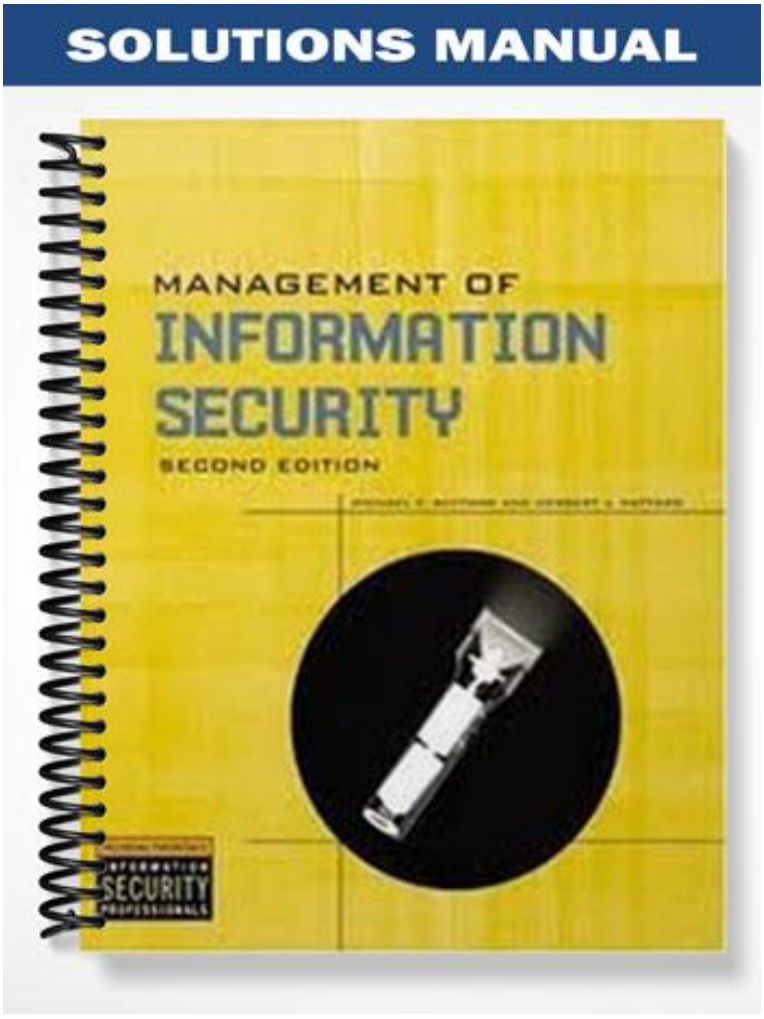
SOLUTIONS MANUAL



Chapter 2

Planning for Security

At a Glance

Instructor's Manual Table of Contents

Chapter Overview

In this chapter, the reader will come to recognize the importance of planning and will learn the principal components of organizational planning. Students will gain an understanding of the principal components of information security system implementation planning as it functions within the organizational planning scheme.

Chapter Outline

Chapter Objectives

When you complete this chapter, you will be able to:

- Recognize the importance of planning and describe the principal components of organizational planning
- Know and understand the principal components of information security system implementation planning as it functions within the organizational planning scheme

Setup Notes

This chapter could be completed in a single class session, if there is sufficient time to cover the material. Unless the students have not had the opportunity to read the material in advance (in some settings, the textbooks are not made available until the first class meeting), it may be prudent to have a general discussion of the topic, with detailed lecture to follow at the next class meeting. The subject matter can be covered in 1.25 to 2.5 hours.

Lecture Notes and Teaching Tips with Quick Quizzes

Introduction

In general, a successful organization depends on proper organizational planning.

In a setting where there are continual constraints on resources, both human and financial, good planning enables an organization to make the most out of the resources at hand.

Planning usually involves groups and organizational processes internal or external to the organization. They can include employees, management, stockholders, other outside stakeholders, the physical environment, the political and legal environment, the competitive environment, and the technological environment.

