Global Information Assurance Certification Paper

Understanding Contingency Planning

By Jeffry C. Boutet, Jr.

Background

Having a contingency plan, whether a well-written Contingency Plan or a stand-by ticket to the Cayman Islands, is essential for any team responsible for the uptime of an information system. Having a good plan in an emergency situation can make that team heroes; not having one can destroy not only the careers of the team, but the business unit as well.

One of the main reasons for having a Contingency Plan is self-preservation of the organization. With the large complex computer infrastructures of today's information systems, it is simply a matter of time before they will experience some kind of disruption event. Whether it is a disruption due to natural, technological, or human causes, pulling out a management-approved plan that outlines actions to be taken makes managing the event easier. As a result, many organizations focus time and effort on trying to predict when these types of events will occur and how to manage them, thus generating a Contingency Plan.

Due to the combination of the organization's uniqueness, its structure, and today's rapid technological advances, the Contingency Plan that is created will be an original work. A team of employees that maintain key technologies and resources for an organization should be responsible for the creation and maintenance of the Contingency Plan. No consultant or expert can come in and effectively generate a plan for an organization. As a result, an explanation of the generic methodology and the commonalities that exist between most plans is necessary.

Introduction

- A hurricane blasts through the East Coast causing billions in damages.
- A fire at a food processing plant results in 25 deaths, a company out of business and a small town devastated. (FEMA)
- A bombing in the Federal Building in Oklahoma results in 169 deaths, hundreds of injuries and the evacuation and shut down of an 8-block radius (Arnold 1997).
- A flood shuts down much of Chicago for days. Lives were lost, businesses declared disasters and closed their doors and millions of dollars in damages incurred.

There are on average 33 major disaster declarations from FEMA (Federal Emergency Management Association) each year with the last four years well above the average (1996-75,1997-44,1998-65,1999-66). There were over 400,000 non-residential fires within the last four years with about 400 deaths (USFA 1999). Although statistically most organizations may seem safe from these types of disasters, there is one type of disaster

that has most likely affected every organization in some way. This disaster is the intentional technological disaster, more commonly referred to as "being cracked" or "being infected."

These events have a detrimental effect on business and industry, both in lives and dollars. Forty percent of small businesses that experience a disastrous event never open again. Business and industry can take preventative action to limit injuries and damages from technological disasters and return to normal operations in less time, by planning ahead and generating a Contingency Plan (EMG FEMA)

.

What is Contingency Planning?

The three hierarchical functions to Contingency Planning are Business Continuity Planning, Disaster Recovery Planning, and Emergency Management Planning. The break-down of these functions is based on the role they play within Contingency Planning. Although most organizations address all three functions in one plan or document, it is important to recognize that each serves a different function. In order for a Contingency Plan to be complete, all three functions must be addressed.

"Business Continuity Planning is a function of the entire organization" (TekCentral 1999). In the event of a complete disaster, this function provides for the survival of the organization by outlining the thought process and overall goals of the entire organization's Contingency Plan. It is used to help identify critical large-scale or corporate-wide vulnerabilities and to help determine how to mitigate and resume business operations.

While the Business Continuity Planning function serves to define actions and goals in a broad setting, the Disaster Recovery Planning function defines the actions and goals of each business unit or department. By having each business unit or department focus on its specific needs in preparation for and during a disaster, the recovery process can be achieved more efficiently. For example, the IT department will need servers and tape drives rather than the keys, security logs, and access cards and other supplies needed by the Facilities and Security department, all of which is critical to the return of normal business operation. It is the responsibility of each department to define the critical materials necessary to continue operation, and the responsibility of management to ensure that all of the departments' needs and concerns have been addressed.

Emergency Management Planning is the function of preparing for, mitigating, responding to and recovering from an emergency. In other words, this is the action plan. To accomplish the goals of the Business Continuity and Disaster Recovery Plan, a process must be built upon the internal level of emergency management capabilities within the organization, and address all types of disasters, phases of management, and necessary participants (the who, what, where, and how of the plan). The Federal Emergency Management Agency (FEMA) institutionalized this approach in 1979.

