

# Disaster Preparedness

## Scott St Louis NDTA Chapter 82 Disaster Preparedness Program Disaster Preparedness and Continuity of Operations Planning Document Recommendations and a Plan for Your Corporate Site March 2009

### PREAMBLE

(Or why should I read this?) Disasters always happen to the other guy/gal, right? If you truly believe this, read no further. Give this document to someone else and don't waste your time.

### BACKGROUND

(Everything needs a background!!) There is probably something in the human gene structure that causes most of us to completely believe in that first sentence of the Preamble. We always hope and think for the best. We think that with good effort and intentions and just dumb luck, all will be well. You have to really convince us that we should spend our available financial resources on insurance of various types rather than on a new set of golf clubs, a new pair of shoes, or a rare stamp for our collection. *Who needs insurance? Who teaches their kids about basic insurance needs? Who needs a plan for those times when things go bad?* If you read the newspaper or are just part of that condition called being a human being, there are plenty of signs out there we should be paying attention to. Car accidents happen (to the other guy AND to us). Folks lose their jobs (the other gal AND us). Natural disasters and floods and tornadoes happen (to the folks across the river AND to our side, too). Medical bills happen (to the other guy AND to us). Financial markets go up and down (for the other gal AND for us). For each of these situations, and for many more like them, there is this thing called insurance. If we're lucky or prudent, we are paying for some of it and it will help us through many disasters or emergencies.

### DISASTER AT YOUR WORK SITE

If you're still reading, that's good – maybe you don't think this is a waste of time. So, while we still have your attention, let's take this disaster planning to another level, namely, your corporate site and the people who work with and for you. This document assumes that there are many different environments that you may find yourself in. You're probably a tenant. You may be renting space from a management company that takes care of your basic facility needs. You may be in government facilities, on or off base. You may have personnel that work at your site, from home, while on the road. Many of your resources may come from your higher corporate headquarters. You may have to shovel your own snow, or someone might be contracted to do it for you; ditto with a leaky roof. You may have a backup power generator (by the way, when was the last time it was tested?). Are your computers and the documents you create backed up or saved on a recurring basis? This document assumes nothing about the physical conditions of your day to day existence, but it does assume that before bad things happen, you need to have a plan, either one of your own making or one that complements a plan that someone else will implement. While we're thinking about it, are you sure that the other guy/gal who you're relying on for some action really has a plan and is ready to implement it? That might be a good first step. What follows is a list of your "average" group of disasters – admit it, things that CAN happen to you. The list is certainly not all inclusive. If they are food for thought for you on an individual or family level, then let's declare success. We've got you

this far; go for it; think about it! Expand your thinking to include your work environment, your site, your people, your family, and your customers.

Have you thought about how you would react to the following?

- Power failure in the neighborhood or your building, any time of year.
- Huge snowstorm, forecasted or not.
- A tornado strikes your building, or down the street, or in neighborhoods where your employees live.
- You're told to evacuate your home or building because a train carrying chemicals derailed a half mile away and a vapor cloud is headed in your direction.
- Local or area wide flood in your home or your place of business.
- You encounter a cyber attack, significant spamming, viruses, or other denials of computer service. This can include all types of computer networks and related issues.
- The flu season really hits your workforce and their families, and significant numbers of personnel call in sick for several days.
- The office in the wing next door or on another floor has a fire and while you have no fire damage, your facilities do receive significant smoke damage and some water damage. It will be three business days until a restoration company can get to your facility, and another three days to make everything right. The safety feature shorts out, and the fire suppression system (all those sprayer things in the ceiling) activates for 3 minutes; it puts out the "almost" fire and literally puts you out of business for a whole lot longer.

