DISASTERCOM

DERA Newsletter | **49 Years of Service** | **April 2011**

Australia, New Zealand & Japan

Preliminary Lessons Learned from Catastrophic Disasters

DERA invites journal-length field reports and research articles on catastrophic events that have far-reaching impact on the global community. Articles may focus on any aspect of preparedness, response, recovery and mitigation. Submissions will be peer-reviewed prior to publication. Articles selected for publication will appear in the DERA DisasterCom World Journal. Submissions must be received by July 31, 2011, and may be mailed or sent electronically to the DisasterCom Editor.

By their very nature, catastrophic disasters initially overwhelm all available response capabilities and seriously strain the resources of even the most highly prepared societies. *Catastrophic* is a relative term, of course, as events that might devastate one community might possibly be within the ability of another to handle. Nevertheless, massive natural disasters and man-made events in recent years have given the world community clear examples of situations that challenge even the global ability to respond: Chernobyl (1986), the Indian Ocean Tsunami (2004), Hurricanes Katrina/Rita/Wilma (2005), the Sichuan earthquake (2008) the earthquake in Haiti (2010), the decades-long famines in Africa, and the horrors of war all have become part of our collective memory and imagery of "catastrophe."

With that as background, the year 2011 has begun with three uniquely different, but history-making catastrophic disasters: The Queensland - Victoria floods in Australia, the Christchurch earthquake in New Zealand, and the earthquake/tsunami/nuclear emergency in Japan. The purpose of this brief article is to summarize preliminary lessons-learned from these events so that preparedness efforts around the world can be enhanced.

Queensland and Victoria Floods

Beginning in December 2010, the state of Queensland in Australia began receiving exceptionally heavy rainfall as a result of the *La Niña* climate cycle. Preliminary forecasts were that flooding might be comparable to that experienced in 1893 and 1973/74, during previous climate cycles, and for which Queensland was relatively well prepared. However, Tropical Cyclone Tasha brought record rainfall to Queensland just as an unusually intense *La Niña* set in. Rainfall, measured by the hour or the month, was the most ever recorded in the area. By the end of December, even heavier monsoon rains had started. Flood control and irrigation projects were overwhelmed and could no longer hold back additional water.

Cities, towns and communities along the Brisbane, Fitzroy and Burnett Rivers, among many others, flooded. An urban flashflood devastated the business district of Toowoomba. Over 70 cities and towns were inundated and 200,000 people were either evacuated or stranded. Hundreds of roads including ten major highways were closed, as were regional and local airports. Mining, industry and commerce were severely affected. By the end of January, 35 people had been killed in Queensland and many were still missing. Also by late January, extensive flooding spread to the western and central regions of the state of Victoria, where over 50 cities and towns were flooded. Many communities remained flooded for several weeks, and some experienced multiple floods over three months.

The Australian Broadcasting Corporation estimates that the economic impact of these floods will exceed $30 billion, with an immediate reduction in Australia's Gross Domestic Product (GDP) or $13 billion. This represents major harm to the national economy, which will complicate the financing of long-term recovery and mitigation.

Photo: Australian Government, Attorney-General's Department

What worked well: (1) Public Alert and Warning (2) Public cooperation with evacuation orders (3) Continuity of Government (4) Widespread volunteerism (5) NGO response and cooperation (5) Cooperation between the Australian Defence Force and civil authorities (6) Mutual Aid (7) Standard Emergency Warning Signal (SEWS)..

Lessons Learned: (1) Planning for a recurrence of the worst flood in modern history may not be enough (2) Individuals and families need to prepare themselves to be self-sufficient for many days, not just a few hours (3) Off-site backup of critical data and vital records is essential (4) Electric power generation and recharging of batteries for communications and medical equipment is critical (5) Land use planning and development projects must take into account climate cycles and potential change, not simply recent weather history.

