Global Information Assurance Certification Paper

Preparing Your Network for Disaster
By Brian McGauran

Prior to September 11, 2001, the word disaster was a vague concept to most people in the IT field often conjuring up images of the Titanic or hurricanes along the Gulf Coast. Hopefully after that date, many IT professionals took a second look at (or in the case of my organization began) their organizations disaster recovery plan. The attacks reminded security experts, network administrators and business leaders, that all organizations and their systems are vulnerable not only from brought on by nature but from man.

An organization that does not have a disaster recovery plan is an organization with a death wish. Within hours after the terrorist attack on the World Trade Center, the head of information security for my organization received a call asking him if there was a disaster recovery plan, unfortunately the answer was "no". The reason that the head of Information Security received the call is that due to of the nature of our work, we are expected to be the most familiar with the enterprise. If there was any good to come out of the events of that day, many organizations began to launch recovery initiatives.

For some organizations, the road to recovery began years ago. In a story in eWeek, Stan Gibson cited the case of the New York Board of Trade (NYBOT) whose offices were located at the World Trade Center. They began their recovery initiative eight years ago in the wake of the 1993 World Trade Center bombing. Less than a week after the attack the NYBOT, the worlds fourth largest commodities trading exchange, was up and running almost at full capacity in a Comdisco, INC disaster recovery site. Although they suffered a loss of their offices in the WTC, they were able to quickly get back on their feet by having a thorough recovery plan that included a backup facility with mirrored data.

According to the American Heritage dictionary of the English language: "a Disaster is a catastrophe. b. A grave misfortune. Disasters occur with sudden and unexpected consequences

for those unprepared. Although it is almost impossible to plan (or conceive) for a disaster such that occurred on 9/11, it is important to note that any disaster, be it brought on by nature or man can cripple an organization that does not plan for the unthinkable or the inevitable. The adverse effects of a disaster increase exponentially for those who are not prepared. It may not be possible to recover all of your organizations assets, but with a plan you may be able to mitigate the severity of the damage done to your organization.

Disasters come in many forms to include:

- Natural disasters
- Hackers bringing down the system
- Terrorism
- Power failures
- Labor actions.

The primary parts of a disaster initiative

There are three primary components found in almost all disaster initiatives:

- Create a disaster/incident response/recovery plan.
- Conduct a vulnerability assessment.
- Create a disaster response/recovery team.

The above bullets represent the three primary elements of a disaster recovery initiative. Note they are not numbered or listed in chronological order or steps. In your recovery initiative, these parts will probably occur simultaneously. It is hard to create a disaster recovery plan without a team and a good plan must include a vulnerability assessment. It is usually best for a small task force with senior management support to conduct the initial vulnerability assessment and create the disaster recovery plan. This team should include key representatives of all department and other stakeholders.

Creating a Disaster Recovery Plan

The first step we will cover in the creation of a disaster recovery initiative is the creation of disaster recovery plan. Writing a disaster recovery is not for the faint of heart. Computing and Networking Services white paper on Disaster recovery Planning states "Disaster recovery planning is not a two-month project, neither is it a project that once completed, you can forget about. An effective recovery plan is a live recovery plan". One source stated that one such plan took two years to write. A disaster recover plan spells out the process for resuming normal operations and should be a guide for all employees during and after the disaster. A good plan should the enable an organization to "see through the fog of chaos" that results from a disaster. It is important that your plan be:

- Concise and easy to understand.
- Have realistic rules and recommendations tailored to meet your organization needs.
- Dynamic.
- The primary objective being to allow the organization to survive and reestablish normal operations.

For those of you who have experience with writing or enforcing a Computer usage plan, you know that the plan must be concise and easy to understand. If your plan is long-winded or too technical, people will not read it at "crunch time". A good rule of thumb is that your plan should be easy to follow by a person outside the organization supporting the recovery operation. Your plan should be a clear and concise statement of appropriate responses for quick and cost effective recovery

The recommendations in the plan should be realistic, practical, and tailored to meet the needs of your organization. I worked for a company where a recently retired Army Colonel with no prior IT experience drew up the plan. According to his plan, at the first warning of a hurricane, the Network Operations Center would telephone all technicians and they would report to the

computer center within 4 hours. However, the local Emergency Management Agency noted that the headquarters of the company (which was located at the intersection of two rivers) would likely be under 14 feet of water in the event of even a modest tropical storm. It is one thing to have the Ranger Regiment on standby in the event of war; it is another matter to require your employees to risk their lives swimming to work to save the latest backup of e-mail. It is obvious that those who originally placed the headquarters in that location weren't taking into account natural disasters. The bottom line here is if your plan is not practical, people will ignore it when it comes time to use it.