### **GENERAL PURPOSE OF THIS DOCUMENT**

DISCLAIMER #1 - there are no solutions in what follows nor will we guarantee that we have thought of everything. Our job is to get those creative juices going, to figure out what applies to your site and what doesn't, and to add those things we have (probably) missed. *The answer to Disclaimer #1 - No plan is perfect, but some plan is better than no plan.*

DISCLAIMER #2 – there is probably nothing too original in this document. You can get a book from the library or go to a website and find some or all of the ideas that are listed below. We freely admit that we are stealing from everyone else who has ever had a good idea on this subject. *The answer to Disclaimer #2 - Any plan needs to be implemented, or else it isn't really a plan. Good intentions in a shelf ware document will not help anyone, at any time, in most situations.*

DISCLAIMER #3 – if we stole these good ideas from others, we will not complain if you share them with everyone you know. Said another way, you can even implement them, free of charge. No royalties are involved. Hopefully, no copyright infringement lawyers will visit us. *The answer to Disclaimer #3 - Disasters are for everyone....(wait, that didn't come out right!)*

### **FACETS OF A PLAN**

OK, here we go. Remember, this is the fire hose treatment; hopefully you will have more than enough to think about. But also remember, "The devil is in the details of the doing."

1. Disaster Plan - do you have one? **This is probably Good Idea Number 1.** Was it developed with input from your employees (for their good ideas and consideration of their local experiences, constraints, and possibilities)? If your higher headquarters has a plan, do you know what it is? Did they ask for your inputs or ideas?

2. Designation of Authority - who has the authority to declare that emergency procedures are to be implemented? Seems pretty obvious, but **this is probably Good Idea Number 2**. When the Fire Chief or someone official looking makes an announcement, we are normally inclined to act. But in the shady areas, we normally look for an established decision maker. If the boss is not available and cannot be reached on the cell phone, where and to whom to we look next (who is next in line)? Remember: decisions like these could have HR, financial, legal, and other ramifications. We don't necessarily want employees making decisions unilaterally, and we do need to have someone in authority making important decisions.
3. Dissemination Procedures – get the plan(s) into the hands of your personnel, by whatever methods is most feasible/acceptable. **This is probably Good Idea Number 3**. Personnel need to know their role in minimizing damage, their roles in the recovering of operations (where feasible), where to go, what to do, and who to talk to. You can put information in a file, distribute hard copies, post notices on bulletin boards, brief items at staff meetings, or use other methods. And remember, this needs to be a continuous education process; just a simple turnover in key personnel will require some retraining or re-familiarization.
4. Continuity of Operations Plan (COOP) - do you have one? Depending on your specific use of that acronym, a COOP can be either of the two items below. Regardless of what you call it, you need to be thinking about both of these.
  - A general plan (with checklists that outline authority and responsibility) that covers all aspects of your operations, to include personnel items, stopgap measures and procedures, reconstitution and recovery actions, and checklists covering a wide range of things to do and/or think about.
  - A document associated with the restoration of software and hardware and your ability to maintain a state of readiness commensurate with mission requirements. Your site assets may need to dovetail with corporate resources and capabilities, government assets, or both.
  - What assets and resources are you starting with (currently in-place or readily available)? What are the items and what is your supply level? Think about disposable items that might be required to maintain a minimal level of operation (paper, batteries, cartridges, etc.).
5. What expertise or talents do your employees have (can be gained either through your company or as part of individual classes or training)? Would you expect that particular employee to be available on a particular day? What are the legal and safety considerations? Have you talked to your people beforehand? For example, people with basic medical skills (CPR, basic first aid, etc.) can be encouraged to identify themselves and step forward when required.
6. What sequence or priority system will you use to accomplish specific tasks or items? Assume there are more things to do than there are people to do them. What are timeframes and levels of importance associated with each item? Have you sat down in a quiet moment – BEFORE the disaster – and made those priority assessments? This whole thing should be part of a Disaster Plan (item a. above) that is polished and ready to be implemented.
7. Are there corporate, community, or locally prescribed safety or operational procedures or laws that should be followed?
8. Have you instructed your employees on what they're supposed to do? Are all facets of your plan discussed, exercised, or practiced every now and then (like once a month or once a quarter)? As with periodic fire drills, we can see that actually leaving the building and gathering at a designated place is a key method of reinforcing a desired behavior.
9. Computer operations, to include personnel, hardware, and software. This is huge area, so we will only provide a quick list of things to think about:

