Instructor's Manual

Chapter 2

Planning and Policy

Learning Objectives

By the end of this chapter, the student should be able to:

- Justify the need for formal management processes.
- Explain the plan-protect-respond security management cycle.
- Describe compliance laws and regulations.
- Describe organizational security issues.
- Describe risk analysis.
- Describe technical security infrastructure.
- Explain policy-driven implementation.
- Know governance frameworks.

Teaching Suggestions

Special Issues

This is a longer chapter than the others and may require additional time to cover it adequately.

Role in the Book

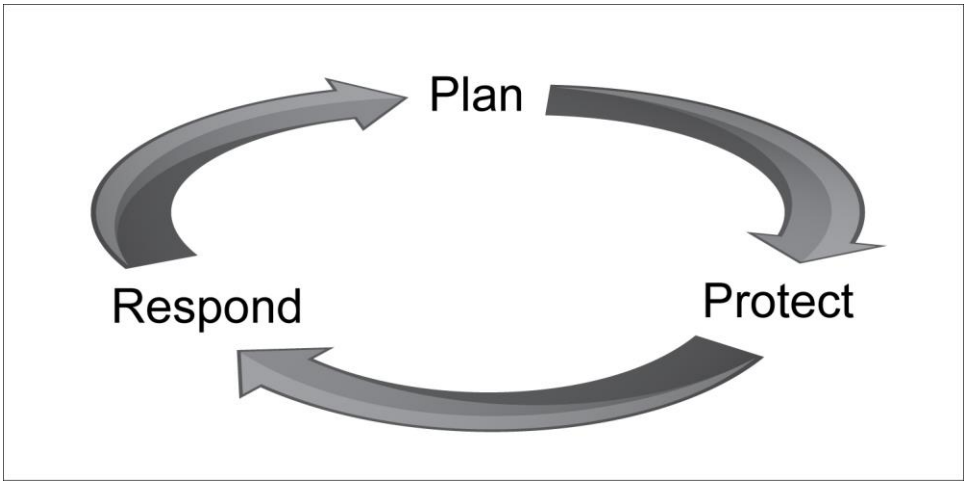
Chapter 1 surveyed the security threats that corporations face today. Chapter 2 and the remaining chapters deal with the management of defenses against these and future threats.

The book is organized around the plan-protect-respond cycle for security management. Chapter 2 introduces the plan-protect-respond cycle and discusses the planning phase of the cycle.

Teaching the Material

Flow of Material

- The chapter begins with a broad look at security management. This section discusses why management is difficult to think about, the need for comprehensive security, weakest link failures, and the plan-protect-respond cycle that will dominate this book and that also dominates practical IT security. It also talks about vision in planning and strategic IT security planning.



- The chapter then discusses the most fundamental management decisions regarding how to organize the IT security function. A key theme is maintaining independence for IT security, because it is difficult to accuse one's boss of security violations.
- The next section, on risk analysis, is absolutely central to network management. The concept of risk management should be emphasized throughout the course.
- Next comes planning the technical security architecture—the mix of tools a company can use to plan its technical aspects of security. This section covers topics that come up frequently in security technology planning, including defense in depth, single points of vulnerability, the need to minimize security burdens, and having realistic goals.
- IT security planning and execution is driven by policies that give high-level directives for how security should be implemented. Policy-based thinking permeates IT security, this book, and almost any IT security course. It is crucial to have students understand policy-based implementation backwards and forwards. Although implementers need freedom to select the best way to implement specific policies,

given current technologies and products, additional implementation guidance is needed to restrict implementer discretion through guidelines, standards, procedures, processes, baselines, and other methods. Policies also govern the oversight needed to keep the security process on target.

- To avoid reinventing the wheel in IT security, many companies use one or more IT governance frameworks to guide them in what to do and how to do it. The final section looks through these frameworks. Each framework adds something to the picture, but no framework does everything.

Covering the Material

Quite simply, this chapter covers a great deal and requires a great deal of lecture time. It is important to keep students from getting lost in the details by putting up posters of general frameworks, such as the policy-based information field, and frequently helping students keep abreast of where they are in the framework.

Much of the material is dry, and students can read much of the material without difficulty. This means that you can jump over the obvious stuff and spend more time on the more difficult and important stuff. For instance, focus on why security metrics are important, what auditing means, the surprising importance of anonymous protected hotlines, why behavioral cues often predate security violations, why vulnerability tests are dangerous, and specific types of sanctions. Explain a concept and then have students tell you why it is important.

For the discussion of policies, have students bring security policies from their university and other sources and have them discuss why each section is in it to see if they can spot anything missing. Typically, they only have access to the university's acceptable use policy, which is oriented toward users. If you can get other policies from other firms, that would be good.

Assigning Homework

To focus students, you can assign specific Test Your Understanding questions, Hands-On Projects, Project Questions, and end-of-chapter questions they should master or even hand in as homework. You can also specify questions or parts of questions they do not have to master. Multiple choice and true/false questions in the testbank are tied to specific parts of specific questions, so creating multiple guess questions on exams is relatively straightforward.

Case Study

Some teachers like to start class off with a case discussion that illustrates the material covered in the chapter. Starting class off with a case discussion increases student involvement and encourages students to read the chapter material before class.

Each chapter includes a business case that directly relates to the material covered in the chapter. The business case comes directly from a real-world example. At the end of each business case, you will find "key findings" from a related annual industry report. The report's key findings are related to the business case and are focused on current industry issues. All industry reports are online and completely free. Footnotes provide URLs to each report. Industry reports tend to be 20-60 pages in length, and can be assigned as additional reading.