As stated above, an effective disaster recovery plan is "live." It should never be considered a fixed, finished product. Your recovery plan should not be allowed to sit on a shelf to be dusted off in the event of an emergency. When writing your plan, you should approach it as a first draft. It is important to get a plan on paper and then worry about making it perfect. Remember, it takes many generations to achieve "Best Practices." The plan must be written down, short (15 to 20 pages), updated regularly and key personnel should keep a copy off-site in their home.

Conducting a Vulnerability Assessment

It is almost impossible to recover from a disaster without knowing what is installed and what must be recovered. This is accomplished by conducting a thorough vulnerability assessment. Remember, the purpose of you recovery initiative is to get your organization back to (some degree of) normal operations. The purpose of your vulnerability assessment is to identify mission critical hardware, software, other critical equipment along with people and their jobs. After making this initial assessment, you must assess what is critical and then quantify the cost and the time it will take to recover. The recovery of non-essential and/or out dated equipment and data is a waste of time and money. Costs must include more than actual monetary value, it must include the cost of life, bodily injuries, privacy, data and public image. It is also important to note that disasters are not limited to hardware and software. Your vulnerability assessment must also

include human resources and account for the loss of essential employees and the smooth transition of their job responsibilities.

One of the most important components of your vulnerability assessment is an equipment inventory. Leo Woebel in his book Business Resumption Planning, Artech House Publications, 1997; suggested that at a minimum your inventory should include the following:

- A listing of all equipment by type and manufacturer
- Associated software packages and their version number
- Date of purchase and original cost

In addition to those items, your inventory should include:

- A listing of all voice and data lines
- Emergency phone numbers
- A list of all cellular phones
- Contracts and maintenance agreements
- Insurance policies
- Client lists and their phone numbers
- Network schematic diagrams

Unfortunately, while most organizations have these records, they are usually not updated and kept off-site. Your vulnerability assessment, like the disaster recovery plan must be updated on a regular basis.

In addition, your vulnerability assessment must attempt to identify risks to your organization and plan how your organization can recover from each of these risks. During this assessment, it is important that your recovery team brainstorm as many scenarios as possible. It is important that the team encourage all employees to participate in the process of identifying these risks. In the wake of the WTC disaster, no risk can be really considered outlandish. It may also be necessary

to obtain information from outside specialist for advice on risks outside of your organizations normal area of expertise. It is important to remember that the time to discover vulnerabilities is before the disaster, not after. Your assessment should enable you to target your resources toward the most important risks. Your assessment should be systematic. You cannot out-guess a disaster. Instead look at the common elements of any disaster and plan accordingly. The following are three common elements that you should focus on when attempting to recover from a disaster.

- Loss of information
- Loss of access to information and facilities
- Loss of personnel

After identifying the risks to your organization, you must evaluate the risk and determine how much damage it will present to your organization. The disaster recovery team with guidance from management must decide how long they are willing to operate without being able to perform each of their daily operations. There are generally 3 time periods following a disaster:

- The immediate period characterized by chaos and disorganization with limited operations.
- A period of makeshift operations where the organization has brought up or is in the process of bringing up critical operations.
- The third period is a period in which somewhat normal operations have resumed. This is a period of time that the organization can go back and review what "lessons learned".

The Disaster Recovery Team

One of the most important aspects of any disaster recovery initiative is the disaster recovery team. Everyone in your organization should be considered a member of your disaster

recover imitative, however each organization should have a team responsible for organizing and leading the recovery. I have broken down the life of the team into two phases:

- The initial Pre-Planning Team
- The Permanent Disaster Recovery Team

The Pre-Planning Team should consist of a small task force empowered by senior management to conduct the initial vulnerability assessment and create the initial recovery plan. It can't be overstated that any disaster recovery initiative must have the blessing of senior management. Organizations that have tried to develop disaster recovery initiatives without the support of management, often fail because the organization will not dedicate the necessary funds and other resources. The pre-planning team will assemble the Permanent Disaster Recovery Team consisting of key personnel, suppliers and others needed in the event of a crisis. The suggested makeup of this ad hoc team should include key members of:

- A representative of senior management
- Information Security
- Facility management
- Legal Staff

The overall purpose of this team is to begin the process. As stated above this team is formed to conduct the initial vulnerability assessment, create the initial disaster recovery plan, assemble the permanent disaster recovery team and attain authority from management for the plan and the permanent team. There is no time limit on how long this team will be together before it hands over the reigns to the permanent team. They are in existence until they feel their job is done.

As stated earlier, your disaster team must include at least one representative of senior management. It is management after all that must provide the necessary funds and resources for the recovery process. They must also empower the permanent team to speak for and act for management in their absence. This will help ensure quick, decisive actions being taken in a crisis.