Christchurch, New Zealand Earthquake

New Zealand has experienced strong earthquakes throughout its history and in general the government and population have taken reasonable precautions. Known begrudgingly by some as "the Shaky Isles", New Zealand normally experiences about 20,000 measurable earthquakes per year, with 200 of them being strong enough to be felt. Following the Hawke's Bay earthquake of 1931 which killed 231 people, national and local governments intensified efforts at controlling unreinforced masonry structures, an effort which first began in 1840 when masonry structures collapsed during the Wellington earthquake. Following the 1968 earthquake, strict building codes were enforced, and these were improved through the years as engineering science improved. ***Cont'd p. 3***

DisasterCom is the quarterly newsletter of DERA International. News items and articles are always welcome.
ISSN 1521-1592 Editor: Kathryn M. Dunlevy-Wilson
Membership in this Nonprofit Association is open to all who share our commitment to effective disaster preparedness and response.
See back page for Membership Application
The Disaster Preparedness and Emergency Response Association, International
P.O. Box 797, Longmont, CO 80502 (USA)

E-Mail: dera@disasters.org News Items: editor@disasters.org www.disasters.org

DERA International

P.O. Box 797
Longmont, CO 80502

DERA is a Nonprofit, U.S. IRS 501(c)(3) Disaster Service and Professional Association Established in 1962
Incorporated in the State of Wisconsin.
Newsletter ISSN 1521-1592.

DERA QR-Code. Please copy & share.

Partnerships & Affiliations Include

ARRL
American Radio Relay League
www.arrl.org

CNA
Colorado Nonprofit Association
www.ColoradoNonprofits.org

EM Forum
www.emforum.org

EMLRC
Emergency Medicine Learning Resource Center
www.emlrc.org

FAIRS
Foundation for Amateur International Radio Service
www.fairs.org

Florida VOAD
www.flvoad.org

International Assn of Emergency Managers
IAEM
www.iaem.com

NIAR
National Institute of Amateur Radio (India)
www.niar.org

New Member Roster

Welcome to DERA!

Scott R. Gothard, W6SRG
Folsom, California

Keith Llewellyn
Yonkers, New York

Dr. Kourtney Nieves
Mascotte, Florida

Ron Whatley
Houston, Texas

Kevin Salsbery
Lakeland, Florida

Pelin Ulrich
Tacoma, Washington

Shane Cork
Cincinnati, Ohio

Chris Krzos
Plainfield, Illinois

Christopher A. Abshire
Clovis, California

Letter from the Chair

"Who You Gonna Call"?

As I travel, I am reminded that the number I need to call in an emergency is highly dependent on where I am and the device I am using. In the United States, if I am at home and call 911, I connect to a Public Safety Answering Point (PSAP). Based on the type of call, it is rerouted to the appropriate response authority. In my area, my Caller ID is also attached when I call so the PSAP can determine the physical address associated with the phone number. If I call through my computer, I will be connected to a service agency, but not necessarily the one that services my home.

Depending on how old you are and where you are in the world, you may have used 112 for some services. If you were in Paris at some point, you would have dialed 18 for the fire brigade, but the initial implementation was limited and did not become widespread until almost 40 years later. Today, a variety of emergency numbers are used around the world, 999 and 000 being perhaps the most common.

The first 911 implementation in North America was in 1959 in Winnipeg, Manitoba.. After the use of 911 in the United States was announced, a small southern independent phone company was the first to implement it. It took many years to expand across the US and now include Automatic Number Identification and Automatic Location Information (ANI/ALI). The mission of the National Emergency Number Association (NENA) is to foster the technology and implementation of a single emergency number.

From cell phones the use of any emergency number may or may not get you where you want to be connected. I was travelling on a highway along a major lake and called 911 to report an unsafe condition. Unfortunately, the nearest connection was on the other side of the lake in a different state.

