

SUNGARD AVAILABILITY SERVICES

White paper

**Choosing, deploying & managing
an emergency notification system**

Summer 2004

How to use this whitepaper

The “Choosing, Deploying and Managing an Emergency Notification System” white paper is divided into four major sections designed to help your organisation successfully select, deploy and manage your emergency notification system.

Section I: What is an emergency notification system?

In today’s tumultuous world, it’s in every organisation’s best interests to deploy an emergency notification system that will help save lives, property and capital during times of crisis. This section of the report describes the need for emergency notification and the evolution of today’s nimble, technology-based solutions.

Section II: Selling management on emergency notification

The benefits of an emergency notification system aren’t always readily apparent to top management. This section reviews various approaches that can be taken to convince them of the need.

Section III: Selecting an emergency notification system

Once the need for a notification system has been established and implementation approved by top management, a dizzying array of choices awaits your organisation. This section covers key factors to consider in the selection process.

Section IV: Deploying, optimizing and managing your emergency notification system

Even the best emergency notification system won’t work well in a crisis if it isn’t properly deployed and maintained. This section describes deployment and management considerations that will help you optimise your system.

Section I

What is an emergency notification system?

*Turning and turning in the widening gyre
The falcon cannot hear the falconer;
Things fall apart; the centre cannot hold...
(William Butler Yeats, "The Second Coming")*

Change happens. The only certainty in life is that there are no certainties. One of the hardest lessons from the 9/11 terrorist attacks, according to an official of the New York City Office of Emergency Management, is that even the best-laid plans don't allow us to predict what's going to happen. The only guarantee is that it won't happen the way you plan it.

In today's tumultuous world, your organisation's ability to respond to unexpected change will dictate its ability to circumvent that change as it occurs. One tenet of contingency planning/disaster recovery is the notion that if you can't communicate, you can't recover. But during a crisis, you don't know how or if you'll be able to communicate. That's where emergency notification comes into play.

From a classic command and control perspective, emergency notification systems provide senior leadership with the ability to respond, direct and manage during a time of crisis. If the leaders can coordinate their efforts and get information out in a timely fashion, they can save lives and money.

The next-generation call tree

Technology-based emergency notification systems can be thought of as next-generation call trees. To get the feel for a call tree, imagine a notification scenario in which school must be cancelled for the day due to snow. Ten parents are responsible for calling and reporting the snow day to ten other parents, who are then responsible for passing the message on to ten more parents, and so on. Each link is at risk—and if one breaks, the impact is exponential. Many parents may not get the message. Without an audit trail, there's no way to determine where the break occurred.

By automating this process, emergency notification technology enables fast, accurate strategic communication delivery that is documented, auditable and repeatable. It's also actionable, providing information to people in time to make a difference.

A company with an automated emergency notification system in place could more effectively get the word out about a snow day, for example. Employees could be reached where they are in the manner they've chosen to be contacted—on their home phones, mobile phones or pagers. If one method doesn't get through, the system automatically attempts a backup channel. After all, what use is the system if an employee never gets the message? An auditable record documents which employees were reached and the channels used.

A variety of notification applications

Organisations in industries with critical infrastructure must enact emergency communication plans by mandate, for example, per the Homeland Security Act in the U.S. and other regulatory statutes. If a spill, gas leak or fire occurs at a power plant, for instance, that organisation has a fiduciary obligation to notify people of possible toxic emissions.

Other scenarios in which emergency notification systems can play a critical role include medical alerts—such as for an Alzheimer's patient who's wandered from home—and Amber Alerts for missing children. From technology failures and computer viruses to natural and man-made disasters, emergency notification gets information out in real-time to the people who can use it.

A world of evolving notification system choices

Historically, one communications company has been the market leader for 22 years. Their solutions, which feature legacy customer premise equipment, are now giving way to newer, more nimble technologies.

The good news: Organisations have their choice of notification systems in a rapidly commoditizing marketplace.

The bad news: With choice comes market noise, making discernment among solutions and vendors more difficult.

This report outlines what you should look for in an effective emergency notification system, as well as how to deploy, optimize and manage the solution of your choice. But first things first: How do you sell upper management on the idea?

Section II

Selling management on emergency notification

Top management at your organisation understands the importance of communicating with and disseminating information to the workforce during a disaster. As a result, you've been handed a substantial budget for an emergency notification system. Congratulations! The hardest part of the disaster recovery implementation battle has been won. You can skip the rest of this section and go on to Section III, "Selecting an Emergency Notification System."

The reality: Organisations that inherently understand and budget for effective emergency notification systems are few and far between. A world-class notification system doesn't usually make an obvious positive impact on the bottom line. Because a disaster recovery system yields no direct ROI, the budgetary purse often remains closed.

All is not lost, however. Depending on your organisation's circumstances, one or more of the following approaches should convince management of the value and critical role played by emergency notification:

- A compelling event
- Regulatory compliance
- Appeal to leadership values
- Tie-in to day-to-day operations
- Threat and risk assessment

A compelling event

Has your organisation experienced a compelling event that could have been better handled with an emergency notification system in place? In the wake of crisis, management is always more receptive to considering such a system. Organisations anticipating a compelling event—such as those located in politically unstable parts of the world—are also likely to embrace some kind of notification system.