Teaching Tip	Note that Chapter 2 covers planning for operational business needs while Chapter 3 covers preparedness planning.

The major components of a strategic plan include the vision statement, mission statement, strategy, and a series of hierarchical and departmental plans.

Developing the organizational plan for information security depends upon the same planning process.

Since the information security community of interest seeks to influence the broader community in which it operates, the effective information security planner should know how the organizational planning process works so that participation in the process can yield meaningful results.

The dominant means of managing resources in modern organizations, planning is the enumeration of a sequence of action steps intended to achieve specific goals, and then controlling the implementation of these steps.

Planning provides direction for the organization's future.

Organizational planning should be undertaken using a top-down process in which the organization's leaders choose the direction and initiatives that the entire organization should pursue.

The primary goal of the organizational planning process is the creation of detailed plans: systematic directions on how to meet the organization's objectives. This is accomplished with a process that begins with the general and ends with the specific.

The primary goal of the organizational planning process is the creation of detailed plans.

Quick Quiz

1. What are the major components of a strategic plan? **ANSWER:** They are vision statement, mission statement, strategy, and a series of hierarchical and departmental plans.

2. What is the dominant means of managing resources in the modern organization? **ANSWER:** Planning

Precursors to Planning

To implement effective planning, an organization's leaders should first develop positions that explicitly state the organization's ethical, entrepreneurial, and philosophical perspectives.

Value Statement

By establishing a formal set of organizational principles and qualities in a values statement, as well as benchmarks for measuring behavior against these published values, an organization makes its conduct and performance standards clear to its employees and the public.

Integrity, honesty, passion, and respectfulness are significant parts of Microsoft's corporate philosophy. A values statement for RWW might take the following form:

RWW values commitment, honesty, integrity, and social responsibility among its employees, and is committed to providing its services in harmony with its corporate, social, legal, and natural environments.

Vision

In contrast to the mission statement, which expresses what the organization is, the vision statement expresses what the organization wants to become.

Vision statements therefore should be ambitious; after all, they are meant to express the aspirations of the organization and to serve as a means for visualizing its future.

The vision statement is the best-case scenario for the organization's future.

Random Widget Works will be the preferred manufacturer of choice for every business's widget equipment needs, with an RWW widget in every machine they use.

Mission

The mission statement explicitly declares the business of the organization, as well as its intended areas of operations. It is, in a sense, the organization's identity card.

The mission statement must explain what the organization does and for whom.

Random Widget Works, Inc. designs and manufactures quality widgets and associated equipment and supplies for use in modern business environments.

The Information Security Department is charged with identifying, assessing, and appropriately managing risks to Company X's information and information systems. It evaluates the options for dealing with these risks, and works with departments throughout Company X to decide upon and then implement controls that appropriately and proactively respond to these same risks. The Department is also responsible for developing requirements that apply to the entire organization as well as external information systems in which Company X participates [these requirements include policies, standards, and procedures]. The focal point for all matters related to information security, this Department is ultimately responsible for all endeavors within Company X that seek to avoid, prevent, detect, correct, or recover from threats to information or information systems.

Teaching Tip	Many schools have faculty who specialize in organizational development and planning. It would be very useful to have an outside viewpoint on the importance of planning in the modern organization.

Strategic Planning

Strategy, or strategic planning, is the basis of long-term direction for the organization.

In general, strategic planning guides organizational efforts, and focuses resources toward specific, clearly defined goals, in the midst of an ever-changing environment.

"In short, strategic planning is a disciplined effort to produce fundamental decisions and actions that shape and guide what an organization is, what it does, and why it does it, with a focus on the future."

Creating a Strategic Plan

After an organization develops a general strategy, it creates an overall strategic plan by extrapolating that general strategy into specific strategic plans for major divisions.

Each level of each division translates those objectives into more specific objectives for the level below.

However, in order to execute this broad strategy and turn statement into action, the executive team must first define individual responsibilities.

