

THE SEVEN STEPS TO SUCCESSFUL BUSINESS CONTINUITY COMMUNICATIONS

Traditional methods of notifying people during a crisis, such as manual call trees and basic alerting systems, are no longer adequate for supporting increasingly vulnerable organizations. Broadening the scope of business continuity, organizations are taking measures to implement reliable, flexible, inbound and outbound communications, aimed at connecting and protecting both their infrastructure and people.

REAL BREAKDOWNS FROM INSUFFICIENT CRITICAL COMMUNICATIONS

Emergencies can widely vary in severity—ranging from natural disasters, pandemics, and terrorist attacks to local food-borne outbreaks and power outages—but their outcomes are often all too similar: a crippled infrastructure, severe financial loss, and even loss of life. While high-profile incidents like Hurricane Katrina are infrequent enough, even disasters at the micro level can cripple an organization. For example, digital attacks, including worms and viruses, have reached record levels in recent years, numbering close to 20,000 virus types and causing more than \$8 billion in damage a year worldwide.

Rudimentary communications solutions show significant draw-backs and can contribute to a large degree of loss. Major events over the past few years and a growing understanding of their associated costs have forced organizations in all industries to implement holistic, more sophisticated communications strategies to recover assets, maintain operations, and account for people's well-being.

Consider the following:

- A power failure caused by a flaring incident occurred at the ConocoPhillips refinery in Rodeo, CA. As a result, the company needed to issue and send notification of a temporary shelter in place for those people affected—both inside and outside of the organization. However, the emergency phone system was only able to call roughly half of the impacted homes and businesses.
- A municipal organization contracted with a company to send automated calls to 6,200 households and businesses, alerting people that spraying for mosquitoes was to begin in response to an Encephalitis warning. After 4,000 calls, an error caused the notifications system to dial the same numbers over and over. Some people got as many as 15 calls and others did not get any message. In addition, another system glitch misidentified the affected community, and triggered a false alarm on the Encephalitis scare.
- In May 2005, a small plane piloted by a student and his teacher accidentally entered air space three miles from the White House. As part of the response, many Federal buildings in Washington, DC were evacuated. Despite swift response to what was later deemed a non-threatening event, the government's emergency notification system became the subject of intense

According to the National Institute of Technology and Standards (NIST), "the inability of first responders from many different agencies to communicate and share data greatly hampered the emergency response to the events of September 11."

scrutiny. Even though the evacuation was a success overall, the President (who was nearby in Maryland) had not been taken to a secure location because the White House's emergency communication system itself had failed.

The outcome of these incidents expose common weaknesses that exist in all too many organizations; they simply do not have reliable communications system to respond to what they can't predict. What may have been learned from these events and others like it is that an emergency response plan is only as effective as the ability to follow through and coordinate during an event.

These events also underscore our growing focus on crisis management—namely, crisis communications—and a new way of addressing emergency preparedness. It's not only critical to have a communications plan in the event of an emergency but also the resources and capabilities to carry out that plan effectively when an emergency strikes.

SEVEN STEPS TOWARD EFFECTIVE BUSINESS CONTINUITY COMMUNICATIONS

To successfully communicate with relevant parties during critical events, organizations need a system that can enhance their preparedness and contribute to the overall security of human, physical, and information assets.

What follows is an overview of common steps organizations are taking in order to connect, protect, and account for their people, while enabling response teams and decision makers to coordinate a successful recovery and help protect assets and infrastructure—even such things as supply chain and key customer relationships. To ensure organizational resilience, business continuity communications should consider the following:

1. Boost the volume and speed of your message delivery
2. Leverage multiple channels (phone, text, email, etc.)
3. Enable decision makers to work together
4. Track and respond to those who got the message
5. Build a reliable infrastructure
6. Employ both inbound and outbound communications
7. Integrate with your current technology

1) BOOST THE SPEED AND VOLUME OF DELIVERY

Generally, emergencies just happen; that's part of what makes them emergencies. When an emergency strikes, it's absolutely critical to be able to communicate the situation to the affected public and key individuals as rapidly as possible. This provides the most effective protection while minimizing the spread of rumors or misinformation, and enables more consistent, better informed decision making. Take, for example, the small plane

incident at the White House: While evacuations were handled in approximately five to six minutes, a plane traveling at 150 mph could reach its target in just over a minute. Real-life incidents leave very little time for error.

In this particular situation, a reliable communications system could have kept people from being told to remain in their buildings, only to be evacuated a minute later by uniformed security guards running through the halls.

