that disrupts phone lines could disrupt the ability to send messages with an onsite system. It is important to note that an onsite system located at a facility that experiences a disaster could be rendered useless.

3. Features

Emergency notification systems are sophisticated applications with many features. With technology rapidly evolving, the capabilities of these systems continue to expand. Some systems provide comprehensive business continuity solutions, while others are designed only for sending one-way communications.

Below is a list of features commonly found in emergency notification systems.

- **Message Initiation** – Messages can be initiated through a number of modalities. All vendors allow message initiation over the phone. Some vendors allow users to initiate a message through a web interface, email, fax, or text message.
- **Multi-Modal** – Most systems are designed to send voice and text-based messages through multiple methods of communication including phone, fax, text, email, pagers, PDAs, Blackberry, SMS, VoIP, and more. Only a few systems continue to send only phone calls.
- **Message Delivery Features** – Most vendors allow users to save message templates and schedule message delivery for a later date and time.
- **Languages** – Some vendors allow language conversion through a text-to-speech function. Users can type a message in a foreign language and the system will dictate the message in the proper language with a simulated human voice.
- **Two-Way Communication** – Most vendors allow inbound communications so that those contacted can respond to the message with either a touch tone or voice response. In-bound communications allows vendors to poll contacts to determine their receipt of the message, their safety, status, location, or any other information.
- **Reporting** – All vendors provide reports detailing which of the contacts received the message and which did not. Some vendors offer more detailed reports including the number of call attempts to reach a contact and other metrics. For hosted systems, vendors can

compile and produce reports of two-way communications responses upon request.

- **Notification Escalation** – Some vendors offer the ability to customize escalation procedures and designate first, second, and third points of contact for each recipient. With this feature, the message will be sent to the first point of contact and if that number or address is unavailable, the system will automatically send the message to the next point of contact.
- **Control of Contact Data** – Some vendors offer a subscribing company or organization the ability to allow their contacts to access the system and update their own contact information. This feature helps relieve the administrative burden on the subscribing company or organization's user.
- **Call Bridging** – Many vendors provide the ability to initiate a conference call bridge on demand. This feature is useful during crisis communications when multiple members of an organization may need to coordinate by conference call right away.
- **Geographic Information Systems (GIS) Capability** – GIS is an information system capable of integrating, storing, analyzing, and displaying geographically referenced information. For emergency notification, GIS technology can allow a user to send geographically targeted notifications to a portion of its contacts by selecting an area code or postal code.

4. Trends

The market for emergency notification systems is constantly expanding. With increased regulatory requirements in a number of industries, demand for emergency notification systems is growing and the market for providers is far from saturated. With multiple vendors emerging and technology evolving, new capabilities and trends are occurring.

- **ASP to SaaS Configuration** – A new trend in technology is for service providers to move from an Application Service Provider (ASP) format to the Software as a Service (SaaS) configuration.

  An ASP transfers a customer's suite of applications and hosts them in a large data center. Hosting many different customers' applications, ASPs were often overloaded and the infrastructure failed under the high cost of maintaining so many different applications at once.

  SaaS is a model of software operation where an application is hosted by a service provider and is accessible to many customers over the internet. With SaaS, the format has shifted to service providers owning and maintaining the applications and customers going directly to them for a hosted service. This system allows for reduction in cost to the subscribing company by eliminating the need to purchase the application up front. Secondly, it allows service providers to control the number and types of applications they host, thus ensuring their infrastructure can handle the management and maintenance of the systems.

  From an emergency notification system perspective, the SaaS approach offers increased reliability. The SaaS configuration tends to improve the speed and reliability of a vendor's web interface. This increased speed and reliability ensure that a user of an emergency notification system can access the vendor's web interface without delay to initiate a message.

"From an emergency notification system perspective, the SaaS approach offers increased reliablility."

- **Languages** – Many emergency notification system vendors offer a text-to-speech function that will dictate a notification in a foreign language. Vendors are currently expanding this feature and the

trend indicates that soon users of these systems will be allowed to select from a number of languages and have their message automatically translated before delivery of the messages.

- **Increased Server and Port Capability** – The value of an emergency notification system lies in the ability to send and receive large numbers of messages quickly. Many systems, particularly onsite systems, have experienced delay or overloading when receiving incoming responses to a message. Vendors are increasing capability for their servers and ports and establishing geographically dispersed back up data centers in order to maximize the reliability of these systems.

5. Lessons Learned

Our experience has shown that the implementation of an emergency notification system is best achieved through a five step process. This process includes the selection of the right product, initial set up of the system, message development, and recording and sending. Set out below is a list of lessons learned.

> “Implementing an emergency notification system is best achieved through a five step process.”