Planning Levels

Once the organization's overall strategic plan is translated into strategic goals for each major division or operation, such as the information security group, the next step is to translate these strategies into tasks with specific, measurable, achievable, and time-bound objectives.

Strategic planning then begins a transformation from general, sweeping statements toward more specific and applied objectives.

Tactical planning has a shorter focus than strategic planning, usually one to three years.

Tactical planning breaks down each applicable strategic goal into a series of incremental objectives.

Managers and employees use the operational plans, which are derived from the tactical plans, to organize the ongoing, day-to-day performance of tasks.

The operational plan includes clearly identified coordination activities across department boundaries, communications requirements, weekly meetings, summaries, progress reports, and associated tasks.

Planning and the CISO

The first priority of the CISO and information security manager should be the structure of a strategic plan.

While each organization may have its own format for the design and distribution of a strategic plan, the fundamental elements of planning are the same.

Elements of a strategic plan:

- Introduction by the President of the Board or CEO
- Executive summary
- Mission statement and vision statement
- Organizational profile and history
- Strategic issues and core values
- Program goals and objectives
- Management/operations goals and objectives
- Appendices (optional) (strengths, weaknesses, opportunities, and threats (SWOT), analyses, surveys, budgets, etc.)

Some additional tips for planning include:

- Create a compelling vision statement that frames the evolving plan and acts as a magnet for people who want to make a difference.
- Embrace the use of a balanced scorecard approach, which demands the use of a balanced set of measures and cause and effect thinking.
- Deploy a draft high-level plan early, and ask for input from stakeholders in the organization.
- Make the evolving plan visible.
- Make the process invigorating for everyone.
- Be persistent.
- Make the process continuous.
- Provide meaning.
- Be yourself.
- Lighten up and have some fun.

Quick Quiz

3. What does a mission statement accomplish? **ANSWER:** The mission statement explicitly declares the business of the organization, as well as its intended areas of operations.

4. Once a general strategy is developed, what happens next? **ANSWER:** An overall strategic plan is developed by extrapolating that general strategy into specific strategic plans for major divisions.

5. What should be the first priority of the CISO? **ANSWER:** The creation of a strategic plan

Planning for Information Security Implementation

The CIO and CISO play important roles in translating overall strategic planning into tactical and operational information security plans.

The CISO plays a more active role in the development of the planning details than does the CIO.

The job description for the Information Security Department Manager from Information Security Roles and Responsibilities Made Easy is:

- Creates a strategic information security plan with a vision for the future of information security at Company X (utilizing evolving information security technology, this vision meets a variety of objectives such as management's fiduciary and legal responsibilities, customer expectations for secure modern business practices, and the competitive requirements of the marketplace)
- Understands the fundamental business activities performed by Company X, and based on this understanding, suggests appropriate information security solutions that uniquely protect these activities
- Develops action plans, schedules, budgets, status reports and other top management communications intended to improve the status of information security at Company X

Teaching Tip	The "… Made Easy" series of books by Charles Cresson Wood is full of excellent examples from many areas of information security. While many examples are provided in the textbook, the source books have many more you may find useful.

Once the organization's overall strategic plan has been translated into IT and information security departmental objectives by the CIO, and then further translated into tactical and operational plans by the CISO, the implementation of information security can begin.

Implementation of information security can be accomplished in two ways: bottom-up or top-down.

The bottom-up approach can begin as a grass-roots effort in which systems administrators attempt to improve the security of their systems.

The key advantage to this approach is the technical expertise of the individual administrators, since they work with information systems on a daily basis.

Unfortunately, this approach seldom works, as it lacks a number of critical features, such as coordinated planning from upper management, coordination between departments, and the provision of sufficient resources.

The top-down approach, in contrast, has strong upper-management support, a dedicated champion, usually assured funding, a clear planning and implementation process, and the ability to influence organizational culture.