If you are in a commercial facility, do you dial 911 or 9-911? The answer depends on how the company wired their

(Cont'd p. 7)

(Cont'd from p. 1)

A magnitude 7.1 earthquake hit the Canterbury area on September 4, 2010, causing major damage, but resulting in no fatalities. Seismologists have technically classified the next event as an aftershock from the Canterbury event: Early on the afternoon of February 21, 2011, a magnitude 6.3 earthquake occurred about 10 kilometers southeast of downtown Christchurch, near the town of Lyttelton. The impact on Christchurch and the surrounding area was devastating, with heavy loss of life, massive collapse of buildings, and irrepairable damage to many historical structures.

At least 172 individuals representing over 20 nationalities perished in the disaster; there are still reports of missing persons and many people rescued have life-threatening injuries.

As many as 10,000 homes in the area and 1,000 buildings in the city center of Christchurch will likely be demolished, including the Grand Chancellor Hotel, one of the tallest buildings in the city. The Canterbury Television (CTV) headquarters and studio building collapsed then burned with heavy loss of life to broadcast staff and faculty, staff and students from an exclusive international school in the building. Other buildings thought to be earthquake-resistant also collapsed or were severely damaged including headquarters for major corporations.

Lyttelton

Photo courtesy Christchurch City Library

Fortunately, the Christchurch Airport remained open with only minor damage, which allowed for massive logistics, medical, and technical support from throughout New Zealand, Austrailia and around the world. Urban Search and Rescue Teams arrived from elsewhere in NZ and Australia, the UK, the USA, Japan, Singapore, China, and Taiwan, and Thailand, UK, Australia, Taiwan and Israel sent Disaster Victim Identification (DVI) teams, all under the command of the New Zealand Fire Service. The first foreign team to arrive was the Australian New South Wales SAR team, which arrived 12 hours after the earthquake, followed shortly by the SAR team and search dogs from Queensland. The great distances involved created long travel times for other foreign teams, leaving the NZ and AUS teams to manage as best they could until additional resources could arrive. The Japanese SAR team remained in NZ until they were urgently called home on March 11th due to their own earthquake and tsunami.

Cathedral of the Blessed Sacrament

Photo courtesy of Gobierne

What worked well: (1) Modern building codes saved lives (2) Emergency planning and exercises prepared the public and responders (3) Orderly incident command resulted in effective prioritization (4) Hospitals remained intact (4) NZ and AUS help was nearby (5) Airport remained open (6) AUS police were quickly augmented into the NZ force

Lessons Learned: (1) Utilities and infrastructure damage will take a long time to repair (2) Not all earthquake-resistant buildings may survive (3) The public may have to deal with sanitation and sewage issues, and may have to collect rainwater for drinking (4) Road and bridge damage hampers rescue efforts (5) Not all persons reported as missing may ever be accounted for (6) Financing recovery and future mitigation projects is a major challenge, given the disaster's impact on the economy.

Japanese Earthquake, Tsunami and Nuclear Emergency

On March 11, 2011, a magnitude 9.0 earthquake occurred off the northeast coast of Japan, causing massive damage and triggering a powerful tsunami that brought widespread devastation to cities and extreme damage to a nuclear power facility. Final casualty figures are not known, but at least 14,600 individuals perished, nearly 6,000 were seriously injured, and over 11,000 remain missing in 18 prefectures. More than 120,000 buildings were damaged or destroyed. Almost five million households lost electric service and over one million lost their source of drinking water for an extended period of time. A bitter winter storm made survival and rescue more difficult. Many major industrial plants ceased operation, leading to world-wide disruption of manufacturing because of supply-chain disruption.

Damage to the Fukushima Nuclear Power Plant was extreme, and a small group of workers, honorably named the "Nuclear Samurai" continue to work around the clock to contain the damage and control the release of radioactivity.

The extent of damage, massive loss of life, and continuing nuclear emergency make it impossible to condense these three interrelated disasters into a brief summary; however some preliminary conclusions are becoming apparent.