The 9/11 attacks on New York City and Washington, D.C. were wake-up calls in terms of emergency notification. On evacuating the World Trade Centre towers, company officials had no means to conduct virtual roll calls or rendezvous to account for staff. Now, those same companies appreciate the need for automated call trees and other features of emergency notification systems.

Regulatory compliance

Another factor actually forces management to implement an emergency notification system: Imposed external pressure from the government or regulatory bodies. Statutes and regulations increasingly dictate the existence of crisis communication notification plans.

By law, for example, organisations with critical infrastructures—such as chemical companies and power plants—must put emergency notification systems in place. As part of the accreditation process, many school districts require individual schools to prepare crisis communication plans. Such plans enable the schools to reach out to parents, vendors, and the district office in case of violence or other compelling events. An association of automotive manufacturers might require supplier-to-vendor emergency notification mechanisms that ensure the availability of critical parts.

Appeal to leadership values

When it comes to persuading management to adopt an emergency notification system, an appeal to leadership values could work to your advantage. Most managers equate communication with leadership. Notification systems extend communication in times of crisis.

Also, most executives wish to show that they care about people—their employees, partners, and vendors. That care includes the health and safety of the workforce. Even the best processes, systems and infrastructure are only as good as the people at the controls. The threat of harm striking those people may be enough to encourage managers to look into emergency notification.

Tie-in to day-to-day operations

Management may very well embrace a notification system if the IT department can tie it in with daily production or activities. Such a system can provide ROI while harbouring emergency notification mechanisms in case of disaster. Also, if your organisation equips employees with mobile phones, two-way pagers and wireless e-mail devices, the deployment of an emergency notification system will provide another justification of the expense.

U.S. law firm Wilson Sonsini offers a good example of how an organisation can use its emergency notification infrastructure in day-to-day business operations. Attorneys, associates, tax partners and researchers all over the country tap into the system for daily business communication and to set up deal teams. If something goes wrong in an office, the same notification system allows them to reach out quickly and mitigate the disaster.

Threat and risk assessment

If none of the previous strategies convince your management to implement an emergency notification system, you can still appeal to them with a well-researched risk and threat assessment. Prepare a business impact analysis (BIA) of disaster scenarios that could threaten your business along with corresponding mitigation strategies. Identify threats and risks, pair those risks with probabilities, and quantify costs to the organisation should the disaster scenario come about.

Note that desperate circumstances only get more severe if the stricken organisation can't deal with a problem quickly using the best information available. Wrong decisions are more likely to be made in a vacuum. The duration, frequency and impact of a crisis event—along with the cost included in your risk assessment—can be radically lessened with the right emergency notification solution. A strategic, critical information delivery plan always transcends a reactive crisis response in terms of time and cost savings.

Mutual fund trader T. Rowe Price applied risk assessment to a scenario that involved its credibility. Each day after the market closes, the company must price the net asset value of its funds and get that information out to the wire services. If T. Rowe Price misses this “Golden Hour,” newspapers all over the world won't print its mutual fund prices the next day—something that's only happened once in 100 years. Not wanting to risk its reputation, the fund trader chose to lessen the threat by implementing an emergency notification system. Now if disaster strikes at the company's centre of operations, fund pricing news still gets out to the press in time.

Section III

Selecting an emergency notification system

Management has given you the green light on implementing an emergency notification solution. But with more than twenty different notification systems on the market, how do you choose the right one for your organisation?

In selecting an emergency notification system, you should take a number of factors into consideration. Each factor encompasses benefits and tradeoffs in terms of system architecture, features/functionality and pricing. (See Chart 1 below.) You should examine them in light of the unique needs, resources and risk tolerance of your organisation. Notification selection factors include:

- Hosted vs. self-hosted system
- Dedicated host vs. shared host
- Carrier connectivity/risk concentration
- Self-administration capabilities
- Support for multiple forms and channels of communication
- Full audit compliance
- Single system of record
- Support for multiple role definitions
- Support for use case scenarios
- 24/7/365 live operations/network operations centre
- Total cost of ownership (TCO)
- Authentication process

Chart 1. Emergency notification system selection factors as they relate to solution architecture, features/functionality and pricing.

SELECTION FACTOR	ARCHITECTURE	FEATURES/ FUNCTIONALITY	PRICING
Hosted vs. self-hosted system	✓		✓
Dedicated host vs. shared host	✓		✓
Carrier connectivity/risk concentration	✓		
Self-administration capabilities		✓	
Support for multiple forms and channels of communication		✓	
Full audit compliance		✓	
Single system of record		✓	
Support for multiple role definitions		✓	
Support for use case scenarios		✓	
24/7/365 live operations/ network operations centre	✓	✓	
Total cost of ownership (TCO)			✓
Authentication process		✓	

Hosted vs. self-hosted system

Should your organisation host its emergency notification system with a company that specialises in application and managed services hosting? Or should you self-host the solution within your own facilities?