High-level managers provide resources; give direction; issue policies, procedures and processes; dictate the goals and expected outcomes of the project; and determine who is accountable for each of the required actions.

The most successful top-down approach also involves a formal development strategy referred to as the systems development life cycle.

For any top-down approach to succeed, however, high-level management must buy into the effort and provide all departments with their full support.

Such an initiative must have a champion—ideally, an executive with sufficient influence to move the project forward, ensure that it is properly managed, and push for acceptance throughout the organization.

Involvement and support of the end users is also critical to the success of this type of effort.

Introduction to the Security Systems Development Life Cycle

The general systems development life cycle (SDLC) is a methodology for the design and implementation of an information system in an organization widely used in IT organizations.

A methodology is a formal approach to solving a problem based on a structured sequence of procedures. Using a methodology ensures a rigorous process, and increases the likelihood of achieving the desired final objective.

The impetus to begin a SDLC-based project may be event-driven; that is, it may be started in response to some event in the business community, inside the organization, or within the ranks of employees, customers, or other stakeholders. Or, it could be plan-driven; that is, it could be the result of a carefully developed planning strategy.

At the end of each phase, a structured review or reality check takes place, during which the team and its management-level reviewers determine if the project should be continued, discontinued, outsourced, or postponed until additional expertise or organizational knowledge is acquired.

Teaching Tip	Most academic programs in IT and related areas will have some element of the curriculum that focuses on system development. When this is the case, it may be useful to explain SDLC methodologies using the approaches and terminology taught in your specific program. You may want to invite another instructor who specializes in system development, or even better, a practicing developer from the community to enrich this discussion.

The security systems development life cycle (SecSDLC), may differ in several specific activities, but the overall methodology is the same.

The SecSDLC process involves the identification of specific threats and the risks that they represent, and the subsequent design and implementation of specific controls to counter those threats and assist in the management of the risk.

Investigation in the SecSDLC

The investigation phase of the SecSDLC begins with a directive from upper management specifying the process, outcomes, and goals of the project, as well as its budget and other constraints.

Frequently, this phase begins with the affirmation or creation of security policies on which the security program of the organization is or will be founded.

Teams of managers, employees, and contractors are assembled to analyze problems, define their scope, specify goals and objectives, and identify any additional constraints not covered in the enterprise security policy.

Finally, an organizational feasibility analysis determines whether the organization has the resources and commitment to conduct a successful security analysis and design.

Analysis in the SecSDLC

The development team created during the investigation phase conducts a preliminary analysis of existing security policies or programs, along with documented current threats and associated controls.

This phase also includes an analysis of relevant legal issues that could affect the design of the security solution.

The risk management task also begins in this stage.

Risk Management

Risk management is the process of identifying, assessing, and evaluating the levels of risk facing the organization, specifically the threats to the organization's security and to the information stored and processed by the organization.

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

To better understand the analysis phase of the SecSDLC, you should know something about the kinds of threats facing organizations in the modern, connected world of information technology (or IT).

In this context, a threat is an object, person, or other entity that represents a constant danger to an asset.

An attack is a deliberate act that exploits a vulnerability.

It is accomplished by a threat agent that damages or steals an organization's information or physical asset.

An exploit is a technique or mechanism used to compromise a system.

A vulnerability is an identified weakness of a controlled information asset—the absence of controls, or the controls in place are no longer effective.

An attack is the use of an exploit to achieve the compromise of a controlled system.

Common attacks include:

- Malicious code
- Hoaxes
- Back doors
- Password crack
- Brute force
- Dictionary
- Denial-of-service (DoS) and distributed denial-of-service (DDoS)
- Spoofing
- Man-in-the-middle
- Spam
- Mail bombing
- Sniffer
- Social engineering
- Buffer overflow
- Timing

Teaching Tip	The world of cyberattacks moves quickly and evolves rapidly. It might be useful to prepare material on the most current attacks in common usage at the time of the lecture and introduce your students to the current events in the world of attacks.