The “buying in “ by management also ensures that the organizations other employees follow the teams directives. This will put the organizations imprimatur on the disaster recovery plan instead of it being viewed as an unenforceable suggestion.

I also selected personnel from the Information Security team to be involved on the pre-planning team (and the permanent team) because they are usually the most knowledgeable people in any systems environment. Information Security specialist are usually involved in all phases of the enterprise. They are aware of the slightest changes to the network. These are the people that are tasked to protect and defend the enterprise on daily basis.

Your facilities management should deal with the nuts and bolts of construction and electrical codes. They know how to “turn on the lights” and “get the water turned off”. They will also be helpful in locating appropriate off-site or temporary work sites before and after a disaster.

I also included the legal staff on this team. I know most people would rather invite a snake into their home, but attorneys do come in handy form time to time. It is important to have attorneys review proposed policies to ensure applicable laws and regulations are properly addressed. Also, in the event of a disaster, you may not be able to deliver your products or services. Regardless of your organizations problems, due to contractual obligations, your customers may require you to take the unexpected into consideration and to deliver them the components that are needed to keep their organization from shutting down.

The Permanent recovery Team is a “different animal” altogether. After the initial assessment and policy is completed, it must be forwarded to the permanent team. The permanent team is much larger. It should consist of key members of all business units and all areas of the enterprise. After receiving the overall plan, they must return to their areas of expertise and share the plan with all members of the organization. It is also important for all team members to appoint a second in command in case this person is injured or otherwise absent. Copies of the plan should be kept not only at the workplace but also at home. Each person must be assigned a specific task with a backup person sharing the responsibilities. Each person must be trained to carry out there

are of responsibility. It is important that mock drills be held from time to time unannounced to test feasibility of the different tasks in the plan. It is important to know in advance if even rudimentary parts of the plan as tape backups work. The plan must be updated regularly and other members of the team must be notified of the changes to the plan. When team members leave the organization, it imperative that new members be installed to take their place as soon as possible.

Here are some suggested areas for the permanent team staffing:

- Information Security
- Facilities management
- Human resources
- Payroll
- Legal
- Public relations
- Telecommunications
- Database operations
- Programming

It is important to have a Team leader and co-lead to lead the team in regular meetings and be involved in the regular administration and direction of the group. Remember, the team will be responsible for seeing to it that the actual parts of the recovery such as cleanup, replacement of computer equipment, furniture, insurance, real estate and so on are taken care of.

In conclusion, every organization should have a disaster recovery initiative. Not having a plan in place is foolhardy at best and wreck less at worst. If your organization does not have such an initiative, it is never too early to begin. Remember, disasters often occur without warning and may destroy your organization. At a minimum, your disaster initiative should:

- Create a disaster recover plan
- Identify what a disaster is to your organization and prioritize these risks

- Determine your organizations short-term, intermediate and extended recovery needs and resources
- Document the plan
- Take a complete inventory
- Assign a disaster recover team
- Train employees on their tasks in the event of a disaster
- Review the plan on a regular basis

References:

Web Sites

http://www.disasterplan.com/yellowpages/

http://www.solinet.net/presvtn/leaf/displan.htm

http://www.colostate.edu/floodrecovery/tips-from-a-disaster-expert.html

http://www.fema.gov/pte/prep.htm

http://www.fema.gov/library/terrorf.htm

http://www.disasterrelief.org/Library/Prepare/

http://www.intracomp.com/contents.html

Articles

"Disaster Planning: A Stitch in Time" by Neil Dunlop, *Canadian Underwriter*, January 1997

"For Want of a Nail.." by Matthew Vartabedian, *Call Center Solutions*, February 1999

"Networks at Risk: Assessing Vulnerabilities by Dana Coffield, *InteractiveWeek,* September 2001

"Getting the Job Done" by Stan Gibson, *eWeek,* September 2001

"How to Design a Useful Incident Response Policy" by Timothy Wright, *SecurityFocus,* September, 2001

Also

University of Toronto CNS

University of Tulsa

Books

Bates, Regis J., Jr. *Disaster Recovery Planning : Networks, Telecommunications, and Data Communications***.** New York : McGraw-Hill, 1992.

Fortson, Judith. *Disaster Planning and Recovery*. New York: Neal-Schuman, 1992

Morris, John. *The Library Disaster Preparedness Handbook*. Chicago: American Library Association, 1986.

Toigo, Jon W *Disaster Recovery Planning, Strategies for Protecting Critical Information Assets* New York: Prentis Hall, 1999

Woebel, John. *Business Resumption Planning,* Artech House Publications.1997

.

Last Updated: May 23rd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event