Minamisanrikucho

Photo courtesy of UMHealthSystem

What worked well: (1) Earthquake-Tsunami analysis systems accurately assessed impact and predicted tsunami locale (2) Public Warning Systems used a variety of technologies including wireless and broadband plus outdoor sirens (3) Public awareness and readiness saved lives when people acted quickly and properly (4) Strong building codes prevented even worse damage (5) Influx of domestic & international aid was orderly

Lessons Learned: (1) Infrastructure needed to manage response, such as communications, roads, airports, electricity, becomes disrupted when needed most (2) Some critical facilities may not be as well prepared as expected...independent verification is essential (3) A few seconds can mean the difference between life and death. Training and drills are essential (4) Outside aid can be delayed for many uncontrollable reasons (5) Emergency teams need adequate backup teams to avoid burnout and damage to health (6) Plan for the worst...not the most likely.

The Small and Medium Size Business Guide to a Successful Continuity Program

by
Sal Meloro
smeloro@comcast.net

A Business by Any Other Name Is Still a Business

We'll start with a simple premise, and your acceptance, that you are a business. It doesn't matter if you previously labeled your entity as a company, business, department, agency, branch, district, firm, organization, hospital, office, institution, publisher, church, corporation, authority, or partnership. You're a business. You may be part of the public or private sector, but you're a business. It doesn't matter if you consider yourself small, medium in size or large, that you produce or deliver materials, goods or services, or you are for profit or not for profit. You're still a business, perform all of the functions any business performs, and you need to think like one.

A business starts with some form of business plan or mission statement. The business grows and expands, remains stagnant or stable, or ceases to exist. Finally, the business has risks and exposures from natural or man-made disasters.

So are small businesses really different from large ones? The answer is very much so, but not really. If you break it down, you will find that the only differences come in the complexity, number of functions performed, and the number of employees. Other than that, small businesses generally do the same things as large businesses; only they perform them on a much smaller scale. As an example, in a small business, the accounting department may be a staff of 1 or 2. In a large business, the accounting department may easily exceed a hundred. In a large company there may easily be 2 or more full time emergency planners that are certified. In a small company it may be an additional assignment given to someone that has no experience. The point is, the basic needs of both large and small businesses are the same; it's just on a different scale.

A Realistic, Achievable, and Functional Continuity Program

Almost everyone reading this article is part of an organization that has interest in developing a disaster recovery or business recovery plan. However, as we progress, you'll learn that both types of plans are really required. Furthermore, at this time you're most likely thinking only about a written "plan". It is my hope that I can expand your thinking beyond just having a plan. Hopefully, you'll want to start thinking about a total "program", one that also includes the plan you're looking for.

A continuity program is a proactive methodology that provides a multi-faceted approach to your business' emergency planning. The steps to achieving this type of ongoing program are outlined within this document. Each identified step follows what is considered "*best practices*"; however, the requirements are scaled down to meet the needs of the small to medium size business.

The bottom line is to keep the process simple and straightforward so that you will implement and maintain a program. Furthermore, this must be accomplished without compromising the integrity of your program or business readiness.

Types of Disasters and Degree of Readiness

As a small or medium size business, you are exposed to the same potential disasters as any large business. You are just as much at risk as every other business within your city, no more and no less.

Disasters fall within two categories:

· Local: This type of disaster generally impacts a narrow geographic area. Usually it is confined to a single building or adjacent buildings. Quite often they are man-made, whether caused by fire, explosion, terrorism, chemical spill, etc. With this type of disaster, you can expect outside assistance in responding to your emergency.

· Regional: This type of disaster affects a wide geographic area and is often attributed to a natural event. The causes could be hurricane, flood, earthquake, tornado, etc. With this type of disaster, both the Red Cross and FEMA recommend that you be self-sufficient for the first (72) hours following the event. Expect no outside assistance.