Answer Key

Introduction

Defense

1. a) Why does the book focus on defense instead of offense?

   This book focuses on defense rather than offense because after students master the principles and practices of defense well, a detailed understanding of attacks will help them very much. Also, this book is preparing students for their real job, which is security defense.

   b) Can IT Security be *too* secure? How?

   Yes, if security is too strict, rigid, or time consuming, it may reduce an organization's effectiveness. For example, if all staff computers were set to automatically lock after 2 minutes of inactivity, it could lead to widespread frustration. Users would also spend considerable amounts of time continually logging in. Even worse, they might look for ways around the new security measures.

Management Processes

2. a) For what reasons is security management hard?

   Security management is hard and abstract. You cannot show pictures of devices or talk in terms of detailed concepts or software algorithms. There are fewer general principles to discuss, and most of these principles cannot be put into practice without well-defined and complex processes.

   b) What is comprehensive security, and why is it needed?

   Comprehensive security is comprised of closing all routes of attack into an organization’s systems from attackers. Comprehensive security is needed because attackers constantly look for one or more weaknesses that can provide initial system access and lead to greater control of system resources. Companies must understand all of their possible vulnerabilities because this is exactly what hackers are doing to determine the best course of action to attack a system.

   c) What are weakest-link failures?

   Weakest-link failures occur when a single security element failure defeats the overall security of a system.

The Need for a Disciplined Security Management Process

3. a) Why are processes necessary in security management?

Security is too complicated to be managed informally. Companies must develop and follow formal processes (planned series of actions) in security management.

b) What is driving firms to use formal governance frameworks to guide their security processes?

One external factor that is motivating firms to formalize their security processes is a growing number of compliance laws and regulations. Many compliance regimes require firms to adopt a specific formal governance framework to drive security planning and operational management.

The Plan–Protect–Respond Cycle

4. a) List the three stages in the plan-protect-respond cycle.

Planning, protection, and response

b) Is there a sequential flow between the stages?

No. They interact constantly.

c) What stage consumes the most time?

Protection

d) How does this book define protection?

Protection is defined as the plan-based creation of operation and countermeasures.

e) How does the book define response?

Response is defined as recovery according to plan.

Vision in Planning

5. a) How can good security be an enabler?

Good security provides not only a sense of confidence in network reliability, but can allow safe and effective implementation of progressive business tactics, such as inter-organizational system connectivity. By having good security, firms can innovate their business practices without having to incur a significant material risk.

b) What is the key to being an enabler?

The key to being an enabler in security is getting involved early within the project.

c) Why is a negative view of users bad?

Viewing users as the enemy is corrosive. Users often are the first to see security problems, and if they feel that they are part of the security team, they can give early warnings to the security staff. Also, users need to be trained in

security self defense so that they can protect their own assets from threats. If "stupid" means "poorly trained," this is the security department's fault.

d) Why is viewing the security function as a police force or military organization a bad idea?

Police and military organizations are often considered oppressive in enforcing their policies. Creating a police-like security atmosphere relies upon fear of internal reprisal when enforcing policy, versus fostering a proactive partnership between employees and security personnel to protect the organization from the real bad guys who seek to harm everyone in the firm.

Strategic IT Security Planning

6. a) In developing an IT security plan, what should a company do first?

It must first assess the current state of its security.

b) What are the major categories of driving forces that a company must consider for the future?

A company must consider the threat environment, the growth of compliance laws and regulations, changes in the corporate structure, mergers, and anything else that will change things in the future.

c) What should the company do for each resource?

Once company resources are enumerated, they must be classified in terms of sensitivity. Not all resources are equally important, and with limited budgets, one must be able to prioritize.

d) For what should a company develop remediation plans?

A company should develop remediation plans for all security gaps and for every resource, unless it is well protected.

e) How should the IT security staff view its list of possible remediation plans as a portfolio?

By viewing the list of possible remediation plans as a portfolio, security staff can assess which remediation plans should get funding and action first, and which projects will provide the greatest gains in security based on the investment.

Compliance Laws and Regulations

Driving Forces

Many companies have relatively good security plans, protections, and response capabilities. To plan for the future, however, even these companies need to understand the **driving forces** that require them to change their security planning, protections, and response.

Perhaps the most important set of driving forces for firms today are **compliance laws and regulations,** which create requirements for corporate security. In many cases, firms must substantially improve their security to be in compliance with these laws and regulations.

This is especially true in the areas of documentation and identity management. These improvements can be very expensive. Another problem for corporate security is that there are so many compliance laws and regulations.

7. a) What are driving forces?

   Driving forces are things that require a firm to change its security planning, protections, and response.

   b) What do compliance laws do?

   Compliance laws and regulations create requirements to which security must respond. In many cases, without compliance laws, many companies would not spend the time or effort to address serious security issues.

   These create requirements to which security must respond.

   c) Why can compliance laws and regulations be expensive for IT security?

   Because some firms need to improve their security to be in compliance with security laws and regulations, these improvements can be very expensive.

Sarbanes–Oxley

8. a) In Sarbanes-Oxley, what is a material control deficiency?

   It is a material deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement in the annual or interim financial statements will not be prevented or detected.

   b) Why was Sarbanes-Oxley important for IT security?

