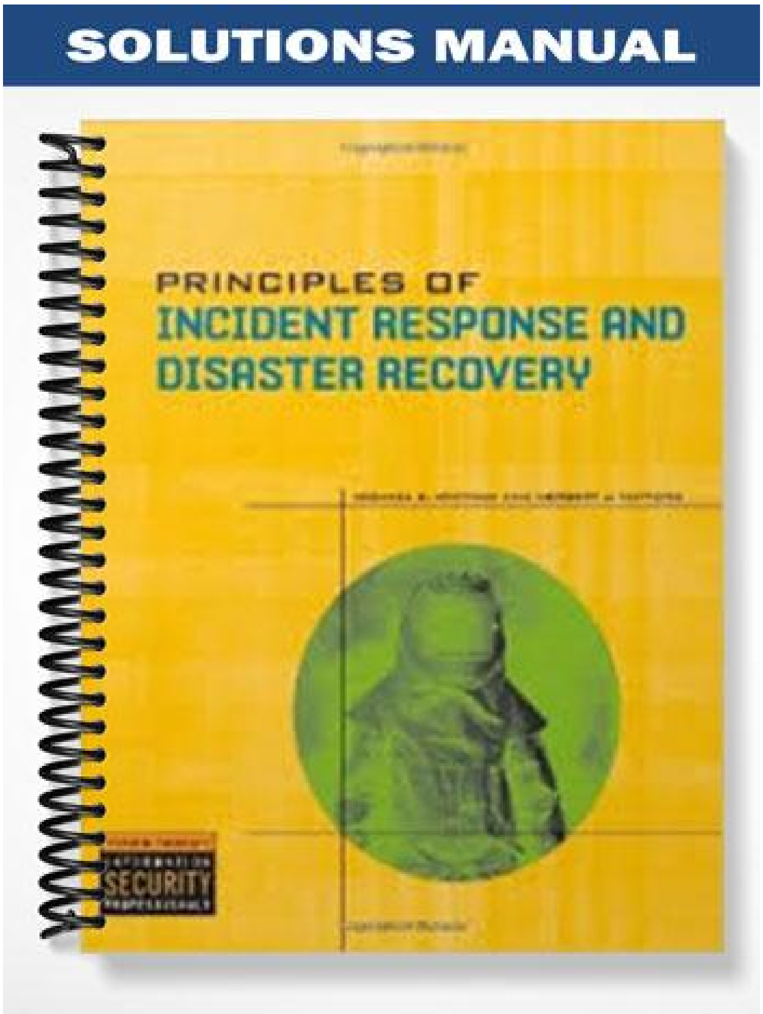
SOLUTIONS MANUAL
PRINCIPLES OF
INCIDENT RESPONSE AND
DISASTER RECOVERY
SECURITY

Chapter 2

Planning for Organizational Readiness

At a Glance

Instructor’s Manual Table of Contents

Lecture Notes

Overview

Chapter 2 provides an introduction to the process of planning for the management of incident response and disaster recovery. Students will learn the steps involved in the planning process, and what constitutes effective planning policy. They will learn about creating weighted analysis tables to assess incident impact. Students will become familiar with business impact analysis. Finally, students will learn about the contents of an effective contingency plan.

Objectives

- Identify an individual or group to create a contingency policy and plan
- Understand the elements needed to begin the contingency planning process
- Create an effective contingency planning policy
- Become familiar with the business impact analysis and each of the component parts of this important process
- Know the steps needed to create and maintain a budget for enabling the contingency planning process

Teaching Tips

Introduction

1. Set the stage for the depth and level of detail that will be presented in this chapter. Point out the complexity of preparing a contingency plan for a large organization.

2. Stress the importance of organizing the approach to planning as well as the importance of thorough planning itself.

3. Remind students that this process must occur in addition to the daily activities of the organization and the normal demands on participants' time.

Beginning the Contingency Planning Process

1. Point out that the first step is to determine who will be responsible for the policy and plans that will result from this effort.

Teaching Tip	Ownership of the process is vital to ensuring results.

2. Describe the typical functions of a contingency planning management team.

Teaching Tip	Commitment of executive level management is vital. Without this, the likelihood of successfully completing a workable plan is very small.

3. Describe the typical roles of individuals on the CPMT.

4. Describe the subordinate teams and how they interact with the CPMT, using Figure 2-1.

Commitment and Support of Senior Management

1. Reiterate the importance of executive level management, and point out that commitment must be formal.

2. Point out that the purpose of executive level commitment is to ensure that the necessary time and resources (key individuals and budgeting) will be readily available to the CPMT.