The last step in knowing the enemy is to find some method of prioritizing the risk posed by each category of threat and its related methods of attack.

This can be done by adopting threat levels from an existing study of threats, or by creating your own categorization of threats for your environment based on scenario analyses.

To manage risk, you must identify and assess the value of your information assets.

This iterative process must include a classification and categorization of all of the elements of an organization's systems: people, procedures, data and information, software, hardware, and networking elements.

The next challenge in the analysis phase is to review each information asset for each threat it faces and create a list of the vulnerabilities.

As the analysis phase continues, the next task is to assess the relative risk for each of the information assets.

We accomplish this by a process called risk assessment or risk analysis.

Risk assessment assigns a comparative risk rating or score to each specific information asset.

Risk management is the part of the analysis phase that identifies vulnerabilities in an organization's information systems and takes carefully reasoned steps to assure the confidentiality, integrity, and availability of all the components in the organization's information system.

Design in the SecSDLC

The design phase actually consists of two distinct phases, the logical design and the physical design.

In the logical design phase, team members create and develop the blueprint for security, and examine and implement key policies that influence later decisions.

In the physical design phase, team members evaluate the technology needed to support the security blueprint, generate alternative solutions, and agree upon a final design.

Between the logical and physical design phases, a security manager may seek to use established security models to guide the design process.

Security models provide frameworks for ensuring that all areas of security are addressed; organizations can adapt or adopt a framework to meet their own information security needs.

One of the design elements of the information security program is the information security policy of the organization.

Management must define three types of security policy:

1) General or security program policy
2) Issue-specific security policies
3) Systems-specific security policies

Another integral part of the information security program to be designed is the security education and training (SETA) program.

The SETA program consists of three elements: security education, security training, and security awareness.

The purpose of SETA is to enhance security by:

1) Improving awareness of the need to protect system resources
2) Developing skills and knowledge so computer users can perform their jobs more securely
3) Building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems

As the design phase continues, attention turns to the design of the controls and safeguards used to protect information from attacks by threats.

There are three categories of controls:

- Managerial controls address the design and implementation of the security planning process and security program management. Management controls also address risk management and security controls reviews.
- Operational controls cover management functions and lower-level planning, such as disaster recovery and incident response planning. Operational controls also address personnel security, physical security, and the protection of production inputs and outputs.
- Technical controls address those tactical and technical issues related to designing and implementing security in the organization. Here, the technologies necessary to protect information are examined and selected.

Another element of the design phase is the creation of essential preparedness documents.

- Contingency planning (CP) is the entire planning conducted by the organization to prepare for, react to, and recover from events that threaten the security of information and information assets in the organization, and the subsequent restoration to normal business operations.

    - Incident response planning (IRP) is the planning process associated with the identification, classification, response, and recovery from an incident.
    - Disaster recovery planning (DRP) is the planning process associated with the preparation for and recovery from a disaster, whether natural or man-made.
    - Business continuity planning (BCP) is the planning process associated with ensuring that critical business functions continue if a catastrophic incident or disaster occurs.

As the design phase progresses, attention now focuses on physical security, which addresses the design, implementation, and maintenance of countermeasures that protect the physical resources of an organization.

Physical resources include people, hardware, and the supporting system elements and resources associated with the management of information in all its states, transmission, storage, and processing.

Implementation in the SecSDLC

The security solutions are acquired, tested, implemented, and tested again.

Personnel issues are evaluated, and specific training and education programs are conducted.

Perhaps the most important element of the implementation phase is the management of the project plan.

The major steps in executing the project plan are:

1) Planning the project
2) Supervising the tasks and action steps within the project plan
3) Wrapping up the project plan

Information security is a field with a vast array of technical and nontechnical requirements.

The project team should consist of a number of individuals who are experienced in one or multiple requirements of both the technical and nontechnical areas.