   Under Sarbanes-Oxley, companies have had to take a detailed look at their financial reporting processes. In doing so, they've uncovered many security weaknesses and, in many cases, realized that these security weaknesses extended to other parts of the firm. Given the importance of Sarbanes-Oxley compliance, most firms have been forced to increase their security efforts.

Privacy Protection Laws

9. a) What have privacy protection laws forced companies to do?

   These laws have forced companies to look at how they protect personal information, including where this information is stored and how they control access to it.

   b) What did they find when they did so?

   In many cases, they have discovered that this information is stored in many places, including word processing documents and spreadsheets. They also discovered that access controls and other protections are either weak or nonexistent.

   c) What institutions are subject to the Gramm-Leach-Bliley Act?

   The GLBA specifically addresses strong data protection requirements at financial institutions.

d) What institutions are subject to HIPAA?

Healthcare organizations.

Data Breach Notification Laws

10. a) What do data breach notification laws require?

These laws require companies to notify affected people if sensitive, personally identifiable information is stolen or even lost.

b) Why has this caused companies to think more about security?

The repercussions of data breaches have companies rethinking security. Loss of personal data can be extensive, which can lead to large government penalties, damaged reputations, and expensive lawsuits.

The Federal Trade Commission

11. a) When can the Federal Trade Commission act against companies?

The FTC can act against companies that fail to take reasonable precautions to protect privacy information.

b) What financial burdens can the FTC place on companies that fail to take reasonable precautions to protect private information?

The FTC can impose hefty fines on firms and has the power to require that firms pay to be audited annually by an external firm for many years, and to be responsive to these audits.

Industry Accreditation

12. Besides HIPAA, what external compliance rules must hospitals consider when planning their security?

Hospitals must comply with all other external compliance rules that apply to other businesses that perform similar functions or transactions. For example, hospitals that process credit cards for payment must meet PCI-DSS standards, physical security requirements that come with treating prisoners, etc.

PCI–DSS

13. What companies does PCI-DSS affect?

All companies that accept credit card payments are subject to PCI-DSS.

FISMA

14. a) Who is subject to FISMA?

Organizations subject to FISMA include all information systems used or operated by a U.S. Federal Government agency or a contractor or any other organization on behalf of a U.S. Government agency.

b) Distinguish between certification and accreditation in FISMA.

Certification in FISMA is certification of the organization itself or by an outside party. Once the system is certified, the organization's IT security is reviewed by an accrediting official. If the official is satisfied with the certification, the accrediting official will issue an authorization to operate (ATO).

c) Why has FISMA been criticized?

FISMA has been criticized heavily for focusing on documentation rather than protection.

Organization

Chief Security Officers (CSOs)

15. a) What is the manager of the security department usually called?

Chief security officer (CSO)

b) What is another title for this person?

Chief information security officer (CISO)

Should You Place Security within IT?

16. a) What are the advantages of placing security within IT?

One advantage of placing security within IT is that it is attractive because security and IT possess many of the same qualities and technological skills. Another advantage would be the centralizing of security and IT under the CIO. The CIO would have IT implement security and is likely to back the security department in its effort to create a strong and safe information system for the organization.

b) What are the disadvantages of placing security within IT?

The disadvantage of placing security within IT is that security has no independence from IT and it is hard to blow the whistle on security issues occurring within the IT department or by the CIO. Having security reside in the IT department creates a situation wherein no one is watching the watchers (who are also the implementers).

c) What do most IT security analysts recommend about placing or not placing IT security within IT?

Most IT security analysts recommend placing IT security functions outside of the IT department.

d) How are security roles allocated in the hybrid solution to placing IT security inside or outside of the IT department?

In the hybrid solution of IT security, the IT department is given the operational aspects such as maintaining firewalls, while planning, policy-making, and auditing functions are placed outside of IT.

Top Management Support

17. a) Why is top management support important?

Top management support is important because few efforts as pervasive as IT security succeed unless top management gives strong and consistent support. The proof of top management support comes in subsequent actions.

b) What three things must top management do to demonstrate support?

In order to demonstrate support, top management must ensure that security has an adequate budget, supports security when there are conflicts between the needs of security and the needs of other business functions, and follows security procedures themselves.

Relationships with Other Departments

18. a) Why is the human resources department important to IT security?

HR is important to IT security because this department is responsible for the hiring and training of employees in security, which makes this process very critical. IT security must work with HR in hiring and terminating to ensure that security issues are taken into account.

b) Distinguish between the three main types of corporate auditing units.

Internal auditing: examines organizational units for efficiency, effectiveness, and adequate controls.

Financial auditing: examines financial processes for efficiency, effectiveness, and adequate controls.

IT auditing: examines IT processes for efficiency, effectiveness, and adequate controls.

c) What is the advantage of placing IT security auditing in one of these three auditing departments?

The advantage is that it will bring more independence to security auditing. It will allow IT security auditing to blow the whistle on the IT security department or CSO if necessary.

d) What relationships can the IT security have to the corporation's uniformed security staff?

The company's uniformed security staff will execute policies regarding building access. The uniformed security staff is also needed to seize computers that IT security finds to be involved in financial crime or abuse. In the other direction, IT security can help uniformed security with surveillance cameras and the forensics analysis of equipment that may have been used to commit a crime.

e) What can the security staff do to get along better with other departments in the firm?

To get along with other departments, security should combine policies with financial benefits analyses and realistic business impact statements.

f) What are business partners?

Business partners include buyer organizations, customer organizations, service organizations, and even competitors.

g) Why are they dangerous?

Business partners are dangerous because they're often granted access to resources within your firm.

h) What is due diligence?