When doing continuity planning, you need to plan for a worst-case scenario. That is, a disaster occurs that prevents you from returning to your normal work location for a prolonged period of time, if ever. Therefore, you need to have a program in place that will enable you to respond to the event, recover your work environment, and resume your business activities. And you need to do this using only a written plan and information you've stored offsite.

If you are ready for a worst-case disaster, you should be ready for a disaster of a lesser magnitude.

Continuity Program Best Practices

Remember, a continuity program is a multi-faceted approach to preparing your business ahead of time. The following steps come after decades of experience. Each step offers something toward ensuring that your business is ready to respond to, recover from, and resume operations after a disaster. Each step is important, and if you simply implement only a few of the steps, you may leave your business far short of truly being ready for a disaster. Would you be better off with only a few steps in place? Probably, but that is not what you want, for in a real disaster, you want to be ready, not just better off.

If you've made it this far into the article, there is a good chance that you are truly interested in developing a continuity program. Furthermore, once the steps are outlined, and you fully understand the concepts and approach, there is a good chance you'll complete the process. At the end of each step I've included some very rough estimates of what each step may cost to implement.

Step 1 – Obtain Management Commitment to a Continuity Program

The development of any continuity program will take hours of staff time to implement as well as financial resources. To obtain those resources, management needs to commit to the process. To

obtain approval, there are numerous justifications that can be presented.

To start with, research any laws, regulations, or codes that pertain to your line of business. These often apply to health care providers, insurance, financial institutions, and government entities. Also, look at any contracts that you may have with your customers that require you to have an emergency plan. If any exist, justification becomes relatively easy.

Additional reasons may include: audit requirements; liability exposures; competitive edge in future business; life, health and safety issues; intangible loses such as customers; or processes in place to save the business following a disaster.

Once you have identified the various reasons for implementing a continuity program, you need to assemble a document to present to management. Within that document, you will want to:

· Identify potential risks to the business
· Define what a continuity program is
· List the steps required for implementation
· Provide an implementation timeline
· Document the justification(s)
· Furnish estimated costs
· Conclude with a recommendation.

Schedule a meeting and present to management. Your objective is to obtain approval to proceed with the process.

Estimated Cost: About 4 – 6 hours to put together a recommendation

Step 2 – Identify Your Disaster Recovery /Continuity Program Administrator

Though a continuity program is an entire business responsibility, one individual needs to assume ownership of the process. That individual will address the risk and business assessment, ensure that written plans are developed and maintained, arrange for offsite storage, identify alternate work locations, and train and test the process.

Estimated Cost: About 2 – 3 hours to put together a recommendation with documented duties

Step 3 – Perform Risk Assessment

We start with a philosophy that it is often easier, quicker, and less costly to prevent a disaster than to try to recover from one. However, in order to accomplish this, you first need to know what your risks and exposures are, and, if economically feasible, you can then eliminate them.

This is where risk assessment comes in. It is a “discovery” process that any business can undertake to identify potential threats. As a starting point, may I suggest that you address: your work area, building location, security, building support equipment, safety, etc. Walk around your building and property to look for situations that can potentially cause problems. Ask questions internally and call in outside assistance if you are not certain. As you undertake the process, identify and list any and all noted risks or problems that could cause or contribute to a disaster.

Though there is a formula to use, we’ll keep the process simple in identifying what you need to mitigate. Sequence the list of identified risks that you previously made, placing the risks with the highest odds of occurring and have the greatest potential for impact on top of that list.

Starting at the top of the list, identify alternate solutions that will enable you to correct the risk. Obtain cost estimates to implement the solution and present to management for approval and subsequent implementation.

Estimated Cost: 2 hours to develop a strategy, 2-4 hours to do an assessment, 2-4 hours to research and document mitigation options, and 2-4 hours to obtain and document costs to correct potential risks. The cost associated with the risk corrections are contingent on the risks you identify and recommend for correction.

