Communication Strategies for Incident Response

Mass Notification and Beyond

Becky Maycock
Impact Technologies

Contents

Introduction **3**

Prepare for the Inevitable **4**

Evolution of Notification Solutions **5**

Unified Mass Notification **6**

Notification Tools and Techniques 6

At the Desktop 6

On the Go 7

In Public Areas 7

In the Enterprise and Beyond 8

Subscriber Management 8

Initiation 9

Reporting and Accountability 10

Beyond Mass Notification **11**

Personal Safety and Security 11

Silent Alarm 11

Panic Button 12

Personnel Monitoring 12

Emergency Call Handling 13

Crisis Team Collaboration 13

Personal Calling Services 14

Coordinated Incident Response 14

Fitting the Pieces Together **15**

Conclusion **17**

About the Author **17**

About Impact Technologies **17**

Introduction

Crisis is inevitable, and sooner or later all organizations will be struck by one. Although some crises do provide warning signs, most often they are unpredictable. Yet despite their unpredictability, crises should not be unexpected or unanticipated. An organization's planning and preparedness determines its ability to respond, directly affecting the impact a crisis will have. The efficacy of response determines the cost of a crisis both in financial and human terms.

Crisis situations allow a limited time period in which to respond. In the midst of a crisis, organizational leaders must formulate a response, make decisions, and take action quickly to avert or at least contain it. These actions can have a far-reaching effect on the institution, its people, its resources, and even its existence. Once a crisis has struck, there is little time to carefully weigh each decision and consider the long-term impact of a selected action. The quality of the decisions made under great time pressure is the single greatest determinant of the ultimate cost of a crisis.

The unique aspects of each crisis require a unique response. The severity, location, magnitude, and visibility of an event must be addressed in the context of the institution's ability to respond. The sudden or overpowering and initially uncontrollable event is rarely resolved by a single action. To contain the incident and ultimately return the organization to normal operating state requires crisis management be adaptable and ready to work in an ad hoc fashion.

Communications is the single most important component of how an organization responds to a crisis. This document delves into communications strategies that organizations can leverage to contain incidents and speed return to normal operating state.

Prepare for the Inevitable

Many organizations are so focused on incident response that they forget the first step – detection and reporting of critical incidents. You can't respond to something that you are not aware of! Don't overlook leveraging your communications network as a portal for reporting events. Your employees, students, staff and/or visitors should never be more than a button push away from being able to report a problem.

Another mistake many organizations make is the concentrated focus on notifications – many times in the form of text messages or e-mails. Notifications are important, but they are not the sole solution. And, how do you determine what message the alert is going to communicate? Do you tell students to "lock down" in their classrooms? Do you tell employees to evacuate? Who makes those decisions? And, how?

Effective incident response requires more than notification technologies. Real-time collaboration among incident response personnel is a critical first step to an intelligent and swift response. Instantly connecting first responders, decision makers and response coordinators to discuss the facts of the situation and strategize on the response is the crucial step to assure the next steps are the right steps to contain the crisis and control panic.

Be prepared. Assume a readiness posture. Be proactive and have technologies and procedures in place for events you expect could occur – such as fires or inclement weather. But, understand that a crisis event may arise that forces the organization to be reactive. You need a communications foundation and strategies that are adaptable to ad hoc demands.

Evolution of Notification Solutions

Notification is not new. But, the solutions have evolved over time. First generation solutions provided location-specific alerts with generalized messaging. Your first encounter with these physical alarms was probably grade school fire alarms or outside speakers at a pool or recreational area. The message provided very simple instructions or basic information.

Telephony was leveraged for the second generation of notification solutions. The message could then be more specific or personalized for the target audience. Telephony expanded the reach of the message. The recipient could be at work, at home or on the go with a mobile device such as a cell phone or pager. Another key enhancement telephony offered was bi-directional communication. The alert recipient could confirm the message or provide more detailed feedback by responding to prompts by pressing a designated key. Finally, remote initiation of notifications was introduced. A person could use a telephone to launch an alert without being tethered to a specific location.