Due diligence entails investigating the IT security of external companies and the implications of close IT partnerships before implementing inter-connectivity.

Outsourcing IT Security

19. a) What is an MSSP?

It is a managed security service provider. It is an outsourced alternative for delegating controls.

b) What are the two main benefits of using an MSSP?

One benefit of using an MSSP is that they have expertise and practice-based knowledge. Another benefit is that they have complete independence from the IT security department.

c) Why are MSSPs likely to do a better job than IT security department employees?

If the MSSP is doing its job, it will examine several hundred suspicious events each day. It will quickly identify most as obvious false positives. Still others will be classified as negligible threats, such as minor scanning attacks. On a typical day, only one or two potentially serious threats may be brought to the attention of the client via pager or e-mail alerts, depending on their potential severity. By distilling the flood of suspicious incidents into a handful of important events requiring client action each day, MSSPs free the security staff to work on other matters.

d) What security functions typically are outsourced?

Intrusion detection and vulnerability testing

e) What security functions usually are not outsourced?

Policy and planning

f) What should a firm look for when selecting an MSSP?

The firm should look at the contract with the outsourcing firm to see if the MSSP scans log files daily or otherwise according to contract. The firm should also see if the MSSP is sending alerts about the company's security.

Risk Analysis

Reasonable Risk

20. a) Why is information assurance a poor name for IT security?

    This is a poor name because it is never possible to eliminate risks and completely assure information.

    b) Why is reasonable risk the goal of IT security?

    Reasonable risk is the goal of IT security because not only is it technically impossible to protect against all current and future risk, but if you could the comprehensive security protections would be prohibitively expensive and most likely impede some functionality that is necessary for business operations.

    c) What are some negative consequences of IT security?

    Most obviously, security tends to impede functionality. Living in a high-security environment is always unpleasant and is usually inefficient. If you live in a quiet and safe neighborhood, putting bars on your windows would create a lock-down feeling, and requiring you to remember a long password to get into your house would slow you down every time you went into your house. Besides these psychic and productivity costs, security is never free and seldom cheap. Security devices are expensive, and the labor to implement and operate them is far more expensive.

Classic Risk Analysis Calculations

21. a) Why do we annualize costs and benefits in risk analysis computations?

    To see if countermeasures will alter the likelihood of losses or decide whether countermeasures produce benefits that exceed costs.

    b) How do you compute the ALE?

    The ALE is calculated by multiplying the single loss expectancy value by the annualized probability of occurrence.

22. [Revised Question] An asset has a value of $1,000,000. In an attack, it is expected to lose 60 percent of its value. An attack is expected to be successful once every ten years. Countermeasure X will cut the amount lost per incident by two-thirds. Counter measure Y will cut the frequency of successful attack in half. Countermeasure X will cost $30,000 per year, while Countermeasure Y will cost $5,000 per year. Do an analysis of these countermeasures and then give your recommendation for which to select (if any).

    The analysis is shown below. Countermeasure Y should be implemented. It reduces expected damage less than Countermeasure X but costs much less than Countermeasure X. While Countermeasure X is expected to save $20,000 per year, Countermeasure Y is expected to save $25,000.

		Base Case	Countermeasure	
			X	Y
Asset Value	AV	$1,000,000	$1,000,000	$1,000,000
Exposure Factor	EF	60%	20%	60%
Single Loss Expectancy	SLE	$600,000	$200,000	$600,000
Annualized Rate of Occurrence	ARO	10%	10%	5%
Annualized Loss Expectancy	ALE	$60,000	$10,000	$30,000
ALE Reduction for Countermeasure	--	NA	$50,000	$30,000
Annualized Countermeasure Cost	--	NA	$30,000	$5,000
Annualized Net Countermeasure Value	--	NA	$20,000	$25,000

Problems with Classic Risk Analysis Calculations

23. a) Why is it a problem if benefits and costs both occur over several years?

When there are uneven cash flows over a number of years, decision makers turn to discounted cash flow analysis, also called return on investment (ROI) analysis. This requires either the computation of net present value (NPV) or internal rate of return (IRR).

b) Why should the total cost of an incident (TCI) be used in place of exposure factors and asset values?

TCI should be used because it gives a better estimate of the complete cost of a compromise, including the cost of repairs, lawsuits, and other factors. The problem is coming up with a realistic value for TCI.

c) Why is it not possible to use classic risk analysis calculations for firewalls?

Classical risk analysis assumes a one-to-one relationship between countermeasures and threats. However, reality is that many countermeasures address many threats, such as the firewall, which protects both servers and clients.

d) What is the worst problem with the classic approach?

The worst problem with the classic approach is that it is rarely possible to estimate the annualized rate of occurrence for threats.

e) Why is hard-headed thinking about security ROI dangerous?

Hard-headed thinking, based upon ROI estimates for security implementation, is dangerous because the risks from having poor security are complex and somewhat implicit. As described above, whether using classical risk analysis calculations or improved TCI values, it is incredibly hard to calculate the damage a significant breach can have on a company (from minimal to catastrophic). In reality, one can mostly calculate the cost of a compromise after the fallout is through, which could take years, and even then there are implicit effects that are hard to quantify (e.g., reputation damage).

Responding to Risk

24. a) What are the four ways of responding to risk?

Risk reduction: Adopt active countermeasures.

Risk acceptance: Used when the impact is small and cost of countermeasure is prohibitive.

Risk transference: Use insurance to have someone else absorb the risk.