Self-hosted solutions have their place. Advantages include potentially tighter security, more control, and lower costs in terms of capital and resources. For some types of applications, on-site hosting is the sensible choice. If your company already maintains its own disaster recovery facility, hosting your emergency notification system elsewhere would be redundant and unnecessary.

A key point to remember, however: In times of disaster—when crisis communications will be needed—your physical facilities may not be available. Any assumptions about normal operations and capabilities will be suspended. If the on-site system fails, only an off-site facility hosting backed up emergency contact data will enable you to reach employees.

But all hosted solutions are not created equal. Critical considerations include features of the hosting facilities and the viability of the host itself. If you decide to go with a hosted solution, you should evaluate the following:

- **Hardened physical security of the facilities.** How well can the building withstand a hurricane, tornado, earthquake, or other natural or man-made disaster that might afflict the hosting location? A facility located in a flood plain, tornado alley or next to train tracks would be a risky place to store your emergency notification system.
- **Availability of alternate power sources.** In the event of a power outage, does the hosting facility have access to one or more alternate power sources for a significant period of time? The best-laid emergency notification system will be rendered useless if the trusted hosting facility has no power during your time of crisis.
- **Separate access points for communication channels.** It is important to note that connectivity should not be congregated into only one access point. If a concentration of communications equipment and circuits had been destroyed during the 9/11 attack on the Pentagon, all command and control communication with U.S. military forces would have been lost.
- **Carrier connectivity/risk concentration.** Is communication handled by only one vendor or by multiple carriers? If the hosting facility is dependent on one vendor—WorldCom, for example—and something happens to that carrier, it could compromise or even destroy the effectiveness of your emergency notification system in a crisis. You are better off if the host diversifies risk by using multiple carriers—AT&T, Global Crossing and XO in addition to WorldCom, for instance.
- **System platform security.** What are the methodologies used to ensure the integrity of the hosting systems? Does the entire staff at the facility have access to the servers? Or can access be restricted to certain employees or a third-party service? Does it include an intrusion detection system (IDS) and/or a set of firewalls? Your emergency notification system will comprise critical personal and proprietary information that must remain secure.
- **Viability and reputation of the hosting facility.** Does the hosting company you're considering have a reputation as a world-class DR/BC facility—like SunGard Availability Services? Or is it just a little Web co-hosting company that's jumped on the disaster recovery bandwagon by adding emergency notification hosting to its bag of services? More reputable, established hosting companies abide by SAS 70, ISO 9660 and other strict standards that protect your data and provide the highest levels of reliability and availability. While these premium services cost more, they store your data securely and deliver what you need in times of crisis.

Dedicated host vs. shared host

If you choose to go with a hosted emergency notification system, there's another decision to be made. Will you share your notification infrastructure with other clients of the hosting company or will you choose a hosting infrastructure dedicated exclusively to your organisation?

By sharing hardware infrastructure with others, your organisation can save money and have reasonable assurance of coverage during very localised events. However, many disaster recovery centres oversubscribe shared services. In case of a regional or global catastrophe, you might not be able to fully enable your emergency notification system due to constrained hardware resources. As with insurance and banking, if all parties attempt to make claims or withdrawals at the same time, most of them will be left with nothing. Is this a chance you're willing to take?

Under the dedicated hosting model, your organisation has access to the highest level of benefits offered by the disaster recovery centre. The hardware infrastructure and ports are yours alone—no other client organisation can use them. Of course, along with ensured availability come higher costs.

For organisations that can't justify the expense of a dedicated hardware infrastructure, a hybrid solution may provide the most cost-effective choice. In this instance, the host allocates a minimum percentage of hardware to your emergency notification system. Your organisation can then "borrow" additional capacity if needed, mitigating the risk implicit in the pure shared-hosting model.

Carrier connectivity/risk concentration

As noted in the section on hosting and self-hosting, it's best to choose an emergency notification system supported by multiple carriers. If the system is limited to one carrier, and that carrier goes down at the time of your event, your notification system will be rendered null and void. Even in the self-hosting scenario, your organisation would be remiss not to enlist backup to your primary carrier.

A stark example of the importance of multiple carrier support occurred during the 9/11 attacks on the World Trade Centre in New York City. Located in one of the WTC towers, the Verizon point of presence (POP) was lost in the disaster. Unfortunately, that POP acted as a conduit for many of New York's telecommunication providers. Even non-Verizon customers at some distance from Ground Zero lost network connectivity and phone service. Backup carrier support would have diffused those company's risks and allowed them to carry on business as usual.

Self-administration capabilities

Unless you've linked your emergency notification system to day-to-day production, you will only use it episodically, if at all. It's like insurance—something you may need during times of crisis. From a cost standpoint, it makes little sense to commit labour-intensive resources to the administration and management of your notification system. The ideal system, in fact, would not require much in the way of costly oversight.