- Is there a general operational plan or diagram that describes your networks, hardware, and software? It should include demarcation points and who to contact on the other side of each point to aid in recovery operations.
  - What are backup procedures for important documents, files, and daily operations?
  - Is there any provision for storage or other capabilities at off-site locations?
  - How are employees, customers, and levels of management notified of problems, mitigation efforts/schedules, and progress toward getting up and operational?
  - What level of manual operation should be implemented if it is hours before you are operational again? If it is days before you are operational again?
  - What level of efficiency can be attained by those who work off site or at home? Would benefits increase if all employees were given these options? Is a single alternate location available for all employees/operations?
  - Are there written procedures or service level agreements for document backups or COOP support services. A test schedule or concept for any/all of the items above. Some guidelines might include a Paper Test (review of the document or procedure, conducted annually), a Tabletop Test (more extensive review by key management personnel and other service providers, to include a discussion of the plan and various contingency scenarios), and a Live Test (full involvement of some aspect of your plan, with full participation of all personnel identified with the effort (this could be as simple as a fire evacuation drill, the exercise of a recall roster with a piece of “artificial data” that must be passed to all personnel, or a simulated power interruption or cutover to test some aspect of a computer recovery or operations plan).
10. Do you have any letters of agreement, contingency plans, or contracts with companies that specialize in disaster response and recovery actions? If not, what other agencies could you call on for support? Options here include the management company you’re paying rent to, your corporate headquarters (alternate sources of manpower, computer support, alternate funded positions or contracts (move your personnel to temporary paid positions)), or your customer if you reside in their facilities.
  11. Are you able to relocate for selected periods of time? This can range from temporary facilities, moving in with another branch of your company or your customer at a different geographic location, to allowing personnel to work from home. Obviously, you will need to consider the nature of the services you provide and match that with any relocation option. Lots to think about here - you’ll need to consider all those agencies who need to know what is going on. It is similar to all those Change of Address cards you need to fill out when you move, and things like mail, bills, electronic change of addresses, existing payment accounts, and other things that drive or impact your business on a daily basis. Computer systems and other major support functions may need to be restarted, in an orderly fashion, after much coordination.
  12. Provide on-going status reports to keep your headquarters, management, customers, and service providers informed. This should include current operational status, projections for increases in your rates of efficiency and effectiveness, and get-well dates.
  13. Plan for a restart and a get well date. A reconstitution team may need to be established to plan for a return to your primary site. This would include planning, dates, changes to capabilities, etc.

### **RISK AND MITIGATION ANALYSIS**

(All is not gloom and doom) So, it looks like there is a lot to think about. But in reality, unless you live under a cloud of bad weather that you often see with a favorite comic strip character, a lot of this stuff will probably never happen to you. But it might be smart to look at a few situations, see what “the experts” think, and then make your own risk determination based on

factors applicable to you. The mitigation section provides some generic answers to each risk, and the last bullet provides room to insert your own approaches.

**Risk #1: Disruption of local power source.**

- **Analysis:** The probability is low, based upon historical data of outages and countermeasures employed.
- **Mitigation:** Alternate facility location has been identified for each customer site and service provider.
- **Additional mitigation options available to me:**
  - Lease, rent, or purchase small UPS for computers and other vital equipment.
  - Lease, rent, or purchase large UPS for the building.
- Risk at my location is.....

**Risk #2: Disruption or discontinuance of service due to water damage, fire, or other natural disaster**

- **Analysis:** The probability is low based upon historical data of natural disaster damage.
- **Mitigation:** Alternate facility location has been identified for each customer site and service provider.
- **Additional mitigation options available to me:**
  - For owned facilities, have a contract with building restoration company for water/smoke damage and minor carpentry repairs.
  - Amend building lease to include use of other available space controlled by the owner during building repairs.
- Risk at my location is.....

**Risk #3: Natural disaster damage over a wide area, e.g., tornado, earthquake, etc., that could force your operation to relocate to an alternate geographic location. This may create operational backlogs.**

- **Analysis:** The probability for a disaster is medium (given this geographical area). Risk to relocation actions is also medium, due to dispersed locations, identification of backup sites, and the probability that a lot of companies will be trying to accomplish the same thing.
- **Mitigation:** Alternate facility location has been identified for each customer site and service provider.
- **Additional mitigation options available to me:**
  - Implement COOP according to severity of disaster.
- Risk at my location is.....