- The champion
- The team leader
- Security policy developers
- Risk assessment specialists
- Security professionals
- Systems administrators
- End users

Just as each potential employee and potential employer look for the best fit, each organization should examine the options possible for staffing of the information security function.

- First, the entire organization must decide how to position and name the security function within the organization.
- Second, the information security community of interest must plan for the proper staffing (or adjustments to the staffing plan) for the information security function.
- Third, the IT community of interest must understand the impact of information security across every role in the IT function and adjust job descriptions and documented practices accordingly.
- Finally, the general management community of interest must work with the information security professionals to integrate solid information security concepts into the personnel management practices of the organization.

It takes a wide range of professionals to support a diverse information security program:

- Chief Information Officer (CIO)
- Chief Information Security Officer (CISO)
- Security managers
- Security technicians
- Data owners
- Data custodians
- Data users

Many organizations seek professional certification so that they can more easily identify the proficiency of job applicants:

- CISSP
- SSCP

- GIAC
- SCP
- Security +
- CISA/CISM

Maintenance and Change in the SecSDLC

Once the information security program is implemented, it must be operated, properly managed, and kept up to date by means of established procedures.

If the program is not adjusting adequately to the changes in the internal or external environment, it may be necessary to begin the cycle again.

While a systems management model is designed to manage and operate systems, a maintenance model is intended to complement a systems management model and focus organizational effort on system maintenance.

- External monitoring
- Internal monitoring
- Planning and risk assessment
- Vulnerability assessment and remediation
- Readiness and review
- Vulnerability assessment

One of the maintenance issues that must be planned in the SecSDLC is the systems management model that will be used. The ISO management model is a five-area approach that provides structure to the administration and management of networks and systems. These five areas are:

- Fault management
- Configuration and name management
- Accounting management
- Performance management
- Security management

Fault Management. Involves identifying and addressing faults in the applied information security profile and then addressing them, and the monitoring and resolution of user complaints.

Configuration and Change Management. The administration of various components involved in the security program and the administration of changes in the strategy, operation, or components of the information security program.

Accounting and Auditing Management. Involves chargeback accounting and systems monitoring. Chargeback accounting happens when organizations internally charge their departments for system use. While chargebacks are seldom used today, certain kinds of resource usage are commonly tracked—such as those on a computing system (like a server or a desktop computer) or human effort-hours—to recover IT costs from non-IT units of the organization. Accounting management involves monitoring the use of a particular component of a system. In networking, this monitoring may simply determine which users are using which resources. However, in security, it may be easy to track which resources are being used but difficult to determine who is using them. At that point, accounting management begins to overlap with performance management, which is addressed in the next section. With accounting management, you begin to determine optimal points of systems use as indicators for upgrade and improvement. Auditing is the process of reviewing the use of a system, not to determine its performance, but to determine if misuse or malfeasance has occurred.

Performance Management. Because many information security technical controls are implemented on common IT processors, they are affected by the same factors as most computer-based technologies. It is therefore important to monitor the performance of security systems and their underlying IT infrastructure to determine if they are effectively and efficiently doing the job they were implemented to do. Some information security control systems, such as Internet usage monitors that look for inappropriate use of Internet resources, operate as pass-by devices.

Security Program Management. Once an information security program is functional, it must be operated and managed. The ISO five-area framework provides some structure for a management model; however, it focuses on ensuring that various areas are addressed, rather than guiding the actual conduct of management. In order to assist in the actual management of information security programs, a formal management standard can provide some insight into the processes and procedures needed. This could be based on the BS7799/ISO17799 model or the NIST models described earlier.