Unfortunately, traditional emergency notification solutions rely on systems of records separate from corporate records administered by HR and other departments. An administrator must get all information updates from HR and manually enter them into the emergency records database. This creates a great deal of overhead for a system that's only as good as the data in it. What happens if disaster strikes and the administrator hasn't had the opportunity to update last week's data?

An emergency notification system should tie directly into organic corporate systems of records—systems that are continually maintained by design. In particular, the corporate e-mail system marries nicely with emergency notification needs. Employee information is updated on a continual basis in the e-mail system, and e-mail distribution lists can form the baseline of emergency call trees. In fact, individual employees can even take responsibility for updating their own information. Managers can focus on their functional responsibilities rather than administration issues, resting easy with the knowledge that emergency notification has access to the most up-to-date information. By leveraging the e-mail system, this emergency notification solution will lower total cost of software administration.

Since IT won't be constantly monitoring an emergency notification solution tied in with e-mail, you need assurance that the system will be available when needed. An intelligent, self-administering notification solution will include built-in tests that check data synchronisation and system viability on a regular basis.

Support for multiple forms and channels of communication

In times of crisis, it's likely that some of the communication channels used during normal operations will not be up and running. The most effective emergency notification system will take that into account by spanning every conceivable communication channel available.

Many notification systems, particularly low-cost options, rely solely on voice channels—a risky proposition. If something happens to an individual or group of mobile phone towers, for example, mobile phones won't work. That channel of communication is no longer viable. You need a system that inherently spans multiple communication channels—from SMS and mobile phones to text-to-voice, voice-to-voice, wireless devices and SMTP-based e-mail.

Full audit compliance

When it comes to emergency notification, wouldn't you prefer a solution that provides visibility into the performance of the system? With insight into every transaction that transpires, you could fine-tune the system for optimal performance when crisis strikes. If your organisation is subject to regulatory compliance, audit capabilities are a must. Unfortunately though, most traditional backup systems don't include full audit compliance features.

An optimised, top-of-the-line emergency notification solution will include an audit module that shows every transaction and monitors the performance of the system. With full audit compliance, management gets a running log of what's going on in the notification system—a way to measure how the system works and calibrate baseline performance. It helps management keep tabs on how employees use the system, reducing opportunities for abuse. In terms of regulatory compliance, full audit features preserve the forensic chain of evidence and prove the repeatability of processes.

Audit compliance capabilities allow you to test the most efficient ways to reach users—the best way to reach people in China at 3:00 A.M. on a Saturday, for instance. Is it by mobile phone? Does a certain carrier perform the job better at that time than another? You can also use audit compliance to set up specific use case scenarios for your emergency notification system. For example, you can document how quickly the system gets a message to users in Singapore.

Most importantly, The audit module of the emergency notification solution must provide real-time visibility, not merely a historical perspective to the system. If there's a fire in the building, a live roll call will help determine who has been reached and the methods taken thus far to notify them. You can then confidently take other measures to reach the non-respondents, avoiding unnecessary backtracking and duplication of efforts.

Single system of record

The last thing most organisations need is another enterprise database to maintain—especially a database for an emergency notification system that offers no direct return on investment. Most organisations simply don't have resources to pour into emergency notification. As noted in the section on self-administration, however, traditional emergency notification solutions require their own separately maintained record systems. No wonder these can be such a hard sell to upper management!

Instead of relying on an unsynchronised data repository, your organisation's emergency notification system should leverage systems that are already funded and kept up to date—namely, the corporate e-mail system. Only one data repository will require administering, and the e-mail system of records is already networked and supported in the enterprise. You get the benefits of a well-integrated notification system at minimal cost.

Support for multiple role definitions

In the working world, individual employees don't fit neatly into single categories. An employee who works in the greater marketing department may also belong to the subset of marketing communications, for example. That same individual may also be a member of the company volleyball team—a group that includes engineers, accountants and others outside of marketing. Since a crisis may occur when an employee is taking on any number of roles, an emergency notification solution should support multiple role definitions. This level of sophistication doesn't exist in all notification systems.

In addition to allowing authorized administrators to create and manage user groups, the optimal emergency notification system should have the flexibility to support multiple role definitions. Since individual users can belong to multiple groups, their emergency contact information should be available to all group managers. However, an individual's expected response in times of crisis can differ from group to group. In one group, they may have to take critical, job-related action in a certain type of crisis; in another, they may only need to be advised of the event. Permissions and restrictions can be set up such that the manager of one group can't affect the composition or performance of another group.

Support for use-case scenarios

As part of the risk assessment process, your organisation should model its most likely emergency scenarios. For example, if one of your company sites is located in a flood zone, your plan might articulate how the organisation will respond to a flood warning. While most serious emergency notification solutions can pre-build responses to likely scenarios, decision makers often gravitate towards low-cost systems that don't include pre-modelling features. After it's too late, they realise that their system can't make good on its reason for existence. If it takes three hours to send a notification message, the tornado has come and gone—and so has your building. A notification solution should allow you to actually pre-build multiple emergency scenarios and corresponding responses into the system. With notification trees modelled and ready for action at the click of a mouse, you won't have to start from scratch during times of crisis. Your emergency notification will deliver on its *raison d'être*, providing you with true disaster-recovery insurance.