To complement the earlier generations, net-centric notification adds expansive IP device reach. Today's employee or student is never more than inches from their laptop, smartphone or e-mail. And, by leveraging the IP network, the alerts can contain rich content – such as pictures, maps or even video clips. Finally, social media is the latest addition as organizations leverage Twitter or Facebook.

Technologies from each generation offer valuable and effective alerting mechanisms. And, in most cases, a combination of technologies is optimal.

Unified Mass Notification

Workforces have never been more mobile and dispersed, and it's an increasing challenge to quickly and reliably communicate with them. Whether it's something as routine as providing notifications of school closures or alerting staff of a computer virus, or something as dramatic as locking down a campus due to a mass casualty event, rapid dissemination of information is critical.

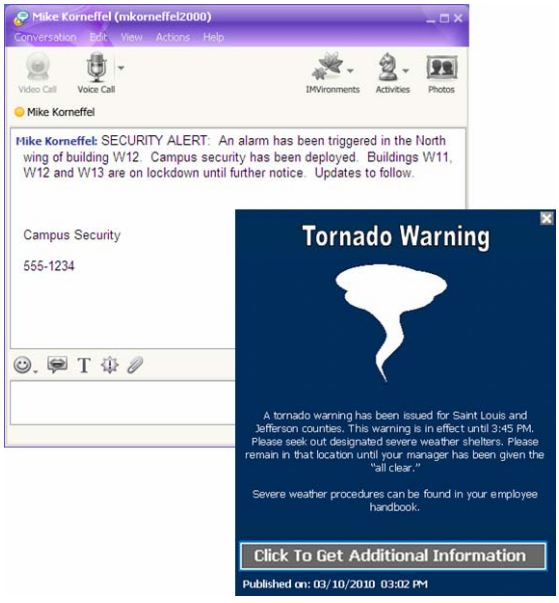
Notification Tools and Techniques

When someone says "mass notification" many people translate that to Short Messaging Service (SMS). But, SMS is only one piece of what can be a complete unified mass notification solution. Let's review many options that are available to your organization. Your optimal notification methods and technologies will be based on your environment and mobility of your recipients (staff, students, employees, visitors, etc). And, as you read on, you may quickly discover that a combination of mechanisms is needed.

At the Desktop

Many people spend a large portion of their day in front of a computer screen, so computer desktop alerts – such as screen pops, instant messaging (IM) and e-mails – are great options.

Screen pop alerts are 'disruptive.' The user may be working on a report or e-mail message and suddenly a window appears that describes the potential threat and may include instructions for action or request for confirmation or feedback. An optional audio alert may also automatically sound over the computer's speakers. The user must react to the screen pop before proceeding.



Many companies allow IM technologies. Don't overlook this technology as a means to disseminate real-time critical information.

Finally, e-mail is available at the desktop. The good news about e-mail is that it is ubiquitous. The bad news is that e-mail is easy to ignore and may not meet timing objectives.

Unified Mass Notification

Most employees in corporate America still have a telephone device on their desks. Leverage your existing telephony network and use phone calls to alert your staff. The call may include a pre-recorded message or it may be an announcement that was just recorded ad hoc with timely information and instructions. Telephony broadcast solutions today support voice prompts for confirmation or feedback. For example, the recipient may hear something like: "There has been a hazardous material spill in the lab. Are you able to respond? Press 1 for a positive response. Press 0 for a negative response."

On the Go

Just because someone is not at their desk does not mean they are out of reach. Cell phones, smartphones and pagers provide links to people on the go.

Similar to calling employees on their PBX extension, you may reach them on their mobile phones. The call may or may not include confirmation options. Or, send an SMS message to the device. Keep in mind, however, that text messages are delivered on a best efforts basis, often arriving late and, if issued in sequence, may arrive out of sequence.