Risk avoidance: Don't take actions that are risky.

b) Which involves doing nothing?

Risk acceptance

c) Which involves insurance?

Risk transference involves insurance.

d) Why is insurance not a way to not deal with security protections?

Insurance is not a complete way to deal with security because insurance companies often require customers to install reasonable countermeasures before they provide coverage. Also, insurance companies will give higher deductibles if a firm's protections are inadequate.

e) What is risk avoidance?

Risk avoidance is not taking the action that is risky.

f) Why does risk avoidance not endear IT security to the rest of the firm?

Risk avoidance does not endear IT security to the rest of the firm because even though it is a good viewpoint, it means a company has to forego an innovation that would be attractive had security problems not gotten rid of it.

The Technical Security Architecture

Technical Security Architectures

25. a) What is a firm's technical security architecture?

It will include all of a company's technical countermeasures—including firewalls, hardened hosts, intrusion detection systems, and other tools—and how these countermeasures are organized into a complete system of protection.

b) Why is a technical security architecture needed?

Without a technical security architecture, companies will not be able to create a comprehensive wall with no holes for attackers to walk through.

c) When is the best time to create one?

Before a company begins to create individual countermeasures

d) Why do firms not simply replace their legacy security technologies immediately?

No company can afford to replace its legacy security technologies all at once; replacement must be tiered based on risk analysis.

Principles

26. a) Why is defense in depth important?

Defense in depth is important because every security measure has occasional vulnerabilities; while a vulnerability in one countermeasure is being fixed (or you are unaware of it), the others in the line of defense will remain effective to repel attacks.

b) Distinguish between defense in depth and weakest-link problems.

Defense in depth requires multiple countermeasures to be defeated for an attack to succeed.

Weakest-link analysis is a single countermeasure composed of multiple interdependent components in series that require *all* components to succeed if the countermeasure is to succeed.

c) Why are central security management consoles dangerous?

They are dangerous because they create a single point of vulnerability—an element of the architecture at which an attacker can do a great deal of damage by compromising a single system.

d) Why are they desirable?

Any security architecture whose devices are not controlled centrally might implement inconsistent policies, and many actions taken to thwart an ongoing attack require a systemic response that can work only through a central point of control.

e) Why is it important to minimize the burdens that security places on functional units in the firm?

It is important to do this because to some extent, security almost always reduces productivity and may slow down the pace of innovation by requiring that security issues be addressed before innovations are rolled out. Minimizing security burdens can avoid these losses.

It can also reduce resistance to security.

f) Why do you think it is important to have realistic goals for reducing vulnerabilities?

It is impossible to eliminate all security threats immediately. Having realistic goals will allow a company to focus on the most critical threats.

Elements of a Technical Security Architecture

27. a) Why is border management important?

To stop or at least reduce external attacks

b) Why isn't it a complete security solution?

First, many attackers are inside the firm, and border firewalls do nothing to stop them.

Second, there are many ways for attackers to break through border firewalls and to avoid border firewalls, such as by coming in through an unsecured access point and entering the network directly without passing through the border firewall.

c) Why are remote connections from home especially dangerous?

Individual employees working from their homes and hotel rooms represent a special problem, especially when employees put personal software on their remote access computers. In fact, they often use their own home computers to access corporate sites. The general lack of security discipline among home users can be mitigated by the management of remote access technology.

d) Why are interorganizational systems dangerous?

These are dangerous because in interorganizational systems two companies link some of their IT assets. In interorganizational systems, neither organization can directly enforce security in the other. In fact, they often cannot even learn the details of security in the other company.

e) Why is central security management attractive?

It is able to manage security technologies from a single security management console or at least from relatively few security management consoles that each manages a cluster of security technologies. Centralized security management enforces policies directly on a firm's devices, bringing consistency to security. It also lowers the cost of security management by reducing travel, and allows security management actions to affect devices immediately.

Policy-Driven Implementation

Policies

28. a) What are policies?

Policies are statements of *what* should be done under specific circumstances.

b) Distinguish between policies and implementation.

Policies are statements of what *should* be done; implementation describes the actions that *are* taken to place the policy guidance into operation.

c) Why should policies not specify implementation in detail?

Policies set goals and vision, but they should not wrongly constrain future implementation changes as conditions change (such as technology improvements).

Categories Security Policies

29. a) Distinguish between the corporate security policy and major security policies.

The goal of corporate security policy is to emphasize a firm's commitment to strong security, and it is brief and to the point. Major security policies are specific policies about major concerns and are more detailed than corporate security policies.

b) Distinguish between major security policies and the acceptable use policies.

Major security policies are very detailed and provide guidance to various stakeholders on required or recommended actions. Acceptable use policies provide users with a summary of the key points of various major security policies.

c) What are the purposes of requiring users to sign the AUP?

The signing provides legal protection so that the user cannot say that he or she never knew company policies. Of equal importance, signing creates a sense of ceremony that is memorable. Required signing also emphasizes the company's commitment to IT security.

d) Why are policies for individual countermeasures and resources needed?

Policies for individual countermeasures and resources are needed because major policies are not sufficiently detailed to cover the requirements of a single countermeasure, such as a firewall. The major policies should provide the guidance, while the individual policies describe in detail the implementation of the major policies.

Policy-Writing Teams

30. Why is it important to have corporate teams write policies?

Policies written by corporate teams carry much more weight with employees than policies written only by IT security. They are also more likely to be effective because they are not based on IT security's limited viewpoint.