24/7/365 live operations/network operations centre

If you've chosen a hosted emergency notification solution or wish to manage your system on a hosted basis, you need to ensure ongoing, secure operations. What happens if there's a power outage and you can't get to the Web to activate the notification system? Is there a plan in place that authorizes representatives in disparate geographies to activate the system on your behalf? If the only way to start a notification process is blocked, you can't set your emergency response plan into motion. One tragic example: New York City's emergency management system—located in one of the World Trade Centre towers—was destroyed during the 9/11 attack.

The most effective emergency notification systems include geographically disparate, 24/7/365 operations support complete with authentication features. If the power goes out and phone service is still available, the administrator can call a geographically immune authorized party. That link in the notification chain can then initiate the emergency response system and take any necessary escalation measures. A trusted, documented support plan backed up by security will ensure the efficacy of your emergency notification system no matter the circumstances.

Total cost of ownership (TCO)

When selecting an emergency notification system, you must factor in the ongoing, “hidden” costs of actually running it—particularly if you’ve chosen a hosted solution. Otherwise, your disaster recovery budget may get hit with some unpleasant surprises.

- **Notification minute/attempt overage charges.** Hosted disaster recovery solutions typically allocate a discrete number of minutes/attempts for notifications per emergency. For example, your solution may include 10,000 voice minutes and 2,000 e-mail attempts. Find out about overage charges—here, what it costs for every minute and attempt over the 10,000 voice and 2,000 e-mail allotments—before locking yourself into a solution.
- **Pricing of notification services.** Every notification service covered in the hosting agreement should be transparently priced. Long-distance voice and voice-over-XML are available at identifiable market prices. SMTP-based e-mail, on the other hand, is virtually free. Your vendor should charge no more than the market price for long distance and other similarly priced types of notifications. E-mail notifications should have very little or no cost associated with them.
- **Barriers to regular testing.** To ensure the most effective emergency notification system, you must subject it to regularly scheduled testing. However, some hosting vendors put up obstacles to system testing. Does the vendor you’re considering allow testing? How often? Do you have to schedule test events at the vendor’s site? Are there charges associated with testing? Any system that charges a testing fee or creates cost/administrative barriers to testing is suboptimal, as you are less likely to use it. You need a system that keeps barriers to a minimum, allowing you to test anywhere, anytime, at any volume and for very little cost.
- **License renewal charges.** Before signing on with an emergency notification system hosting vendor, carefully examine fee escalation charges at time of license renewal. Is the renewal fee capped by a percentage with which you’re comfortable? Some vendors will entice you with an inexpensive one-year license. Once you’re invested in their system, however, they may raise the fee astronomically in subsequent years. An 8% annual escalation fee, for example, will turn that bargain system into a costly venture over the course of a few years. In such a case, negotiate with the vendor. Tie the fee to the cost of living index, for example, or cap fee escalation at 2% or another low rate.
- **Conference call bridging charges.** Many emergency notification systems include a conference call bridging feature. Popular with executive management, these bridges call several people at once and conference them together so that they can discuss an issue. Ideally, your notification system provider should let you use your own bridge. While hosting vendors will offer full-featured proprietary conference call bridging, you may not really need all the bells and whistles—and the higher level of functionality that comes at a higher cost.

Authentication process

For maximum effectiveness, your emergency notification system must include a PIN-based authentication process that can prove that users actually receive messages. If a message is sent to a mobile phone, for instance, the system should be able to distinguish whether or not the designated user has picked it up. There should also be a mechanism that allows the user to acknowledge receipt of the message. Then the system knows that the user is aware of the message, it’s not languishing in the voice mail box of a mobile phone with a dead battery.

Section IV

Deploying, optimizing & managing your emergency notification system

Using the guidelines in Section III, you've selected an emergency notification system that matches your organisation's needs and resources. However, a great notification system is of little use if it can't be successfully deployed and managed.

All too often, the best-laid emergency notification plans die on the deployment and management vines. The landscape is littered with enterprises that bought best-of-breed solutions only to get bogged down in discouraging, drawn-out deployment processes. Even if the initial deployment is successful, lack of attention to management issues will cause a good system to atrophy, diminishing its effectiveness in times of crisis.

To ensure optimal availability of your emergency notification system when you need it, your organisation should adhere to the following deployment and management considerations:

- Getting help with deployment
- Leveraging and configuring data sources
- Determining the most efficacious communication channels
- Identifying and overcoming common activation and programming issues
- Penetrating caller ID, TeleZapper and other call-screening systems
- Supporting peak concurrency
- Optimising through day-to-day use
- Scheduling regular testing
- Managing to the lowest TCO
- Documenting system use and efficacy
- Promoting visibility of the system

Getting help with deployment

The first rule of thumb in deploying an emergency notification system: Get help. Within your enterprise, leverage the support of departments that can generate value from the system. For example, your HR department will save on data-entry labour costs if its employee database ties in with the new self-administering notification solution. In this case, it's to HR's advantage to use its pull with IT to get the system deployed. You may also persuade IT on its own terms by demonstrating how the emergency system can be used for routine technical support notifications, such as server outages.