For your team members that carry smartphones, you can go beyond phone calls, e-mails and SMS messages and deliver interactive text alerts. By leveraging the corporate wi-fi network if the user is on site or the GSM network if off site, you may swiftly dispatch text alerts with immediate acknowledgement or rejection. This will allow online text dialogs while the user is on another call. History of all calls and responses is also available.

To many, pagers have been relegated to storage with cassette tapes and VCRs. But, just like there are folks still watching "Star Wars" on VHS tapes, there are institutions that leverage pagers every day – particularly in the healthcare environment. If pagers still have applicability in your world, don't forget them when you are developing your notification strategies. Pagers may be the best means to access your staff members in the field.

In Public Areas

You may not have a direct link to every individual on your campus or within your office space. You most likely don't have contact information for all visitors, partners, vendors or other guests. But, their safety and security is still key when they are on your property. So, how

Unified Mass Notification

do you get information to them? Sometimes the older technologies are still the best technologies.

For public areas, such as lobbies, cafeterias or parking lots, message boards, sirens or loudspeakers provide universal coverage to broadcast your message. You will not have access to recipient confirmation or audit tracking, but the important task of delivering information is accomplished.

In the Enterprise and Beyond

The enterprise is often the spotlighted arena when building a notification plan. But, your plan may need to account for individuals that may not be "inside your four walls" when you need them. Clearly, technologies like cell phones, smartphones and pagers extend beyond the enterprise. Twitter and Facebook are also options, particularly if your target group is the younger generation. However, there are technical considerations that come into play as your constituency reaches outside your enterprise. We will discuss this point later.

Hopefully you now have a grasp on what notification tools and techniques will fit best in your environment. Let's move on to other practical aspects of mass notification.

SUBSCRIBER MANAGEMENT

If you only need to alert a few dozen people, subscriber management is not a high priority issue for you. But, if you have hundreds or thousands of individuals to alert, where do you start? The first question that must be answered is "where do I have the contact information for my subscribers?" Do you have a database or spreadsheet that contains the contact information you need to leverage? Information could include: PBX extension, cell phone number, e-mail address, pager number, location and more. Whether you have the data repositories or you must create them, the next step is integrating the information with your notification solution. Consider integration options such as Active Directory, common database or scheduled imports.

Unified Mass Notification

In a dynamic environment—particularly in the education market—a self service option is a popular subscriber management tool. Users can update their profile and/or opt in or opt out based on rules you define.

A final piece of subscriber management is group definition. Based on the type or location of the crisis event, you may only want to notify a select subset of users. So, you need quick access to a logical subdivision of your subscribers based on a particular characteristic, such as location or job responsibility.

INITIATION

By this point, mass notification may be starting to sound complicated and overly intricate. It doesn't have to be! Don't fall into the trap of trying to glue together a bunch of siloed solutions. You can unify discrete notification channels and disparate sensors for simplified alert activation and redundant reach. Given you don't know when or where the next event is going to occur, you need flexibility in initiating the notification alerts. And, ideally, you need a combination of manual and automated initiations.