Implementation Guidance

31. a) Distinguish between standards and guidelines.

Standards are mandatory implementation guidance, while guidelines are discretionary.

b) For guidelines, what is mandatory?

It is mandatory for decision makers to consider guidelines.

c) When are guidelines appropriate?

Guidelines are appropriate in complex and uncertain situations for which rigid standards cannot be specified.

Types of Implementation Guidance

32. a) Distinguish between procedures and processes.

Procedures specify the low-level detailed actions that must be taken by specific employees. Processes are high-level descriptions of what should be done.

b) When would each be used?

Procedures are used to steer a well-defined action, such as the steps required to issue a new employee a password. Processes are used to provide high-level descriptions of what should be done, such as the process of nominating a new product for development.

c) What is the segregation of duties, and what is its purpose?

Segregation of duties requires two or more people to complete a specific act. This prevents one person from acting alone to do harm.

d) When someone requests to take an action that is potentially dangerous, what protections should be put into place?

Limit the number of people who can request an approval.

Limit the number of people who can approve such actions even more.

Ensure the person who approves is not the same as the requestor.

e) Why is it important to enforce mandatory vacations or job rotation?

It is important to enforce mandatory vacations or job rotations because they create a period under which a person cannot take an action, such as implementing an unapproved practice.

f) How do guidelines differ from procedures and processes?

Baselines are checklists of *what* must be done. Procedures and processes specify *how* things should be done.

g) Distinguish between best practices and recommended practices.

Best practices are descriptions of what the best firms in the industry are doing about security. Recommended practices are prescriptive statements about what companies should do and are put together by trade associations and government agencies.

h) Distinguish between resource owners and trustees in terms of accountability.

Owners are accountable for a resource or control. Trustees are delegated the responsibility to implement a resource or control, but are ultimately not held accountable.

i) What can the owner delegate to the trustee?

The owner can delegate the work of implementation of a resource or control to a trustee.

j) What can the owner not delegate to the trustee?

The accountability for the resource cannot be delegated to the trustee.

33. a) Why is ethics unpredictable?

Ethics is unpredictable because different people of good will can make different ethical decisions in the same situation.

b) Why do companies create codes of ethics?

Companies create codes of ethics in order to make ethical decision making more predictable.

c) Why is good ethics important in a firm?

It is important to have good ethics in a firm because good corporations with poor security are poor places to work, and because any lapse in ethics can severely damage a firm's reputation, which can lead to lost sales and profits.

d) To whom do codes of ethics apply?

Codes of ethics apply to everyone, including part-time employees and senior managers.

e) Do senior officers often get an additional code of ethics?

Yes. Most firms have additional codes of ethics for corporate boards and officers.

f) If an employee has an ethical concern, what must he or she do?

If an employee has an ethical concern, he or she must discuss it with his or her superior or the corporate ethics officers.

g) What must an employee do if he or she observes unethical behavior?

If an employee observes unethical behavior, he or she must report it to the corporate ethics officer or to the firm's audit committee.

h) What examples of conflicts of interest were given?

The examples given were preferential dealings with relatives, investing in competitors, and competing with the company while still employed by the company.

i) Why are bribes and kickbacks bad?

Bribes and kickbacks are bad because the perpetrator is likely to act against his or her firm's best interest in order to benefit personally.

j) Distinguish between bribes and kickbacks.

Bribes are monetary gifts to induce an employee to favor a supplier or other party.

Kickbacks are payments made by a supplier to a corporate buyer when a purchase is made.

k) What types of information should an employee not reveal?

An employee should never divulge confidential information, private information, or trade secrets.

Exception Handling

34. a) Why shouldn't exceptions be absolutely forbidden?

Exceptions are almost always necessary. While they should be minimized, they should not be absolutely forbidden.

b) Why is implementation guidance for exception handling necessary?

The implementation of guidance for exception handling is critical because exceptions are inevitable but dangerous, so they must be tightly controlled and documented.

c) What are the first three rules for exceptions?

Only some people should be allowed to request exceptions.

Even fewer people should be allowed to authorize exceptions.

The requestor and approver should be different people.

d) Why would documentation and periodic auditing be important?

The exception must be carefully documented in terms of specifically what was done and who did each action. Without proper documentation, it would be impossible to accurately identify who made the exception. Exceptions above a particular danger level should be brought to the attention of the IT security department and the authorizer's direct manager.

e) What is an example of a dangerous exception that would need to be reported to a manager?

An example of a dangerous exception would be a person approving his or her own budget or expenditures without oversight.

Oversight

35. a) What is oversight?

Oversight is a term for a group of tools for policy enforcement.

b) How is oversight related to policy?

Policy drives oversight. Those involved in oversight must develop oversight plans based upon specific policies.

c) What is promulgation?

Promulgation is telling affected parties about policies underscoring the vision behind specific policies.

d) What is stinging employees?

Stinging employees is setting them up with the opportunity to follow or fail a policy and see what they do.

e) What are its costs and benefits?

The benefits of stinging employees are that it raises awareness and it can be used as a ploy to increase IT security awareness training money. If specific stings are repeated annually, they can also be used to indicate positive trends. Stings can create resentment if not handled well. They can also sometimes be seen as punishment instead of teaching.

f) Is electronic employee monitoring widely done?

Yes.

g) What should you tell employees before your begin monitoring?

Why it is being done.

h) What are security metrics?

Security metrics are measurable indicators of security success.

i) Why is periodic measurement beneficial?