In addition to tapping internal support, you should also consider reaching out to experts for help with deploying the emergency notification solution. Business-continuity/disaster-recovery vendors and consultants can help you at any stage of deployment—from answering simple configuration questions to designing and installing the complete solution. Also, many representatives from organisations that have successfully implemented these systems are happy to share their experiences.

Leveraging and configuring data sources

Deployment starts with tying the necessary organisational data to the emergency-notification system. Good primary data sources include corporate e-mail systems, comprehensive HR systems from companies such as PeopleSoft and SAP, and proprietary databases. Key data from these sources must be imported and synchronised to the disaster recovery software—data such as usernames, e-mail addresses, mobile phone numbers, home phone numbers, pager numbers and other contact information. As noted in Section III, a good emergency notification system will automatically leverage the information in existing databases.

Group structure information—departments, predefined response teams, and other ways of organising people—should also be synchronised with or added to the emergency notification system. From there, you need to add escalation orders among communication devices and channels. Which devices to try first, how much time to wait before contacting the next device, and which devices to contact during different times of the day or week must all be programmed into the system for maximum effectiveness. Finally, you should input any predefined disaster scenario information that could help expedite response in times of crisis. Once mapped, emergency notification data is ready to be pulled and acted upon when necessary.

Determining the most efficacious communication channels

The selection discussion (Section III) advised choosing an emergency notification system that supports multiple forms and channels of communication. All communication channels won't survive a crisis, so you need to make as many available as possible. From a deployment standpoint, you must also design an emergency escalation sequence that will best cover your organisation's needs.

- **E-mail as star.** During two recent disasters in New York City—the 9/11 terrorist attacks and the August 2003 power outage—e-mail took its place as the most reliable communication channel. In the immediate aftermath of 9/11, the demise of Verizon's POP took out the use of landline phones; people could only communicate via mobile phones and wireless e-mail. The opposite happened during the Northeastern U.S. power outage, with the lack of electricity downing both mobile and cordless phones but leaving traditional landline phones operational.

The inherently distributed nature of the Internet gives e-mail advantages over both mobile and landline phones. A phone connects to a carrier on a particular network and either does or doesn't work. E-mail, on the other hand, can be checked wherever there's an Internet connection—from a private residence, the library, an airport kiosk or an Internet cafe. If you can't access the Internet from one location, there's a high probability you can do so from somewhere else. Communication may not be immediate, but it has a higher likelihood of getting through.

- **Nature of the audience.** How you sequence the escalation of communication channels also depends on your audience. Executives, for instance, may prefer using a conference-call bridge to discuss an issue. Someone in IT would likely rather be notified via two-way pager, especially for a relatively minor problem such as a server going down.
- **Contingency planning.** Another consideration in regard to preferred communication channels: What types of contingencies do you need to plan for? Some channels are more conducive to delivery of certain pieces of information. For a virtual roll call to a rendezvous point, phone notification may be the most expedient way to reach people and ask for acknowledgement. In a medical emergency requiring high levels of interactivity, asynchronous communication that offers visual clarity and allows written response—such as e-mail—will be far more effective than a nine-layer-deep phone tree. Think about the types of scenarios you need to plan for, the most appropriate channels for the delivery of that information, and the necessary level of interactivity.

Identifying and overcoming common activation and programming issues

When it comes to selecting an emergency notification system, 24/7/365 live operation is vital. Once the system is in place, you must configure activation paths that build in redundancies and distribute risk. If a power outage or other circumstance occurs and the principal operator can't activate the system, there should be other mechanisms in place to carry through with the activation. Designate people in geographically disparate locations with the proper levels of authorization to take over. Also, ensure that the system can be activated via more than one channel. Even if the usual interface is a Web-based console, for example, the system could fall back on phone access in case of Internet failure.

In terms of programming, take care that notification scripting isn't too complicated or ambitious. People will be shocked and scared during a crisis event. A complex script may fluster them and defeat its purpose of ameliorating chaos. Keep it simple.

Penetrating caller ID, TeleZapper and other call-screening systems

An effective emergency notification system must get through to the people who need the information. In this time of ever-intrusive communication, however, many would-be recipients may screen out unidentifiable phone calls using caller ID, TeleZapper and other systems. To ensure that an emergency notification call is answered, your disaster recovery team should configure the system with an outbound caller ID to which users will respond. Use the organisation's main telephone number and the company name, for example, to ensure that your employees will pick up the phone and get emergency messages sooner rather than later.

Supporting peak concurrency

When you embarked on selecting an emergency notification system, you chose a solution based on your peak concurrency model for projected usage requirements. If you decided on a hosted solution, the vendor will provide the capacity needed by your organisation. An in-house deployment, however, will require the provisioning of additional T1 lines and other telecommunication support to meet concurrency needs.