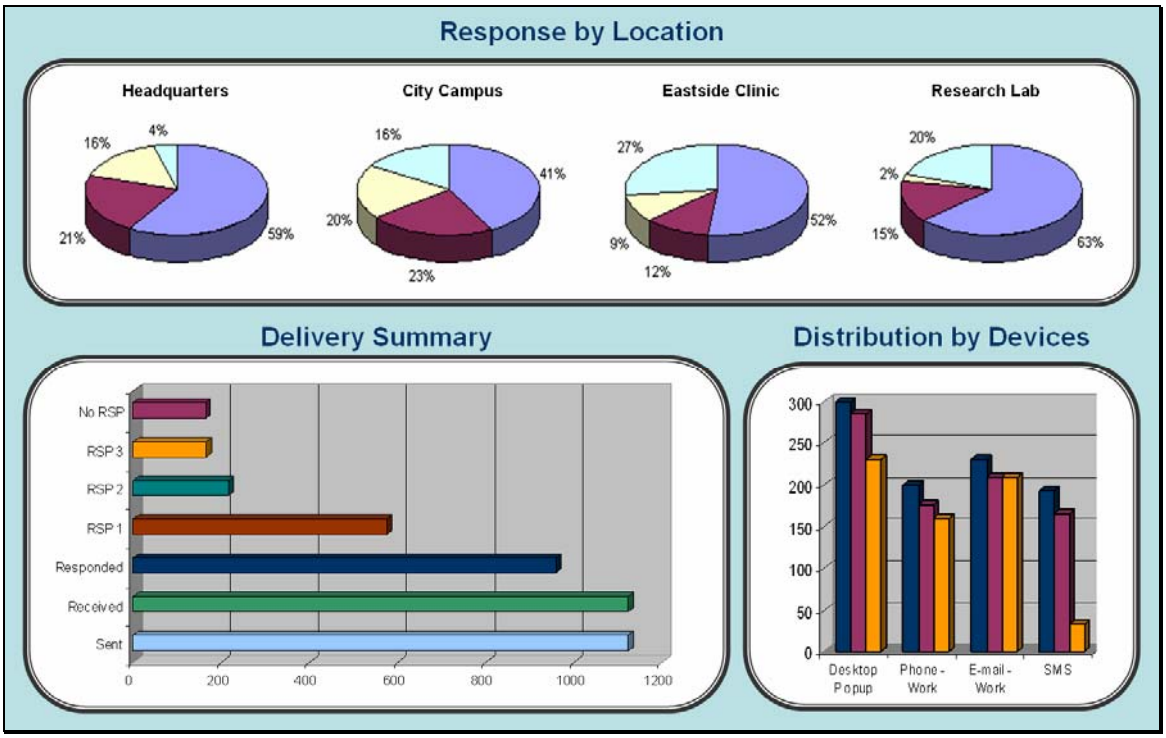
You want to be able to manually initiate an alert from home, on the road or at the office. And, depending on the type of content you want to include, you need options. For instance, maybe you need to transmit an ad hoc message, so you want to be able to record a voice announcement via any telephone (PBX extension or external device) and push a button to start the outbound calls. Or, maybe you want to type a message and send a combination of text messages while also leveraging text-to-speech for audio alerts. Or, access a list of predefined alerts on your smartphone and launch immediately.

In other situations, you may choose to automate the alert initiation. If human intervention is not required, why wait? Integrate third party systems or devices, and based on a threshold or specific event, launch a predefined alert. For instance, if a refrigerator storing vaccinations or medications fails, automatically dispatch maintenance. Or, if a data center triggers a temperature alarm or a door is ajar, automatically alert the appropriate resource(s). Finally, if a fire alarm goes off, automatically send screen pops to all students in a classroom or dormitory. Standard interfaces and protocols might include: RS 232, ESPA-X and XML.

Unified Mass Notification

Reporting and Accountability

Real-time visibility into the status of the mass notification along with summary and detailed reporting afterwards is key for accountability and audit purposes. As you evaluate solutions, don't forget to ask about reporting. You may want to follow the progress of the alert in real time to see the breakout of the responses – reached, not reached and selected response options, if applicable. You may also want to dig into the notifications by device type. Maybe you are very successful reaching your audience with desktop popups and internal phone calls but have poor success rates with SMS.



Beyond Mass Notification

If a safety or security incident occurred within your enterprise, is your communications infrastructure ready? Will it:

- Provide easy, ready means for a person to communicate a threat?
- Be fully leveraged to protect the safety and security of your staff and visitors?
- Use latest communication technology to contain the incident and return the organization to the normal operating state in a timely manner?

In other words, have you gone beyond mass notification and leveraged technologies and practices to assure that you are prepared to respond to safety and security threats? Have you fully leveraged your existing IP and telephony networks to protect your people and assets? This section will highlight safety and security scenarios to help you lay a communications foundation and strategy that will contain incidents and speed return to normal operating state.