3. Introduce the concept of communities of interest.

4. Describe the three major communities of interest for information security.

5. Discuss each community of interest, comparing and contrasting the major objectives of each, and pointing out how those objectives might conflict with other groups.

Teaching Tip	Encourage class discussion on why these groups each have a different focus, and the conflicts that may arise in daily activities. Discuss how these varying objectives will influence each community's vision of what is required for the contingency plan.

Elements to Begin Contingency Planning

1. Describe the elements necessary to begin the process of creating a contingency plan.

Teaching Tip	Students may have never been involved in a complex planning process in which a methodology is required. Stress the importance of having a road map to guarantee that the team will not become lost in the complexity of the process. Point out that a planning methodology helps to guarantee that the end goal will ultimately be met.

2. Describe the CP document as the focus and collection point for the deliverables that will be produced by the other steps.

3. Describe the seven step process of the CP. Point out that each of these steps will be discussed in detail in the rest of this chapter.

Contingency Planning Policy

1. Introduce the concept of policy for the contingency planning process, describing its purpose and its effects.

Teaching Tip	By establishing and endorsing policy at the highest executive levels, executive management effectively “puts legs on” their commitment to the entire process.

2. Point out that policy defines the activities and the responsibilities, in essence formalizing the process in terms of job duties for those involved in the process.

3. Describe the contents of a typical CP policy.

Teaching Tip	A walk-through of the sample generic policy on pages 53-54 of the textbook will help students understand the purpose of the policy and what it accomplishes.

<u>Quick Quiz 1</u>

1. Who is responsible for obtaining senior management commitment and support at the outset of the planning process?
   Answer: the Contingency Planning Management Team (CPMT)

2. Describe the role of a champion on the CPMT.
   Answer: a high-level manager with influence and resources, who provides a strategic vision for the project

3. Who should set the policy for the contingency planning process?
   Answer: executive management

Business Impact Analysis

1. Introduce the concept of a business impact analysis and describe its purpose.

Teaching Tip	Point out that defining and analyzing each possible type of attack or disaster allows the plan to be usable regardless of the type of incident or disaster.

2. Describe the intended use of the BIA as the detailed steps to be taken when preventive controls have failed.

3. Describe the five stages that occur in conducting the BIA using Figure 2-2.

Teaching Tip	Discuss the importance of being very thorough in the BIA. All possible attack types should be considered and detailed scenarios should be developed.

4. Point out the need to determine the requirements of executive management so that the BIA results can be presented in a manner that meets those requirements.

Threat or Attack Identification and Prioritization

1. Point out that the risk management process described in Chapter 1 should have already identified and prioritized the threats facing the organization.

2. Describe the process of converting threats to attack profiles.

Teaching Tip	Stress the importance of including human factors such as work stoppages, loss of key personnel due to accidents, illness, or leaving the company, or other human-related factors. Having plans for information only will still leave an organization vulnerable to interruptions due to human factors.

3. Point out that some attacks may encompass several categories, and some categories may encompass several types of attacks.

Teaching Tip	This, of course, increases the complexity of both the planning process and the detailed incident response actions.

4. Discuss the specific types of threats and attacks listed in Table 2-1.

Teaching Tip	The stakes are more than simply lost data in today's world of highly-networked technology, and may include human life, as this incident proves: "The U.S. Dept. of Justice indicted Christopher Maxwell on charges that he caused disruptions at Seattle's Northwest Hospital in 2005. Maxwell attempted to introduce his software 'bots' into the hospital's network, and, in the process, caused operating room doors and intensive care unit computers to shut down, among other things." Source: SecurityWatch newsletter, http://mcpmag.com/columns/columnist.asp?columnistsid=16

Threat or Attack Prioritization

1. Discuss the importance of prioritizing the threats. Point out that most organizations do not have unlimited resources, so focusing on the priorities will provide the most return on investment.

2. Describe the creation of a weighted analysis table to assist in the prioritization.

3. Review Table 2-2, which shows a sample weighted analysis table of attacks.

Business Unit Analysis

1. Describe the process of analyzing and prioritizing business functions.

Teaching Tip	If a business cannot function normally, the priority must be on restoring those functions that are most critical – those with the most impact on the generation of revenue. A good example is the city of New Orleans after Hurricane Katrina. With businesses shut down and residents gone, tax revenue effectively dried up. With little or no income, the city was forced to lay off city workers, or ask them to work without pay.