In either case, physical deployment of the system will reveal how close the model is to real-world use. You should change the model and your notification infrastructure as appropriate and keep both up-to-date as testing and notions of risk and capacity morph over time. After all, the last thing you need at the time of a disaster is to find out that your emergency system is port-constrained and can't get out notifications.

Optimising through day-to-day use

The best way to optimise your emergency notification system is to use it in day-to-day business applications. Use in routine operations will ensure the system's availability as well as data viability. Also, leveraging the system in this way will distribute associated costs over other applications.

Real-world examples of how organisations can tie the emergency notification system to day-to-day operations include:

- Law firms putting together deal teams
- IT departments responding to intrusion detection viruses
- Technical support staff transmitting event tickets
- Salespeople entering orders and sending them from the field
- Trucking companies dispatching information to drivers
- National retailers testing individual store responsiveness to phone calls

Scheduling regular testing

At a time of crisis, you don't want the stress of wondering whether or not your carefully deployed emergency notification system will actually work. Regular system testing guarantees its efficacy and ensures the viability of contact information. This testing may occur through scheduled "fire drills" that familiarise users with the system or through daily system use in other business applications.

- **Efficacy of the system.** To ensure that emergency notification will reach users at the time of crisis, you must test the system. If employees are familiar with how they will be notified and understand how to acknowledge messages, you can more comfortably count on them receiving and responding to notifications during a real emergency. You can focus rescue or other appropriate actions on those who don't respond, knowing that they truly need help.
- **Validation of data quality.** Every time you run a test of the emergency notification system, you get empirical feedback on the quality of the data. If regular tests yield an 85% response rate, that's the expected "normal" response rate at least until you get to the bottom of why 15% aren't responding. Corrective actions can be taken to get you closer to a 100% response rate—from updating mobile phone numbers to changing users' escalation sequences to simply reminding some users to turn on their pagers.

As a best practice, weekly or monthly test messages should be sent using the emergency notification system. This doesn't mean annoying staff with notifications at 2:00 A.M. every Saturday morning. Tests can be run during normal working hours. You may even want to make the test notifications fun or interesting so that employees look forward to receiving them. If they miss the next segment of an evolving saga, ongoing joke or contest, for instance, they'll know something is wrong and will have the motivation to correct it—before disaster strikes.

You should test the efficacy of each communication device to determine the best and fastest ways to reach people as well as which channels to support. Is it easier to reach employees over mobile phones, regular e-mail or wireless e-mail devices? Will contacting people through wireless devices increase the response rate?

If your organisation leverages the emergency notification system for use in day-to-day business processes, "testing" of response times and devices will occur during the course of normal operations. A system used and tested in this manner is much more likely to contain up-to-date information when needed in an emergency.

Managing to the lowest TCO

You've selected an emergency notification system that lowers total cost of ownership while providing the functionality that your organisation needs. Now you can pragmatically manage these known costs for maximum system utilisation.

- **Sequence of notification escalation.** How your emergency notification escalation is sequenced can make a big difference in cost savings. While people may be contacted more quickly via voice communication, the virtually free nature of e-mail makes it the most cost-effective first line of defence. For example, reaching 1,000 people via voice call may cost 8 pence per call—while sending e-mail notifications will cost almost nothing. The system will only default to the notification method that involves cost if the recipient doesn't respond to the e-mail notification.

Thoughtful escalation sequencing can help keep down the cost of notification overages, assuming a high number of e-mail allotments. Limiting voice notifications can also lower voice port contention, reducing the need for dedicated hosted space or providing dramatic efficiencies in the self-provisioning of T1 and/or T3 lines.

- **Distributed data administration.** If you've wisely chosen a self-administering emergency notification system, there should be little or no hands-on management involved in updating and changing employee information. Simply train employees to update their own information—from their mobile phone number to the escalation order of communication channels. When a manager needs a new group on the system, they or someone on their staff can create the group. By putting updates in the hands of employees, you won't incur the expense of dedicating staff to routine administration.
- **Conference call bridging.** While your organisation can save money by using its own conference-call bridge, that isn't always feasible. Smaller organisations, for example, may not want to invest in a bridge that they will only use infrequently. In such a case, you can minimise costs by invoking the use of the provider's bridging feature only when absolutely necessary.

Documenting system use and efficacy

As noted in the selection section of this document, full audit compliance is an essential feature of an emergency notification system. Very detailed, real-time tracking of all notification results will help you evaluate and improve on the quality of the data in the system. To ensure the availability of the audit report, it's a good management practice to store it in a non-mutable format on a secure server.

Promoting visibility of the system

Ongoing management of your emergency notification system also involves providing visibility of the solution's success within your enterprise. You must continually stoke awareness of the notification system—from setting organisational expectations to reporting deployment, management, testing and usage milestones.

By promoting the emergency notification system, you will keep it top of mind and help ensure optimal usage at a time of crisis. Follow the time worn adage: Tell users and management what you're going to do, tell them why you're doing it, tell them what you did, and tell them why it was successful. The resulting preservation of lives, property and capital will be worth it.