Personal Safety and Security

The greatest asset of any organization is its employees. So, let's start with options to provide your employees and staff with mechanisms to effectively report problems.

Silent Alarm

In the event someone makes a verbal or physical threat to one of your employees, a silent alarm provides a mechanism to alert security of a potential problem without bells and alarms sounding to make a situation more dangerous. This is an ideal solution for receptionists, emergency rooms, pharmacies and other locations where employees interact with the public. It is also perfect for scenarios involving counselors, doctors and staff that meet in private with employees, students or visitors who might become threatening.

The silent alarm can be implemented with a physical alarm button, programmed telephone key or smart badge. By leveraging the existing phone network, the silent alarm can be deployed enterprise-wide so every phone becomes an emergency reporting portal. When the preconfigured key is pushed, an alert (phone call or screen pop, for instance) is sent to the security office, and the source (location/ID) of the distress call is shown on their system telephone displays or computer screen. Note that the caller's line may be dropped immediately so there is no persistent visible (no lamps are lit) or audible (no dial tone is heard) indication on the phone.

Beyond Mass Notification

Panic Button

A panic button provides a mechanism to alert security of a potential problem and also allows them to hear what is happening at the location. This scenario goes beyond the silent alarm discussed above by establishing a conference call with the security officer. Based on the sounds from the site, the security personnel will be able to glean additional insight into the situation and dispatch appropriate resources to the location.

Pressing a panic button (realized by speed dial key on a phone) triggers a conference call that starts with the source (location/ID) of the distress call shown on the system telephone displays and the security office personnel phone muted. In many cases, the dial tone and ringing are not audible when the call is placed so there is no audible indication that the room is being monitored. The notification can also be directed to patrol officers carrying mobile phones, administrators who need to be made aware of panic button events, and/or management and support staff who may be in the vicinity of the threat. Panic buttons are ideal for classrooms and staff that must meet behind closed doors with others.

Personnel Monitoring

In some cases, you may have employees that have potentially hazardous work assignments (e.g. security patrol, rescue team member, psychiatric ward attendant, etc.) and need a mechanism to periodically contact those staff members to assure their safety. For example, a security guard that patrols the campus may follow this process:

- Log in with a mobile phone device to activate surveillance at the beginning of shift
- At a regular, specified interval (e.g. every hour), he may be asked to:
  - answer a call and disconnect after listening to a short announcement
  - answer a call and acknowledge by pressing a key
  - answer a call and provide a current status/location update when prompted

If the guard fails to answer a call, an automated alert is sent to designated contact(s) reporting that the surveillance call was not answered and including, when available, the last status/location update provided by the monitored worker or noted by a positioning server if deployed with location services (RFID). Maybe the guard was in a tunnel with no wi-fi or cell coverage and didn't receive the call, or maybe he was attacked and needs assistance. Monitoring lets your organization be proactive and notifies your team when a potential incident has occurred.

Beyond Mass Notification

Emergency Call Handling

Organizations often struggle to respond efficiently to 911 emergency calls placed within their campus. Fire trucks, rescue personnel or police arrive on campus and the internal security team is unaware of the situation, thus is unable to assist in directing the resources. And, since internal security was not aware of the situation, they have not been able to potentially dispatch assistance (internal resources) quicker.

To ensure best use and effectiveness of distress calls, you may want to immediately notify your local resources when an emergency call is placed. Instead of only routing the call to the municipal 911 services, consider the following options:

- Emergency Call Assist/Intervention Scenario
  - The caller, a local security agent and a municipal 911 service agent are joined in a three-party, no-hold conference
  - The local security agent sees the identity of the caller and can assist or intervene to resolve the call
  - The local security agent can add additional parties to the conference without putting the caller on hold or injecting tones
- Emergency Call Intercept Scenario
  - The caller and a local security office agent are joined in a two-party, no-hold conference
  - The local security agent sees the identity of the caller and determines if municipal emergency services are required
  - The local security agent can extend the conference to 911 municipal services and/or additional local responders