How quickly and accurately you disseminate information is what allows response teams to effectively carry out a plan. While it's certainly important to pre-plan as much as possible, the nature of critical events is such that they will frequently push past the design scope of any possible planning. When an organization uses a more sophisticated crisis communication system that can send a large volume of messages very quickly and reliably, the much higher are the odds that the crisis can be successfully negotiated.

Organizations are increasingly managing this issue by employing solutions that provide a high degree of flexibility, including such elements as ad hoc messaging, where an "on-the-spot" message can be recorded immediately by an authorized individual, then, with the push of a button, delivered to thousands or tens of thousands of people within a few minutes.

2) LEVERAGE MULTIPLE CHANNELS

As organizations become increasingly more distributed and operations more dispersed, reaching everyone affected by a crisis requires leveraging every available communications device (e.g. text messages, e-mail, voice). Outbound and inbound multi-channel communication increases the likelihood that those directly affected by the situation will receive critical information and updates when they're most needed.

Further, effective crisis communications should have a rules-driven incident escalation capability. This capability enables recipients to specify devices for receiving emergency messages and choose how messages will be escalated. For example, escalation rules can set a pre-determined number of retries to a landline phone, then default to a cell phone that is designated as the first backup channel. In addition, organizations can also apply person-to-person escalation rules, so that if Recipient A cannot be reached, Recipient B is contacted. These rules help ensure that messages reach their intended target to keep people informed of an incident, and to better help manage through the crisis.

The best communications systems also have international message capabilities, which means they can handle multiple languages, and can navigate through ring tones and dialing conventions unique to different countries.

3) ENABLE DECISION MAKERS TO WORK TOGETHER

The major decisions any enterprise organization makes on a normal day are often based on research, careful deliberation, and collaboration among leadership. Any move that poses significant impact to employees and other constituents is rarely made by one person on the spot. Emergencies don't allow for this luxury.

Response teams are often limited in their ability to work together. Staying on top of an emergency situation as it unfolds requires input from the field and uniform decision making across satellite groups and multiple channels. For first responders in particular, it is critical to be unified and organized before, during, and even after an incident. Further, a successful emergency response calculates known risks, evolves and changes based on information returned from a field that may span multiple locations and responds to what you know at every minute throughout the crisis. Response teams execute decisions more effectively when they are able to communicate with one another—frequently and consistently.

Automated notification systems are often key to facilitating this type of collaboration. Not only can these systems send the emergency communications to an organization's first responders, but can also be used to alert executives and seek their decisions on procedure. Calls can be placed to their home, cell, hotel, etc. with a brief message detailing the incident. If discussion is warranted, organizations can plan to set up a conference bridge or intranet site for executives to collaborate in real time.

4) TRACK AND RESPOND TO THOSE WHO GOT THE MESSAGE

The only way to monitor and respond to everyone affected by a crisis is to track their status through detailed reports. Flexible, real-time reporting helps the enterprise interact with message recipients during emergency situations, making it easier to monitor personnel, better manage the crisis situation and provide immediate assistance. This helps ensure that business continuity plans and procedures are followed, and creates audit trails for regulatory compliance.

In addition, analyzing results through a rich set of reports means that future communications to response teams and your entire organization can be tailored even more effectively, potential system weaknesses can be uncovered and attended to, and ongoing improvements can be made on a systematic basis.

A wide range of response options help the enterprise to interact with message recipients during emergency situations, making it easier to track and monitor personnel, provide immediate assistance, and ensure procedures are followed.

5) BUILD A RELIABLE INFRASTRUCTURE

A reliable communications infrastructure should contain three key attributes:

High availability and reliability: The communications infrastructure should be a multiple-tier, multiple-server architecture that provides redundancy at every point in the message delivery process. Redundant servers should support each system function, data connections are distributed to separate backbones, and telephone connections should be sent to multiple telephone switches.

High security: Because of the sensitivity of business continuity communications, the infrastructure should provide multiple levels of security to ensure that only authorized individuals can initiate, administer, and receive messages. These security layers include username and password authentication to prevent unauthorized access, and an authenticated user-level of access to define what individual users are allowed to do. The integrity of messages during transmission should be protected using industry-standard, 128-bit Secure Socket Layer (SSL) encryption. And physical hosting sites should provide a secured cage and locking cabinet environment, continuously monitored cameras that are placed throughout the facility, and sophisticated personnel entry controls.

High Capacity: As a single message can generate multiple delivery attempts, business continuity messages can number in the hundreds of thousands, if not millions. To ensure delivery of extremely high message volumes within guaranteed timeframes, the communications infrastructure should allow for large-scale message volumes, should it be needed, and guarantee delivery to meet service level agreements (SLAs) every time.

Who will you call?