Step 4 – Perform a Business Impact Assessment

In order to progress any further in the development of your continuity program, it is important that you understand your total business. First, all work groups within your business need to be identified. This is important, as you will be meeting with the managers of these groups later in this process.

Next, develop a questionnaire for your upcoming meetings with the various work groups. As a starter, find out in detail what functions the group performs. Understand the group’s reliance on both internal and external information and data. What tools and resources do they use? What are their critical systems? Where does the information they produce go? Do you use critical hardcopy records that are not replicated offsite? What is the impact on the business if they could not perform their business functions for a day, three days, a week, or a month? Do they require special equipment or tools? Do they have certain functions they perform that are more critical than others? Who are their vendors? Add other questions that may be pertinent to your specific business. Are there financial penalties associated with missed deliveries?

Finally, schedule some time with each of the work group managers or supervisors and walk through the questionnaire. When you have finished with all of the work groups, retain this information for later use.

Cost Estimate: About 1 - 2 hours preparing questions and 1 hour x 2 staff members for each work group you meet with.

Step 5 – Identify Recovery / Resumption Strategies

Schedule a planning session with management to discuss the business recovery objectives. Have available the information you collected in your impact assessment. During this session, address alternate work locations, work group recovery priorities, recovery time lines, an emergency command center location to coordinate recovery, and information system recovery strategy.

The agreed upon recovery and resumption strategies will be used in the development of your written continuity plan.

Estimated Cost: About 4 – 8 hours depending on the number of staff members you want to include in the planning session.

Step 6 – Develop a Written Continuity Plan

So what is a Continuity Plan (CP)? At a high level, a CP is really three types of emergency plans that have been merged into a single and all-inclusive written document. It is a comprehensive written plan designed to address:

1. *Emergency Response* – Life, health, safety, evacuation, floor wardens, emergency notification, exit routes, etc.

2. *Disaster Recovery* – Recovery and resumption of your information systems hardware, software, data, and network functions.

3. *Business Recovery* – Recovery and resumption of your primary business functions and the various support groups such as: accounting, HR, payroll, etc.

Any CP should address five primary stages or phases that take place from the time of the event to the time you relocate back to your permanent work location. Those stages are:

STAGE 1 – Response - Activity immediately following the event. Life, health, and safety actions are your primary concern. If possible, contain the source of the problem. Provide first aid, evacuate personnel, notify emergency services, alert other team leaders, etc.

There is no recovery within this stage, as actions are limited to damage assessment, making notifications, and assembly of the incident management team.

STAGE 2 – Recovery of work area and resources. When safe, or at another location, you must now start to restore your work environment. Until this has been completed, you cannot resume your business functions. The objective is to recover your work environment as nearly as possible to the way it was before the event occurred.

STAGE 3 – Resumption of business functions. Following your work area recovery, you are ready to resume certain business functions. Depending on the situation, some or all of the functions will resume operation in a systematic and prioritized fashion. Also of note, if a function is resumed, it may be limited in scope for a period of time.

STAGE 4 – Reconstruction of damaged facility. In this stage, the recovery team documents the steps that will need to be taken to clean up damage building and/or reconstruct facilities. If the building has been destroyed, another permanent facility will need to be located.

STAGE 5 – Relocation back to your rebuilt facility. Documents the process you will take
to move back.

For the smallest of businesses, those with less than 20 employees, the CP will be one document that addresses all five stages. However, for small businesses that have more than 20 employees, the concept of recovery teams will need to be used. That is, your CP will be comprised of multiple recovery teams.

Recovery teams are a simple way to break your CP into manageable groupings of activities. Furthermore, the larger a business is, the more recovery teams you will utilize. An easy way to understand this concept is to provide some examples for you to reference.