**Risk #4: Disruption of communication services through internal and external tampering.**

- **Analysis:** This has a medium probability of occurring. Information can be obtained by intercepting non-encrypted data communication.
- **Mitigation:** Data can be encrypted prior to communication transmission. But you need to stay current with firewalls, security processes, and other protection devices that stay abreast of the latest dangers.
- **Additional mitigation options available to me:**
  - Manually isolate internal LAN from external connections for an external intrusion. Restore when tampering is identified and defeated.
  - Manually isolate internal servers until tampering is identified and defeated.
- Risk at my location is.....

**Risk #5: Unauthorized persons gaining facility access for sabotage or to vandalize equipment.**

- **Analysis:** This has a low probability of occurring. Unauthorized access to the facility may result in damaged or stolen equipment.
- **Mitigation:** Ensure entry access to facility is controlled. Ensure personnel are trained to report badge violations, un-escorted personnel, or other infractions of policy.
- **Additional mitigation options available to me:**
  - Install alarm and monitoring system that report after-hours infractions to local law enforcement, and in turn, to you.
  - Shoot to kill (OK, OK, only kidding!! Just wanted to see if you were paying attention).
- Risk at my location is.....

**Risk #6: Unauthorized persons gaining access to servers, LANs, and workstations for sabotage or for obtaining, altering, or destroying information.**

- **Analysis:** This has a medium probability of occurring. Unauthorized access could cause damage to the effectiveness of the accounting support operation.
- **Mitigation:** Continue to review system security and ensure security countermeasures are in place and effectively operating.
- **Additional mitigation options available to me:**
  - Lockdown equipment, as appropriate, until extent of intrusion and damage can be ascertained.
- Risk at my location is.....

**Risk #7: Disgruntled employee sabotaging the system network.**

- **Analysis:** This has a low probability of occurring. This could lead to disruption or destruction of data files.
- **Mitigation:** Limit access for those employees experiencing adverse personnel actions.
- **Additional mitigation options available to me:**
  - Proper out-processing procedures when employees are terminated.
  - Isolation of subject employee through control or surrender of keys, cards, and badges
  - Have IT shop ensure denial of access by removal of permissions.
- Risk at my location is.....

**Risk #8: Your facility is directed to shut down due to a contamination event nearby.**

- **Analysis:** This has a medium probability of occurring and probably presents the widest range of issues to deal with; timeframe can run from hours to days, depending on the situation. A wide range of options must be considered.
- **Mitigation:** Well conceived plans for all functional and operational operations, supported by identification of key players and actions, supporting checklists, and coordination with corporate officials and your user.
- **Additional mitigation options available to me:**
  - Employees can work from home.
- Risk at my location is.....

**EMPLOYEE CONSIDERATIONS** (Navigation of personal issues for your most important assets!)

Remember, in times of disaster, it is not business as usual for anyone! While you may be tempted to think about your roles in helping the business and your customers, focus must also

be on helping employees navigate personal issues, from family needs to home disruption. This type of employee support will come back to the company in the form of loyalty.

The most critical aspect of emergency planning is getting employees to think ahead. To protect your employees through a disaster, take these key steps:

1. **Start with an acceptance of a disturbing fact – while you might not like it admit it, disasters can, and do, happen to anyone, anywhere, at any time.**

Accepting this idea and laying out some simple, basic plans will go a long way to minimizing the consequences to your operations and your personnel. While some disasters might overwhelm even the best of plans and intentions, a coordinated thought process that considers assets and supplies, provides contingency directions, and controls operations as they scale up and down is a huge first step. Encourage a practical thought process that applies to individuals and families. There are multiple plans and agencies that start at the individual level and work their way upward.