In an emergency notification situation, there are three main audiences with whom an organization must communicate:

1. **First Responders** – These resources include the Business Continuity, Disaster Recovery, and IT Teams who are charged with containing the damage and resolving the situation.
2. **Employees** – These are the people who will be most directly affected by the incident. They need to know what is going on and what they should do as soon as possible.
3. **External Stakeholders** – This includes vendors, partners, key customers, media, and local authorities/ regulators, as necessary.

Even though there are three distinct levels, it is critical that all be reached with the information they need to manage the incident within a precisely defined and constrained period of time – if not instantaneously.

6) INTEGRATE BOTH INBOUND AND OUTBOUND COMMUNICATIONS

Effective emergency communications cannot be a one-way street. In addition to being able to reach out to constituents rapidly and effectively through a variety of channels, organizations must also provide a reliable method for receiving critical updates and other information from staff.

Outbound communications is critical for notifying workers of an unplanned event, providing accurate, tension-defusing information, and delivering critical status updates. But, outbound communications, by itself, can have significant limitations in an emergency situation. Outbound communications can inform, but cannot receive information from the field.

Integrating inbound communications enables workers to report on status and well being from the field, let others know of urgent needs, and provide on the spot updates of work-readiness. In short, inbound communications offer organizations a real-time view of employee status, field readiness and more. This provides a further safety net for workers, both from an organizational and psychological standpoint, as they are not simply receiving information, but are communicating back inwards, providing information from the field, making requests for assistance, and more.

7) INTEGRATE WITH YOUR CURRENT TECHNOLOGY

How well you integrate with your current system often defines success. Communications system should easily integrate with corporate applications, systems, and databases. Enterprises need to leverage existing information to personalize messages with pre-populated data, such as an individual's name and account number extracted from a customer database. It also enables automatic message delivery to be triggered by events captured in corporate systems. Finally, integration with corporate systems, such as a human resources database, helps ensure that contact information is current and consistent. Enabling self-service updates of contact information can also allow for data accuracy and integrity. For example, integrating sign-up and entry via a simple one-stop Web site makes it easy to update contact information.

HOW TO SELECT THE RIGHT CRISIS NOTIFICATION TECHNOLOGY

While technology isn't the only consideration in planning your emergency communications efforts, it is a vital component. The last thing you want is for administrators and recipients to be well-trained, and then find that the system you chose can't meet its promises.

The consequences of a failed notification system can be more severe than not having an automated system at all. Therefore, choosing a solution requires comparing competing technologies on the basis of risk/reward and cost/quality. A low-cost solution may seem like a good deal, but with millions of dollars' worth of sales and assets at stake, the

purchaser should be willing to bet his or her job – and the company’s future – on the bargain paying off.

When choosing an automated solution, demand to see metrics from the provider, such as the number of messages delivered, peak-volume performance and capacity, availability rates, and, of course, the range of service level agreements (SLA's) offered and attained. Providers should be able to present prospective customers with demonstrable proof of SLA compliance over time. Guarantees mean nothing without a documented history of compliance behind them. Vendors should also be able to reference a strong disaster recovery plan and demonstrate the extent to which their solution is fault-tolerant.

Organizations also need to partner with a vendor whose solutions can address the real world challenges they experience in times of crisis. To promote recovery and resilience during disaster recovery, emergency communications must connect with affected individuals, regardless of infrastructure challenges.

Your hosted vendor needs to include multiple-tier, multiple-server architecture that provides redundancy at every point in the creation and delivery process with shared phone lines for inbound calls to assure bandwidth. An ongoing dialogue with your vendor can also help you best determine who you will need to contact in an emergency and identify those in your organization who can make critical decisions. But, don't take their word for it: prove it by requesting a test.

About Varolii Corporation

PAR3 Communications and EnvoyWorldWide are now Varolii Corporation.

Seattle-based Varolii Corporation provides interactive communication solutions delivered through a Software as a Service (SaaS) model. Derived from the *Pons Varolii*, the pathway in the brain that unites intelligence and learning with the ability to communicate, the name Varolii evokes the blending of innovative communications technologies with knowledge, learning, and best practices. Enterprises across industries leverage these solutions to automate more of the communications process, resulting in improved operational performance and enhanced customer relationships. Varolii's multi-channel solutions deliver ongoing value based on its unique delivery model which combines the convenience of SaaS with a fully managed services environment, an approach that ensures clients achieve an immediate, sustainable ROI.

Varolii is headquartered in Seattle, WA, with offices and data centers in Denver, CO; Chicago, IL; and Boston, MA. For more information visit www.varolii.com.

For more information, please contact Varolii Corporation at:

1-800-206-2979 or info@varolii.com

Or visit: www.Varolii.com

821 Second Ave. • Suite 1000 • Seattle, Washington 98104