A small business with about 20 to 40 staff members may use 4 recovery teams:
· Emergency Response and Damage Assessment Team
· Crisis Management and Administration Team
· Information Systems and Voice and Data Team
· Core Business and Support Function Team

A small business which has expanded to about 40 to 80 employees, may use 8 recovery teams:
· Emergency Response Team
· Damage Assessment and Reconstruction Team
· Information Systems Team
· Corporate Support Team
· Core Business Team
· Voice & Data Team
· Administration Team
· Crisis Management Team

Finally, taking it another step further, a larger business of around 140 employees may use the previously mentioned 8 teams, but may add 3 additional Core Business Teams, and/or they may want to split the Information Systems Team into two different teams (one for hardware/systems and one for application software).

The bigger the business, the more recovery teams you will need. Each team will have a team leader and backup. The team leader is responsible for developing their team's plan by identifying what tasks need to be performed within each stage. Finally, each team leader must document how to perform each task.

Once the team plans are completely developed, the continuity plan administrator will review each plan for accuracy and detail. The information gathered in the previously taken business impact assessment can be used as a reference and check point.

In closing, once all the team plans have been developed, then, and only then, do you have a CP.

There are some very good software plan development tools available. Select a product that meets your needs as opposed to trying to develop it yourself. By utilizing software templates, your CP will be more comprehensive, it will utilize proven methodologies, the plan will be developed quicker, and it will probably cost less than if you did it yourself.

A comprehensive Word based software product that provides the required team plan templates and structure is all you'll need. This software will work extremely well within any small or medium size business. Finally, in selecting the software choose one with an extensive introduction and guide that clearly addresses continuity planning.

Estimated Cost: Plan development software, less than $1,500. Also, about 4 – 12 hours to develop each team plan.

Step 7 – Offsite Storage of Information & Data

If you want to recover your business following a disaster that destroys your facility, it is imperative that you have critical information stored offsite. This offsite storage of information must include both hard copy records and backups of your information systems. The information that needs storage should be identified during your impact assessment. Full volume backups of all of your systems should be performed at least weekly and rotated immediately offsite.

Note: If you have critical information, files, data, manuals, records, etc. that you use in your business and the only copy is at your work location, you are at risk. Furthermore, that risk becomes a disaster if your information is destroyed or becomes unavailable to you. If you do not have access to an offsite copy, or if you are unable to replicate it, it is gone forever.

Estimated Cost: Using a once a week pickup schedule and four storage containers, plan on about $200 to $400 monthly.

Step 8 – Recovery Location

The feasibility associated with the use of alternate work locations needs to be addressed prior to a disaster. There are three areas that need consideration:

1. Emergency Command Center: This is an alternate location that is generally removed from your normal work location. The primary purpose is to have a location where the management team and certain identified staff members can meet to coordinate and direct the recovery efforts. It should be stocked ahead of time with emergency supplies and phones.

2. Work Area Recovery: This is an alternate location that is generally removed from your normal work location. The primary purpose is to

have a location where various recovery teams can go to recover their work area and resume their normal business functions.

3. Hot, Cold, or Mobile Site: This is an alternate information systems recovery location that is generally removed from your normal work location. It is a facility that has, or is ready to receive, computer hardware.

Estimated Cost: Depends on the recovery locations you decide you need and the resources that you want readily available for use.

Step 9 – Plan Validation, Training, And Plan Maintenance

Testing – Any CP should be tested and/or exercised once it has been developed. The objective is to find any errors in the plan strategy, tasks that do not provide accurate detail, or omissions in the plan. If shortcomings are found, the CP can be corrected and updated before a real disaster occurs. Plan validation can be made in one of two ways:

1. Schedule and perform an actual test. This process is frequently utilized to validate the Information Systems Team Plan(s). To conduct a test: schedule it, locate resources, recall backups from offsite storage, and then restore and bring up the processor following the detailed tasks contained within the team plan.