2. Describe the use of a weighted analysis table for prioritizing business functions using Table 2-3.

Teaching Tip	Point out the repeated use of weighted analysis tables. By putting numbers on every aspect of the process, a true picture of the priorities will emerge. This is helpful in getting all departments "on board" with the final plan, as everyone will be able to see the "big picture" for the organization.

Attack Success Scenario Development

1. Define the terms attack scenario or attack profile.

2. Describe the purpose of defining attack scenarios.

3. Discuss the sample attack scenarios in the textbook on pages 63-65.

Teaching Tip	Ask the students to comment on the level of detail shown in the sample attack scenarios. What are the implications for the planning process when this much detail is required?

Potential Damage Assessment

1. Point out that developing detailed attack scenarios allows the estimation of the cost of best, worst, and most likely outcomes.

Teaching Tip	This is useful in budgeting resources for incident response and disaster recovery.

2. Discuss the scenario end case in the textbook on pages 67-68.

3. Point out that a side benefit is that a clear picture of recovery costs may allow business units to justify additional spending on protective and preventive measures by performing a cost/benefit analysis.

Subordinate Plan Classification

1. Introduce the concept of subordinate plans for dealing with the aftermath of an attack.

2. Discuss the differences between disastrous attacks and non-disastrous attacks, and point out that the main difference is the threat of injury or loss of life.

3. Describe the sample subordinate plan end case in the textbook on page 69.

<u>Quick Quiz 2</u>

1. The first step in the Business Impact Analysis is to identify and prioritize ___.
   Answer: threat attacks

2. Threats are converted to attacks and then used to create attack ____.
   Answer: profiles

3. The analysis of business ____ focuses on identifying which are the main revenue producing operations.
   Answer: functions or units

BIA Data Collection

1. Point out that BIA data is actually gathered at many different stages of the process, as well as from outside activities.

2. Briefly describe the ways that BIU data may be collected.

Teaching Tip	Highlight the diversity of sources, and point out that determining the impact of failure requires attention to physical, financial, and reputation-based aspects of damage.

Online Questionnaires

1. Discuss the use of an online questionnaire to collect information directly from people in specific business units.

Teaching Tip	Point out the need for good design of the questionnaire.

2. Discuss the sample questionnaire in the textbook shown in Tables 2-4 and 2-5.

Teaching Tip	Remind students that such a questionnaire will require a significant amount of time by the respondents. Executive level commitment and policy will ensure that those receiving the questionnaire will actually feel compelled to complete it.

3. Point out the importance of identifying recovery point and recovery time objectives.

Teaching Tip	It may not be possible to recover everything completely. Even if it is possible, it may not be cost-effective to do so. Having reasonable and measurable objectives allows you to measure the level of success in recovering from an attack.

Facilitated Data-Gathering Sessions

1. Introduce the concept of facilitated data-gathering sessions.

2. Point out that these sessions are conducted directly with end users and business managers.

Process Flows and Interdependency Studies

1. Describe the use of systems diagramming for modeling process flows and interdependency.

Teaching Tip	Consider the importance of such system documentation in the event of a major disaster, when key personnel may be unable to participate in the recovery process.

2. Discuss the sample use case diagram in Figure 2-3 and the sample use case description in Table 2-6.

3. Describe the sample class diagram shown in Figure 2-4, the sample sequence diagram shown in Figure 2-5, and the sample collaboration diagram shown in Figure 2-6.

Teaching Tip	Point out that while the particular methodology used is not as important as the completeness of the documentation, using industry standard modeling tools makes the documentation immediately usable by anyone brought in to help with the recovery.

Risk Assessment Research

1. Remind students that the risk management process is actually the starting point for the BIA, and will provide much information for the BIA.

2. Point out that outside sources can also be used to help quantify risk and potential damage.

IT Application or System Logs

1. Point out that logs can be used to gather statistical information on the frequency of occurrences, probability of success, etc., for various types of attacks.

Teaching Tip	A thorough review of logs may also uncover errors or obsolescence in system flow diagrams.

Financial Reports and Departmental Budgets

1. Point out that financial information helps prioritize business functions that contribute the most to revenue, and helps quantify the cost of lost sales, idle production, and lost opportunity costs.

Audit Documentation

1. Compliance with federal, state, and local regulations must be maintained even during recovery periods, so this must be accounted for in the contingency plan.