Product Selection Process

- **Adopt a collaborative approach** – Involve all interested parties (e.g. IT, HR, Finance, Emergency Response Team, Crisis Management Team, Corporate Communications, local emergency officials, etc.) in the decision-making process. Define roles and responsibilities for the individuals involved.
- **Document requirements** – Before venturing out to the marketplace, agree upon the intended usage of system. Estimate the anticipated number of recipients and corresponding number of messages to be disseminated on an annual basis. Determine if the organization has the technical resources in-house to manage an on-site system. Assess if the emergency notification system will integrate seamlessly with existing systems/applications. Finally, decide if cost is a key factor.
- **Integrate the emergency notification system with existing programs** – Ensure the product selected will be suitable for emergency response, crisis management, disaster recovery, and/or business continuity activities.
- **Product demonstrations** – At a minimum, ask each vendor to demonstrate the capabilities of their product with sample data. Some vendors will allow a free trial for a defined period of time prior to purchasing the emergency notification system.

Minimize System Setup Errors

- **Product integration** – Wherever possible, integrate the emergency notification system with existing systems/applications containing the recipients’ information as this will limit the likelihood for human error should data need to be re-keyed from one system to another.
- **Recipient services** – Some emergency notification systems allow the recipient to maintain their own contact details. Whenever possible,

put the onus on the recipient to update/validate personal information in the emergency notification system.

Crafting Messages

- **Establish messaging guidelines** – The Crisis Management Team, usually in conjunction with Human Resources, Corporate Communications, and Legal should decide on strict guidelines for usage of the emergency notification system. To avoid sending misinformation or prematurely sending unsubstantiated information, the organization should have detailed criteria for what is considered an emergency, how many people need to approve the message content, who may record the message, and who may authorize the release of the message.
- **Draft emergency messages ahead of time** – Prepare several pre-scripted emergency messages that the organization may likely send out. Ensure messages are concise and accurately explain the crisis situation. This will save wasted time drafting and approving an emergency message at a moment's notice.
- **Use the 3-3-30 rule** – Keep messages short and direct. In an emergency message write no more than 3 short sentences that convey 3 concepts in 30 words or less.
- **Identify message as an "Emergency"** – If the emergency notification system would be used for more than crisis communications, it is good practice to highlight that the message is related to an emergency. Make sure messages are direct, accurate, and urgent. If applicable, include a source to receive additional information.
- **Vet messages** – Validate the content of the message with another person before it is sent out.

Recording and Sending Messages

- **Record messages** – Ensure the message is recorded by someone with a clear voice and calm manner.
- **Keep track of emergency messages sent** – Most likely an organization will send more than one message during an emergency. It is a good practice to number each message or at the beginning of each message, state the time so that recipients can ensure they receive each emergency message in sequence.
- **Vary methods of communication** – During an emergency, phone lines can go down and websites can crash. Emergency messages should be disseminated in a variety of formats such as SMS text, email, and phone call.

Practice/Prepare

To fully realize the benefits of an emergency notification system, practicing sending a message is crucial. Without continuity of process and comfort with the system, sending a message during a crisis will present challenges.

- **Create a training program** – Train designated personnel to use the system, including how to access and update recipient lists. Develop a "how to" manual and checklist and make them available in hard and electronic copy. Include these instructions in your organization's Crisis Management Plan and store a copy off site.
- **Test the hosted emergency notification system** – If using a hosted system, be sure to test the system you have selected at the beginning of your relationship with the vendor. Without notifying the vendor, a message should be sent to all recipients. This will test the server load and delivery capability of the vendor.
- **Conduct real time tests** – Train as you will execute. It is crucial to test the system in a simulated emergency situation so that issues and challenges that need to be addressed are realized before an event occurs. Document the outcome of each test and follow up all remedial action items.
- **Monthly practice** – Individuals involved in the Emergency Response, Crisis Management, Disaster Recovery, and/or Business Continuity activities who will be responsible for sending emergency messages should practice using the system monthly. It is crucial to test the system frequently to ensure processes are effective and users understand their roles.

Misuses

Misusing an emergency notification system can upset the recipients and diminish the credibility of urgency in your emergency messages.

- **Overuse** – Often times, organizations use an emergency notification system for more than just communications during a crisis. While this is legitimate use, it is imperative that the organization ensure that the recipients understand when there is urgency with a message. Overusing the system can cause recipients to not listen when a real emergency message is sent out and therefore not act on important instructions.
- **Over-reliance** – As a general rule, it can be dangerous to rely too heavily on technology during a crisis or emergency. It is good practice to maintain other avenues for communication in addition to an emergency notification system. The use of blow horns, fire alarms, and loudspeakers are effective back up methods of communication should all else fail.

6. How Marsh Can Help

At Marsh Risk Consulting, our Business Continuity Risk Management consultants can assist your company in acquiring all the tools necessary to ensure your business is truly resilient. In addition to developing a robust business continuity program, we can help you find an emergency notification system that not only fits your needs, but fits your budget as well. To find out how Marsh Risk Consulting can help protect your company from the potentially devastating effects of a business interruption, please contact your local Marsh representative or Fiona Raymond-Cox, Senior Vice President, Business Continuity Risk Management Practice at (415) 743-8644 or **Fiona.Raymond-Cox@marsh.com.**

MARSH

MARSH MERCER KROLL
GUY CARPENTER OLIVER WYMAN