Considerations of What to Include in a Contingency Plan

Starting a plan can be difficult, but it is helpful to keep the following things in mind (this is just a list to start the thought process; other items can be added):

- Purpose of the Plan
    - States the purpose of having a Contingency Plan and how it fits into the normal operations of the organization.
- Priority of Life Statement
    - Includes a Priority of Life statement. Safety and well-being of the employees are the most important aspects of the organization.
- The Hazard or Disaster Identification
    - Provides for identification of the potential hazards that could affect the organization. If an office is located in the Sahara Desert, then planning for flooding isn't as a critical as contamination of the water supply.
- Business Impact Analysis
    - Outlines the potential financial, data, and communication losses that will occur if the network is down for 24 hours, 48 hours, and 72 hours. This shows management the "bottom-line" impact of these losses and how planning can reduce these costs. Indirect costs should not be ignored.
    - "There are risks and costs to a program of action — but they are far less than the long range cost of comfortable inaction" John F Kennedy.
- Prevention Strategies
    - Outlines the policies and procedures to be followed to prevent normal events from jeopardizing the ability of the organization to perform its mission.
- Critical Applications and Structure of the Network
    - Provides information on the why, what, and where of the organization's network. The areas addressed will be why is the network important, what are the main purposes of the network, and how is the network physically structured.
    - Identifies all applications that are critical for the organization to perform its mission, as well as applications that are critical for data recovery.
- Responsibility, Notification, Authority, And Approval Of Funds
    - Provides detail information on the who of the plan. Answers questions such as: Who is responsible for the action that need to occur; who is going to notify everyone in the organization; and who has the authority to declare a disaster or disperse funds for emergency operation.
- Action Plan
    - Outlines the policies and procedures to be followed in case an event occurs which jeopardizes the ability of the organization to perform its mission.
- Testing
    - Outlines the testing of the plan, the policies and procedures to be followed, the purpose and scope of the testing, and the frequency of the tests to be conducted.
- Plan Maintenance
    - Addresses how revisions, updates, and maintenance of the plan occur. Once developed, the plan should be a living, breathing entity, which is

under constant review and updates. If the maintenance falls short, the plan will be ineffective and obsolete.

- Training
  - Includes policies and procedures for training your organizations employees, managers, vendors, and emergency response personnel. The frequency of training and retraining, the degree of information needed, and the methodology used will all be covered.
- Appendices
  - Includes appendices that should be indexed and cross-referenced, with the use of graphics and flow charts encouraged when possible. All lists should be updated with current information on a regular schedule. This would include the inventory of people,

Conclusion

Although writing a Contingency Plan seems like a monumental task, remember it is a team effort. Management and employees all need to be involved. Start the plan small. Create a general plan that could be adapted to almost any hazard and then adapt it to the hazards that are most likely to affect the organization. The importance of the Contingency Plan is to have a set of policies and procedures of how to identify and handle incidents that occur within the organization. It is a survival guide. However no amount of planning will completely cover every type of disaster. The Contingency Plan needs to be a continuous effort. Generation of a Contingency Plan not only increases the organizations chance of survival but also will improve the economic structure and sustainability of the organization itself (FEMA).

References

Arnold, R.L. "Hurricane Andrew." *Disaster Recovery Journal*. URL:
http://www.drj.com/special/andrew.html
(1997).

Arnold, R.L. "Oklahoma City." *Disaster Recovery Journal*. URL:
http://www.drj.com/special/ok.html
(1997).

Arnold, R.L. "Underground Flood Hits Chicagos's Loop, Shutting Down Businesses for Weeks." *Disaster Recovery Journal.*
URL: http://www.drj.com/special/chicago.html
(1997).

TekCentral. "Business Continuity versus Disaster Recovery Planning."
URL: http://www.tekcentral.com/messages/ubb/Forum1/HTML/000002.html
(1999).

"Disaster Recovery Planning.ORG"
URL: http://www.drplanning.org

"Disaster Recovery Planning without Destroying Your Budget."
URL: http://www.disasterplan.com

FEMA. "Disaster Declaration Count Statistics." Federal Emergency Management Agency.
URL: http://www.fema.gov/library/dis_graph.htm
(1999).

Foster, D.R. "Species and stand response to catastrophic wind in central New England, USA." *Journal of Ecology* 76:135-151. 1988.

Moore, R. E. "The All-Hazards Contingency Planning Kit"
Altamonte Springs, FL.
Email: rmooreinc@aol.com
(1999).

Novelli, P. "Project Impact." Federal Emergency Management Agency.
URL: http://www.fema.gov/impact/prjimpct.ppt

(1999).

"Orange County Comprehensive Emergency Management Plan." Contact: Lemley, R.L.
Prepared by: Orange County Fire Rescue Department Office of Emergency Management and Emergency Support Function Planning Group.
(1999).

Toigo, J.W. Disaster Recovery Planning: Strategies for Protecting Critical Information. Prentice Hall. Upper Saddle River, NJ. 2000.

Thompson, T. "Emergency Management Guide For Business & Industry." Sponsored by a Public-Partnership with the Federal Emergency Management Agency.
URL: http://www.fema.gov
(1998).

USFA. "Non-residential Properties." United States Fire Administration.
URL: http://www.usfa.fema.gov/nfdc/non-resident.htm
(1999).