Comparing the SDLC and the SecSDLC

Table 2-2:

	Steps common to the SDLC and the SecSDLC	Steps unique to the SecSDLC
Phase 1: Investigation	■ Outline project scope/goals ■ Estimate costs ■ Evaluate existing resources ■ Analyze feasibility	■ Define project process and goals and document them in the program security policy
Phase 2: Analysis	■ Assess current system against plan developed in Phase 1 ■ Develop preliminary system requirements ■ Study integration of new system with existing system ■ Document findings and update feasibility analysis	■ Analyze existing security policies and programs ■ Analyze current threats and controls ■ Examine legal issues ■ Perform risk analysis
Phase 3: Logical Design	■ Assess current business needs against plan developed in Phase 2 ■ Select applications, data support, and structures ■ Generate multiple solutions for selection of best ■ Document findings and update feasibility analysis	■ Develop security blueprint ■ Plan incident response actions ■ Plan business response to disaster ■ Determine feasibility of continuing and/or outsourcing the project
Phase 4: Physical Design	■ Select technologies to support solutions developed in Phase 3 ■ Select the best solution ■ Decide whether to make or buy components ■ Document findings and update feasibility analysis	■ Select technologies needed to support security blueprint ■ Develop definition of successful solution ■ Design physical security measures to support technological solutions ■ Review and approve project
Phase 5: Implementation	■ Develop or buy software ■ Order components ■ Document system ■ Train users ■ Update feasibility analysis ■ Present system to users ■ Test system and review performance	■ Buy or develop security solutions ■ At end of phase, present tested package to management for approval
Phase 6: Maintenance	■ Support and modify system for its useful life ■ Test periodically for compliance with business needs ■ Upgrade and patch as necessary	■ Constantly monitor, test, modify, update, and repair to respond to changing threats

Quick Quiz

6. What is the SDLC? **ANSWER:** The SDLC is the general systems development life cycle, a methodology widely used in the IT industry as an aid in creating quality systems that are delivered on time and within budget.

7. What is the SecSDLC? **ANSWER:** The SecSDLC is a variant of the SDLC that focuses on the needs of the information security projects that it might be used to manage.

8. What is a threat? **ANSWER:** An object, person, or other entity that represents a constant danger to an asset

Discussion Topics

1. Which group poses the most risk to the organization, insiders or outsiders? ANSWER: The answer to this question will vary, but can be used to provoke discussion. Historically, insiders have always posed a bigger threat, but the rise of the Internet and the interconnection of organizational systems to the public networks introduces risks that change that balance for many organizations.

2. Are threats geographically based? ANSWER: Some threats, specifically threats from natural disasters, are often based on where the organization is located. A business in San Francisco should be planning to counter the threat of earthquake, while a school in Oklahoma City should be planning for tornadoes.

Key Terms

Analysis phase
Attack
Bottom-up approach
Business continuity planning (BCP)
Champion
Chief Information Officer (CIO)
Chief Information Security Officer (CISO)
Contingency planning (CP)
Control
Data custodians
Data owners
Data users
Disaster recovery planning (DRP)
Ethical hackers
Event-driven
Exploit
Feasibility analysis
Implementation phase
Incident response planning (IRP)
Information security policy
Investigation phase
Joint Application Development (JAD)
Logical design phase
Maintenance phase
Managerial controls
Methodology
Mission statement
Operational controls
Penetration testing
Physical design phase
Physical security
Plan-driven
Red teams
Risk analysis
Risk assessment
Risk management
Safeguard
Security education, training, and awareness (SETA)
Security Managers
Security systems development life cycle (SecSDLC)
Security technicians
Strategy
Structured review
Systems development life cycle (SDLC)
Technical controls
Threat
Threat agent
Tiger teams
Top-down approach
Values statement
Vision statement
Vulnerability
White-hat hackers

Additional Project Ideas

1. There are many interesting sources for information on current cyberattack threats. Break your students up into teams and have them identify a list of five known cyberattacks. Then research each attack using at least three different Web resources. Ask them to note the similarities and differences of the information found at each reference location.

2. Every IT department in most medium and large businesses has a planning process. You can assign your students to visit/contact these organizations in your area to find out how they undertake the planning processes described in the textbook.

Solutions to Review Questions can be found within the Instructor's Resource Kit (CD-ROM) that accompanies this text or at the following link:

www.course.com