Periodic measurement is beneficial because it indicates whether a company is doing better or worse in implementing its policies.

36. a) What is the purpose of auditing?

The purpose of auditing is to develop opinions on the health of controls, not to find punishable instances of noncompliance.

b) Distinguish between log files and documentation.

Log files is information recorded in database form, and documentation is information recorded on forms or memos.

c) Why is the avoidance of compliance a serious red flag?

The avoidance of compliance indicates a deliberate circumvention of security, which is dangerous.

d) Distinguish between internal and external auditing.

Internal audits are done by an organization on itself; external audits are done by an outside firm.

e) Why is regularly scheduled auditing good?

Periodic auditing is good because it allows a company to compare results over time.

f) Why are unscheduled audits done?

Unscheduled audits are done to try to identify those who are avoiding security without tipping them off of an upcoming audit.

37. a) Why should companies install anonymous protected hotlines?

Companies should install anonymous protected hotlines because oftentimes a coworker is the first person to discover a security violation. Anonymous protected hotlines help to minimize the fear of reprisal amongst informers.

b) Why are anonymity and protection against reprisals importance when hotlines are used?

This is important because some employees may be reluctant to speak for fear of reprisals. When there is an anonymous hotline for people to call, and by guaranteeing protection against reprisals, companies can maximize participation from employees.

c) Why should general employee misbehavior be a concern?

General employee misbehavior should be taken as a red flag because in many cases of serious security violations, the perpetrator had a history of unacceptable overt behavior.

d) What are the three elements in the fraud and abuse triangle?

Opportunity, pressure, and rationalization

e) Give an example of pressure not discussed in the text.

An example of pressure not discussed in the text is peer pressure. An employee may be pressured by fellow employees to bypass security in order to accomplish a team goal.

There is also the pressure of revenge. Getting back at a company for employee mistreatment is often a pressure employees can face after committing misbehavior.

f) Why are rationalizations important?

Rationalizations are important because people do not like to take actions when they consider the actions as bad, making them bad people. They need to rationalize a way to retain their sense of doing the right thing even when it isn't.

g) Give two examples of rationalization not given in the text.

An employee takes customer PII home to work on it in a nonsecure environment because the work environment is too slow or restrictive to get the job done, and the company would rather have the work done sooner than later.

An employee violates a security policy (such as the use of thumb drives) because the company's alternative is not convenient. Again, violating the rule will save the company time and money, as long as nothing happens.

An employee can rationalize that a risky action was done before so it can be done again. A related rationalization is that an employee will think that because everyone else is doing it, it's okay for them to do it.

38. a) What is a vulnerability test?

Vulnerability testing is done to attack the system yourself to see if you can find vulnerabilities before attackers do.

b) Why should you never engage in a vulnerability test without a signed contract?

Because vulnerability attacks look exactly like actual attacks, even if vulnerability testing is in a person's list of written responsibilities, uncontracted vulnerability tests can easily get an IT security professional fired or worse. An attack is still an attack, no matter what the label.

c) What should be in the contract?

The contract should specify what will be done in detail and when it will be done. It must also hold the internal vulnerability blameless if such damage occurs.

d) What should you look for in an external vulnerability testing company?

You should look for expertise, experience, and insurance against possible damage.

e) Why is follow-up needed on recommended fixes?

It is needed to confirm that the fixes were made.

39. Why is it important to sanction violators?

    If violators are not sanctioned, there is no consequence to violating security protocols, and protocols will not be followed by employees.

Governance Frameworks

40. a) What is a governance framework?

    A governance framework specifies how to do planning, implementation, and oversight.

    b) Compare the focus of COSO with that of CobiT.

    COSO focuses on corporate-level governance.

    CobiT focuses on IT governance.

    c) Compare the focus of CobiT with that of the ISO/IEC 27000 family of standards.

    CobiT focuses broadly on the governance of the IT function. The ISO/EIC 27000 family of standards focuses specifically and in detail on IT security.

COSO

41. a) What are the four objectives of COSO?

    Strategic, Operations, Reporting, and Compliance

    b) List COSO's eight components.

    Internal environment, Objective setting, Event identification, Risk assessment, Risk response, Control activities, Information and communication, and Monitoring.

    c) What is the control activity, and why is it important?

    Control activities are the establishment and implementation of the company's policies and procedures to help ensure risk responses are effectively carried out. If control activities are weak, all other control elements are unlikely to be ineffective.

CobiT

42. a) Distinguish between the focuses of COSO and CobiT.

    Where COSO is a general control planning and assessment tool for corporations, CobiT provides a more specific framework for IT governance.

    b) List the four CobiT domains.

    Planning & organization; acquisition & implementation; delivery & support; and monitoring.

    c) How many high-level control objectives does CobiT have?

    34

d) Which domain has the most control objectives?

The delivery and support domain has the most control objectives.

e) How many detailed control objectives does CobiT have?

More than 300

f) Why is CobiT strongly preferred by U.S. IT auditors?

CobiT is strongly preferred by U.S. IT auditors because it was created by the ISACA, the primary professional association for IT auditors in the United States.

The ISO/IEC 27000 Family

43. a) In the 27000 standards family, what is the function of ISO/IEC 27001?

ISO/IEC 27001 specifies how to certify organizations as being compliant with the ISO/IEC 27002. This is important because COSO and CobiT are self-certifying, which can be biased.

b) In the 27000 standards family, what is the function of ISO/IEC 27002?

To specify what should be done to provide protection

c) List the 11 broad areas in 27002.