2. **Build Solid Contact Lists:** Keep contact information for the following updated and easily accessible.
  - **Employees.** Maintain complete information for communicating with employees and their extended family. Include home/cell phone numbers and email addresses for next of kin and spouses/relatives; do not forget to make use of text-messaging capabilities and other communications devices as they may be the only way to stay in touch.
  - **Emergency phone numbers.** Include local fire and police departments, hospitals and ambulance services, building security, utility companies, as well as government disaster-relief agencies. The management company that controls/operates your facility should certainly be on this list; understand where their responsibilities begin and end (what they will or will not do for you).
  - **Key vendors and suppliers.** Maintain a list of vendors and suppliers that can be relied upon to respond quickly. For regional disasters, it may be necessary to reach out for assistance to a supplier with facilities located outside of your primary business area.

3. **Establish Emergency Communications Procedures**

Establish a clear process for communications and plan how you will contact one another in different scenarios. Meet with your employees periodically to review and update emergency plans.

4. **Organize Supplies**

There are many things you could consider, and some may not be applicable or practical. However, think through the following: make sure your company and its satellite sites have access to funds (cash or another form of payment for immediate purchases), generators, flashlights, batteries and supplies, camping equipment, first aid kits, ice and water, personal care supplies, food, and the ability to charge cell phones, laptops and other communication devices.

5. **Provide Employee Assistance**

Encourage your employees to become more aware and self-sufficient. Recommend and support training your personnel or staff member in CPR and first aid. Encourage an

active family plan that includes the ability to make the best of a bad situation. There are many concepts about what you need and how to prepare, and there are many websites that will develop the concept of a family disaster kits (more on those sites later in this document). In addition to the items mentioned immediately above (Organize Supplies), some additional items for a site might include the following:

- First aid kit
- Bottled water
- Battery powered radio
- Plastic containers to seal critical information
- Disposable camera
- Post-event cleaning supplies

## 6. **Know How to Store Data**

Find the right data storage solution for your business based on the importance and quantity of data you need to protect, the timeframe for restoration and, of course, your budget. Here are two options:

- Copy data to removable media, including DVD-R or CD-R discs, tapes, or to removable disk drives that connect to systems via their USB ports. For more than 50 percent of the small businesses that responded to an Office Depots survey, this is the preferred data storage solution.
- For larger volumes of data that require quick restoration, look for specialized software for continuous data copy, or use an e-vaulting company to which you can send your data electronically for secure back-up and storage.

## 7. **Back-Up Data On a Regular Schedule**

To protect your business from faltering after a disaster, you will want to:

- Back-up your key data at least every week. If you don't have a tape back-up system, make copies of your most important data on CDs, portable disk drives that quickly connect to your computer's USB port, or even to a laptop.
- Take a copy of your software used to make back-ups to a secure off-site location. Follow these guidelines:
  - Don't leave your back-ups sitting next to your systems. If a disaster hits, you don't want to lose both your data and the back-up.
  - Move back-up media to a secured, alternate or off-site location.
  - Establish a routine back-up system to ensure the most current data is retained.
  - Make sure to mark the media with content and dates.
- Store copies of key forms and hard copy documents you use day-to-day at a safe location to help keep your business functioning.
  - A simple consultation with your operations people will guide you to critical application software and documents you should protect.
  - Scan critical documents (e.g., insurance) for electronic storage.
  - Include photos of major building and manufacturing sites, protected in watertight storage containers and stored in a fireproof safe, in case you need to present these materials to your insurers.
  - Periodically review the data being stored to ensure that the right data is being copied and that it can be restored.

**LIST OF REFERENCES AND WEB SITES**

This planning (and thought-provoking) document will only take you so far, but we're going to get you as far along as we can. So, this last section will provide ready links to reputable agencies that do this "disaster planning thing" for real. There are not too many sites that routinely talk about corporate-level actions, but with some corporate level thinking, you can use these sites as a springboard to a corporate plan. Refer to these sites for more information, programs, and local events.

Local Red Cross offices (local area programs and opportunities) -- <http://www.redcrossstl.com>

US Department of Homeland Security (excellent corporate information) --  
<http://www.ready.gov>

Illinois Emergency Management (threat warning and local/state information) --  
<http://www.DisasterCenter.com>

**CONCLUSION**

Ok, the rest is up to you.