Production Schedules

1. Point out that production schedules can provide valuable information for assessing impact and for planning for required resources during recovery periods.

Budgeting for Contingency Operations

1. Discuss the need for appropriate budgeting to allow the execution of recovery activities.

Teaching Tip	Once again, the commitment of executive level management is crucial to ensuring that budgetary resources will be available for recovery activities.

Incident Response Budgeting

1. Point out that incident recovery may already be part of a normal IT budget.

2. Describe the various hardware and software tools that are used for both preventive and recovery purposes.

Disaster Recovery Budgeting

1. Point out that significant budgeting is required to carry an organization through a major disaster.

2. Remind students that while insurance may cover loss of physical plant, most policies do not cover loss of revenue.

Business Continuity Budgeting

1. Restoring operations in an alternative location or in locations without basic services may require the use of mobile/temporary solutions.

Teaching Tip	Discuss some of the mobile solutions that are available, such as mobile power units, mobile networking units, disaster recovery centers, etc. Complete mobile data center: http://apcc.com/resource/include/techspec_index.cfm?base_sku=ISXT440MD12RMBL.

Crisis Management Budgeting

1. Point out that the major item here involves financially supporting employees who may be unable to work due to the nature of the crisis.

Quick Quiz 3

1. The ____ analysis provides information about systems and the threats they face.
   Answer: BIA (or Business Impact Analysis)

2. Name two methods or sources for collecting data for the BIA.
   Answer: online questionnaires, focus groups, application and system logs, financial and budget documents, audit documentation, production schedules, risk assessment research, and process flows (systems diagramming)

3. (Disaster recovery or Incident response) budgeting is usually part of a normal IT budget.
   Answer: Incident response

Class Discussion Topics

1. Discuss the level of detail shown in the sample attack scenarios. What are the implications for the planning process when this much detail is required? Do you think this much detail is actually required? What are the advantages and disadvantages of including this much detail? Disadvantages may include the amount of time to produce the scenarios, the difficulties to determine all of the details, the potential for this information to become outdated in a short amount of time, etc. Advantages include the ability to quickly identify the type of attack, to know exactly what the impacts may be, and to have a detailed series of steps to use in the heat of the attack.

2. Why do you think it is important to include end users in the process of creating the contingency plan? What are the possible pitfalls of end user inclusion? Do you think it is possible to create a contingency plan with no end user involvement? Answers for inclusion might include the knowledge of the business functions and operations, ability to help prioritize attacks and critical operations, and ability to assess impact of damage or loss. Answers against inclusion might include “turf wars”, unrealistic expectations, etc.

Additional Projects

1. Assume that you have been hired by a small veterinary practice to help them prepare a contingency planning document. The practice has a small LAN with 4 computers and Internet access. Prepare a list of threat categories and the associated business impact for each. Identify preventive measures for each type of threat category. Include at least one major disaster in the plan.

2. You are now in the phase of developing a business continuity plan for the same veterinary practice. Describe the basic activities that must be managed by the BCP. Develop plans for alternate site relocation, and develop an estimated monthly budget for the alternate site operations.

Additional Resources

1. Data security, regulations, and disaster recovery – white paper: http://whitepapers.silicon.com/0,39024759,60168978p-39000437q,00.htm

2. Justifying the contingency plan: http://whitepapers.zdnet.com/abstract.aspx?promo=50002&docid=23791

3. The legal issues of disaster recovery planning: www.amaonline.com/dlps/liability.pdf

Key Terms

- **Attack scenario** (**attack profile**): depicts the methodology, indicators of the attack, and the broad consequences
- **Attach scenario end case**: estimates the best, worst, and most likely outcomes of a specific attach
- **Business Impact Analysis (BIA)**: an investigation and assessment of the impact of various types of attacks
- **Champion**: a high-level manager with influence and resources who provides the strategic vision for the contingency planning process
- **Contingency Planning Management Team (CPMT)**: a group of individuals responsible for writing the contingency plan document, conducting the BIA, and organizing subordinate teams
- **Contingency Planning Policy**: statement of intent and scope that establishes responsibility for development and operations of the CPMT
- **Community of interest**: a group of individuals united by their shared interests or values within the organization
- **Recovery point objective (RPO)**: the point in time to which systems and data must be recovered
- **Recovery time objective (RTO)**: the period of time within which functionality must be recovered
- **Subordinate plan**: a plan that deals with the aftermath of an attack
- **Weighted analysis table**: a table of items that have been prioritized and optionally assigned values to represent the priority of the item