The time for emergency notification has come

Natural and man-made disasters, regulatory compliance and the increasingly complex nature of distributed organisations all point to the need for comprehensive, effective emergency notification systems. Technology can now deliver on that need, and a variety of notification solutions are on the market today. However, all of these solutions are not created equal. After winning executive-level support for emergency notification, you must select the appropriate system for your organisation and then deploy and manage it for maximum effectiveness.

Conclusion

Selecting the right system: SunGard's AlertFind emergency notification & escalation system

As identified in this report, important features to look for in an emergency notification system include: carrier connectivity/risk concentration, self-administration capabilities, support of multiple forms and channels of communication, full audit compliance, a single system of record, support for multiple role definitions, support for use case scenarios, 24/7/365 live operations support and an authentication process. Hidden costs that will impact total cost of ownership also must be considered – including notification minute/attempt overage charges, pricing of services, potential barriers to testing, license renewal charges and conference-call bridging charges.

Based on this assessment, SunGard's AlertFind is one of the most powerful, affordable enterprise communication tools in the market today. During a crisis or disaster, normal lines of communication will likely fail when you need them most. AlertFind provides executives and crisis managers with a direct communication channel to large numbers of employees, customers, partners and other constituents. AlertFind provides the most effective method to quickly, securely, and reliably distribute and collect information in real-time using all available modes of communication.

AlertFind feature & benefit summary

AlertFind Feature	Details	Benefit
Data synchronisation & management	<ul style="list-style-type: none"> ■ Automated synchronisation of users & groups from enterprise e-mail systems. ■ Automated data synchronisation capabilities with other enterprise data systems. ■ Automated import of excel spreadsheets or CSV files. ■ Web-based administration and web or phone activation. 	Emergency notification systems are only effective if the contact information they contain is accurate and up-to-date. AlertFind automatically synchronises with e-mail systems, directory services, HR systems, and DR planning systems to ensure accurate and complete lists of users, contacts, and groups.
Multi-device notification (outbound)	<ul style="list-style-type: none"> ■ Voice alerts to landlines, home phones, and mobile phones using text-to-speech engine. ■ SMTP-based alerts to e-mail, pagers, PDAs, and other devices. ■ User-specific escalation orders across an unlimited number of devices. ■ Customised escalation rules based on time of day or day of week. 	Reach any user, anywhere and at anytime via text-enabled devices or voice enabled devices. Give your employees maximum flexibility by allowing them to be contacted at over a dozen different devices ranging from home phones, mobile phones, pagers, wireless devices, SMS, personal e-mail accounts, and more. Easily specify device-to-device escalation rules as well as user-to-user escalations.
Multi-device acknowledgement (inbound)	<ul style="list-style-type: none"> ■ Multi-mode acknowledgement over telephone, 2-way pager, email, or web-browser. ■ Escalation within group to locate "First Responder". ■ Real-time message acknowledgement and status reporting. ■ Support for secure message acknowledgement using PINs. ■ Automatic conference call bridging of recipients. ■ Automated polling of contacts to collect real-time data. 	AlertFind provides true two-way emergency communication to help you reach your audience – no matter where they are or time of day.
Real-time status reporting	<ul style="list-style-type: none"> ■ Self-serve, web-based interface allows administrators to view detailed reporting status 24/7. ■ Granular status reporting showing progress, devices attempted, delivery status, times, etc. ■ Downloadable reports that can be incorporated into the results of any DR test. 	AlertFind offers you detailed reporting on pending as well as sent notifications. These reports offer simple summaries as well as extremely detailed descriptions of the notification progress on a device by device basis.

Enterprise-wide Information Availability

Since 1978, SunGard Availability Services has pioneered Information Availability and business continuity. We understand the enormous impact technology change has upon business and that any organisation's vital ingredients are its people and information.

That is why we developed a continuum of **proactive, reactive** and **interactive Information Availability** solutions comprising **business continuity, disaster recovery** and **high availability/managed services**. For a complete, robust, future-proof solution that will keep your business critical processes running, talk to us – whatever your business sector or size, IT, time or budget requirements.

10,000 customers worldwide trust us to keep them in business by keeping their people and information connected. Regardless of whether you measure your tolerance to disaster in seconds, minutes, hours or days; trust us to do the same for you.

Local presence, global strength

- > 20,000 end-user positions
- > 60 locations
- > 3 million sq ft of secure dedicated operations space
- > 25,000 miles of dedicated network backbone
- > 50 mobile recovery units
- > 100,000 recovery tests undertaken
- > 10,000 business continuity projects undertaken
- > 10,000 clients worldwide
- > 2,500 Information Availability professionals at hand
- > 1,500 invocations supported with 100% success!

SunGard Availability Services

12-13 Bracknell Beechess, Old Bracknell Lane West, Bracknell, Berkshire RG12 7BW
Tel: 0800 143 413 infoavail@sungard.com www.availability.sungard.com/uk.

SUNGARD® | Keeping People
Availability Services | and Information
Connected.™