Crisis Team Collaboration

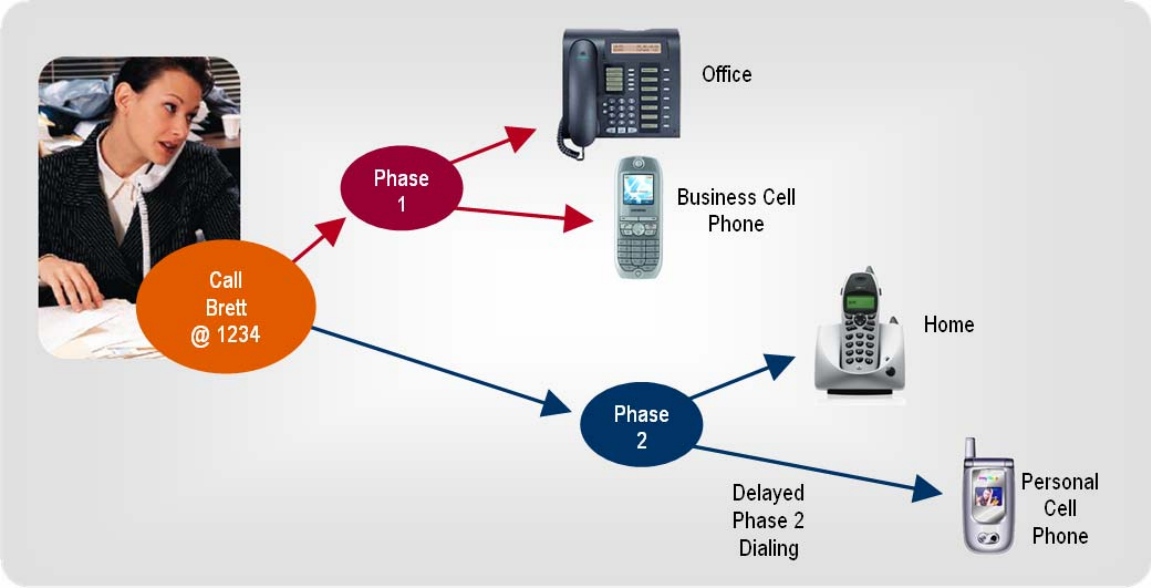
The first step in incident response, in many cases, is real-time collaboration among crisis response personnel to gather facts, coordinate activities and determine the messaging for notification alerts. Activation of an emergency conference that instantly connects first responders, decision makers and response coordinator is the missing piece at many companies today. You do not want to waste precious seconds while someone tries to manually join key resources in a conference or while you wait for the resources to dial into a bridge. Leverage available technology that can be preconfigured to dial out to key people with the click of a mouse, the push of a button or a telephone call from the site of an incident. And, if a resource does not answer on one phone number (such as office number), automatically dial secondary numbers until the contact is successfully reached.

Beyond Mass Notification

Personal Calling Services

Within all organizations, key resources – executives, security directors, IT manager – must be accessible at almost all times. To facilitate, these resources have many contact numbers – desk phones, wi-fi phones, mobile phones, pagers, etc. However, during a crisis event, time is critical and your goal is to accelerate and simplify the accessibility of key persons. How? Introduce calling services (sometimes also referred to as one number services) to use intelligent dialing of various target numbers. These targets can be called either simultaneously or sequentially, with one or more target number(s) dialed after the other.

For example, in the graphic, the caller dials extension 1234 to reach Brett. If Brett is not reached after a defined time of calling his office extension and cell phone, calls to his home number and personal cell phone are added. When Brett answers the call on one device, all other connections are released.