2. Schedule and perform a tabletop exercise. This process is frequently utilized to validate the strategy and logic of the CP as a whole. To conduct an exercise, schedule a meeting with all team leaders, develop a realistic but imaginary scenario to play out, and moderate the exercise walking through the scenario and changing events as you go. As the moderator, you will need to call on various team leaders as the scenario is played out. Each team leader will need to utilize his/her plan to explain how their team will respond.

Training – Training is an important part of the overall continuity program. You are encouraged to have your staff take first aid and CPR courses. An occasional "awareness" flyer delivered to the employees can remind them of the importance of emergency preparedness.

Plan Maintenance – Keeping your CP up-to-date and accurate is imperative if you expect it to be a viable document at time of need. Changes will need to be made as changes take place in your business (new server, new team leader, change in a business process, etc.). Also, each team leader should make a semi-annual review of all team plans.

Estimated Cost: Testing – 24 hours
Exercise – 20 hours
Training – Varies according to target objectives
Plan Maintenance – 16 hours

Conclusion:

In closing, a continuity program is an achievable goal within any small to medium sized business. Each step that has been presented within this article is important, and each one takes your business closer to being prepared should a disaster occur. The process is truly straightforward and it all starts with your commitment to the process.

Sal Meloro is a business continuity professional with over 25 year's experience in the telecommunications, banking and disaster recovery field. He is currently DERA's Regional Coordinator for New York, New Jersey, Puerto Rico and the Virgin Islands and has led DERA professional development seminars, drills and exercises. Sal welcomes questions or comments by email to: smeloro@comcast.net.

"Who You Gonna Call? *(Cont'd from p. 2)*

switch. In some cases, dialing 9 is required to get an outside line. Were you to follow that initial 9 with a 11, you would not get connected at all.

You should check locally, when travelling to see what the emergency number is for the area where you are located. The local phone book or area residents can usually provide this information.

Tied directly to the question of "Who am I gonna call?" is the even more basic question of "Where am I located?" Today I am in a part of New York that proudly calls itself Hawthorne. In reality I am in an unincorporated hamlet that is better known by the city name Mount Pleasant. While the hamlet may be better known as the final resting place for Babe Ruth and James Cagney, it is not an identifier used by the National Weather Service.

If you are driving down the highway, do you ever listen to the radio for the weather? If you do, do you know where you are? What county are you in? Recently the National Weather Service started issuing warnings that include mile markers on the interstate. I was recently in severe weather and could hear the forecast and warnings, but had no idea where I was located.

As you move through your daily life, pay attention to your surroundings, know where you are and "who you gonna call."
.

Howard Pierpont
Board Chair - DERA

Professional Affiliation

Membership Application

Name: _____ Title: _____

Organization: _____

Street Address: _____

City: _____ State: _____ ZIP/Postal Code: _____

Country, if not USA or Canada: _____ Phone: _____

Email: _____ Radio Callsign: _____

Please Select Membership Classification

Enclose Check or Money Order for Dues Payment

Amounts are in U.S. Dollars

❑ **Individual Membership - Professional**
$50.00 per year
$35.00 for Student, Retired or Unemployed

❑ **Individual Membership - Management Level**
$75.00 per year

❑ **Lifetime Individual**
$475.00

❑ **Nonprofit Organization**
$75.00 per year

❑ **Governmental Office**
$95.00 per year

❑ **Small Business**
$125.00 per year
Please contact us for corporate membership

Foreign currency and drafts are credited at commercial exchange rates. All checks must be payable through a U.S. bank.
Add $5 per year if you wish newsletter sent by Airmail, or $35 for Global Priority Mail. Rates good for 2011.

Join online with any major charge card at www.disasters.org

or mail this application with check or money order to

DERA Membership
P.O. Box 797
Longmont, CO 80502-0797
USA

Please tell us if a member referred you so we can thank them: _____ NP-2011-04

DERA was founded in 1962 and is a Nonprofit U.S. IRS 501(c)(3) Tax Exempt Organization. FEIN 39-1777651.