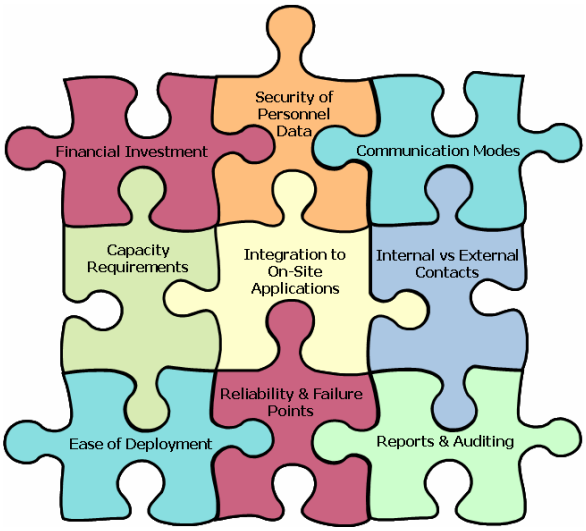
Coordinated Incident Response

Whether small or large, the unique aspects of each crisis incident require a unique response. And, each response may be a combination of collaboration, notifications and status updates. Coordinating the right steps at the right time, while leveraging the technologies that you have invested in, will contain the crisis and minimize panic.

Fitting the Pieces Together

Just like each crisis event is unique; each enterprise is unique. There is not a "cookie cutter" or "one size fits all" option that works for every organization. Each enterprise must assess their business requirements and environment and evaluate the priorities for their incident response solution.

Ask questions to uncover the key characteristics that are vital for your deployment. Questions may include:



- What is the financial investment I am willing to make? Do we have budget available or where can I find funds?
- What are the capacity requirements? Do we need to alert 50 people? 500 people? 50,000 people?
- Where does security of personnel data rank? Am I willing to have personnel information (such as names and contact information) stored at a hosted provider or do we prefer to keep that information behind our firewall?
- Is integrating to on-site applications important to my organization? Do I want to have automated alerts from fire alarms, refrigeration units, building security systems?
- Is subscriber management a priority? How do we keep contact information updated?
- What communication modes are most applicable for the enterprise? Do we want an emergency conferencing option? For mass notifications, will our organization have greater success with phone calls, screen pops, SMS, e-mail or some combination?
- Are there regulatory compliance issues that I need to consider? For instance, do the alerts need to be accessible to people with disabilities to meet Section 508 standards?
- What type of reporting and auditing is important? Do I need real-time visibility to the status and response during an alert?
- Is our business model to typically own and operate products on site? Or, do we prefer a hosted solution?

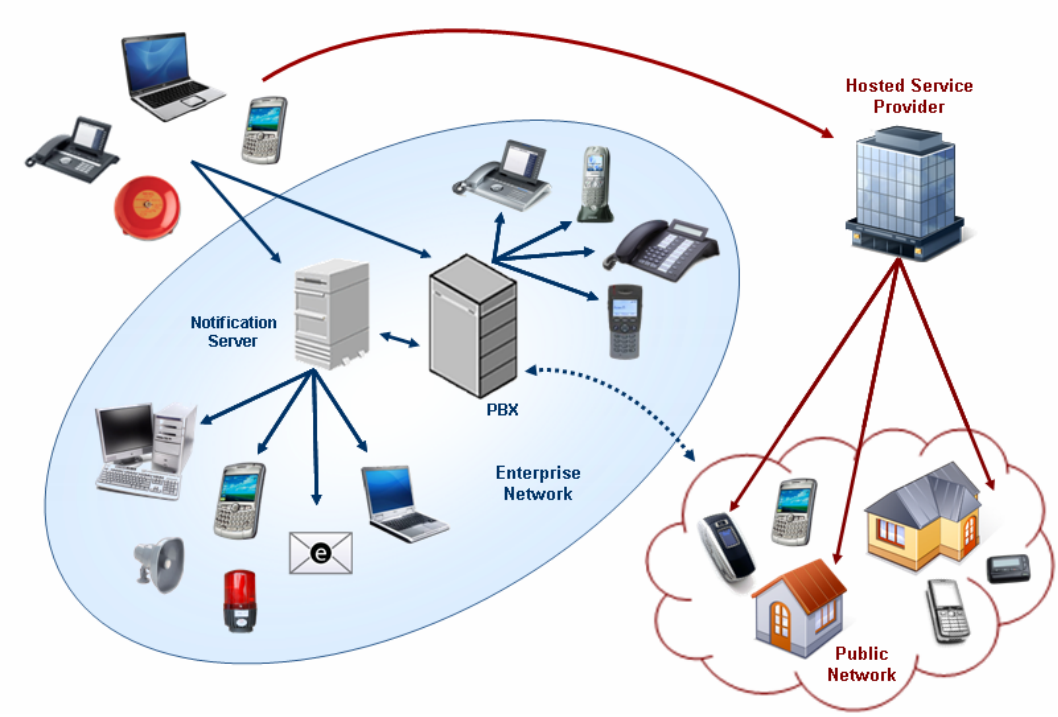
There are no wrong or right answers to most of the questions above. But, consider each topic carefully to assure you truly get the flexibility you need. For example, let's dig a little deeper into that last deployment model question. There are multiple deployment options, including:

- **On-Premise** – Entire system is deployed behind your firewall leverages secure integration with user directory databases and internal resources including IP network, PBX, Giant Voice and physical security sensors.

Fitting the Pieces Together

- **Hosted** – Available as a service from a remote hosting facility, speeds deployment and eliminates the need for on-site hardware.
- **On-Premise with Remote Telecommunications Option** – Application software is installed locally with secure access to remote center that handles mass telephony dialing and text messaging without taxing local telephony resources.
- **On-Premise with Failover** – Application software is installed locally with failover to another premise location or host facility, assuring redundancy.

In considering deployment strategies, the goal is to make best use of all your resources. If the vast majority of your communication is within your enterprise, leveraging a premise solution is optimal. You can mitigate the risks associated with hosted services, such as the PSTN network being overloaded and blocking calls into your facilities. If you have a split target base (on-premise devices such as desktop alerts, PBX extensions, wi-fi phones along with many cell phones and home numbers), then consider leveraging premise solution for internal alerts and complement with hosted system for SMS and PSTN/mobile phone calling.



Conclusion

Turn on the television, pick up a newspaper or surf your favorite news website and sadly the headlines continue to be safety and security events. A campus shooting, violence in the workplace, fires, deaths due to inclement weather. Are you prepared if the inevitable strikes your campus or business? Will incidents be contained without escalating? Will the impact to the organization and the time to return to normal operations be minimized?

Technology exists to contain an incident and return the organization to the normal operating state in a timely manner. And, in many situations, you don't need a complete overhaul or huge financial investment to meet the challenge. Transform your existing IP and telephony networks into a mass notification system. Turn desktop phones into silent alarms and panic buttons so employees are a button push away from help. Improve your 911 call response. Complement your existing communications infrastructure with the technologies and practices to assure that when seconds count after a crisis strikes, your organization will have the adaptive, rapid response you need.

About the Author

Becky Maycock is Director – Product Management for Impact Technologies. With more than 19 years of experience in telecommunications and 3 years working with customers in the emergency response business, Becky continually seeks ways to creatively and effectively leverage communications technology to solve real-world challenges. She is a registered Professional Engineer and has a BSEE degree from the University of Missouri-Rolla and an MS Information Networking degree from Carnegie Mellon University.

About Impact Technologies

When Impact Technologies was founded in 1990, our first product resulted directly from asking the simple question, "What can we do that will have a significant positive impact on your success?" We've never stopped asking that question. We have built a portfolio of high-impact solutions based on the input of customers like you. We remain passionate about and dedicated to the success of our customers.

Our experienced staff will partner with you to deliver communication solutions that are easy to use, and more importantly, highly adaptive to support your business rules and incident response strategies.

16650 Chesterfield Grove, St. Louis, MO 63005
voice: 314.743.1400
e-mail: solutions@impacttech.com
web: www.impacttech.com