Security policy

Organization of information security

Asset management

Human resources security

Physical and environmental security

Communications and operations management

Access control

Information systems acquisitions, development, and maintenance

Information security incident management

Business continuity management

Compliance

d) Why is ISO/IEC 27000 certification more attractive to firms than COSO or CobiT certification?

ISO/IEC 27000 is more attractive to firms than COSO or CobiT because 27000 certification is conducted by third-party certifiers, which external parties (companies, in general) value highly.

Conclusion

Synopsis

Thought Questions

1. List the 12 PCI-DSS control objectives. You will have to look this up on the Internet.

   1: Install and maintain a firewall configuration to protect cardholder data
   2: Do not use vendor-supplied defaults for system passwords and other security parameters
   3: Protect stored cardholder data
   4: Encrypt transmission of cardholder data across open, public networks
   5: Use and regularly update anti-virus software
   6: Develop and maintain secure systems and applications
   7: Restrict access to cardholder data by business need-to-know
   8: Assign a unique ID to each person with computer access
   9: Restrict physical access to cardholder data
   10: Track and monitor all access to network resources and cardholder data
   11: Regularly test security systems and processes
   12: Maintain a policy that addresses information security

2. The chapter discussed three ways to view the IT security function—as a police force, as a military organization, and as a loving mother. Name another view and describe why it is good.

   Another view for IT security is that of a family practice doctor. In this view, IT security makes sure that all aspects of a company's security health is addressed via preventative care policies, inoculations (countermeasures) and, when required, medicine or surgery (response). The doctor advises against corporate network promiscuity and dangerous behavior in general, but can prescribe preventative measures to reduce the risk of infection when the temptation of innovation and collaboration is too overwhelming to "just say no." When a company's computer resources do become ill, the IT security doctor takes the necessary steps to address the cause of the problem and assigns rehabilitation methods to get the patient back to full operational strength. By ensuring overall health of the company from the IT security perspective, the doctor enables a stronger and more efficient and effective organization.

   Or one could view the IT security function like that of a priest. Instead of hating the enemy or looking at them with a jaundiced eye, look at the enemy like your "brother". Or view the whole situation as turning evil into good or providing positive for all to follow. Also, it can be seen as educating the user and ultimately giving them the choice to chose. The whole idea should be approached before this whole fact.

3. A company has a resource XYZ. If there is a breach of security, the company may face a fine of $100,000 and pay another $20,000 to clean up the breach. The company believes that an attack is likely to be successful about once in five years. A proposed countermeasure should cut the frequency of occurrence in half. How much should the company be willing to pay for the countermeasure?

	Base Case	With Countermeasure
Single Loss Expectancy	$120,000	$120,000
Annualized Rate of Occurrence	20% (1 in 5 years)	10% (1/2 of base frequency)
Annualized Loss Expectancy	$24,000	$12,000
ALE Reduction for Countermeasure		$12,000

The countermeasure's annualized expected benefit is $12,000. The company should be willing to pay up to $12,000 annually, but no more.

Hands-on Projects

NOTE: Screenshots for individual students will vary.

PROJECT 1

SANS is a great source for information about current IT security trends and training. It also has an excellent collection of security-related white papers to help keep you current. In this project, you are going to look at some important security problems, investigate a security career, read a white paper, and look at one of several ready-made templates designed to help you write a good security policy for your business or organization.

1. Open a Web browser and go to www.ans.org.
2. Click Resources, and Top 20 Critical Controls.
3. Take a screenshot.
4. Click Resources and Additional Resources.
5. Scroll down and click on the link labeled 20 Coolest Careers.
6. Scroll down to the description of a career that interests you.
7. Take a screenshot.
8. Click Resources and Reading Room.
9. Click Top 25 Papers Based on Views.
10. Click on a paper that interests you.
11. Take a screenshot.
12. Return to the SANS.org main page.
13. Click Resources and Security Policy Project.
14. Click the link labeled Email Security Policy.

15. Scroll down and click the link labeled Download Email Policy (Word doc).
16. Open the e-mail policy document you just downloaded.
17. In the Microsoft Word window, press Ctrl-H.
18. Click on the Replace tab.
19. In the Find what text box, enter "<COMPANY NAME>."
20. In the Replace with text box, enter "YourName Company." (Replace YourName with your first and last name.)
21. Click Replace All.
22. Take a screenshot of your new policy.

PROJECT 2

Refog® is a keylogger with an easy-to-use interface. There are monitoring suites available that have more functionality but they can cost $50–$100. Refog is one of the few GUI-based keyloggers that is completely free. Refog can stay completely hidden until you press the specific key sequence to recall the main window. It can automatically load the keylogger and hide it from users. It also monitors programs, websites, chats, and can take screenshots.

Note: You may have to disable your antivirus software to get Refog to work correctly. Some students have reported that their antivirus client automatically disabled Refog because it was labeled as "harmful." It is not harmful. However, this is good news because your antivirus would, in theory, keep someone else from loading a keylogger on your computer without your permission.

1. Download Refog from http://www.refog.com.
2. Click Download for the REFOG Keylogger.
3. Click Download Keylogger Trial Version.
4. Click Save.
5. Select your download folder.
6. If the program doesn't automatically open, browse to your download folder.
7. Right-click refog_keylogger.exe.
8. Select Run as administrator.
9. Click Yes if prompted.
10. Click Install.
11. Click OK, Next, I Agree, Next, Next, Next, Install, and Finish.
12. Click Start, All Programs, REFOG Keylogger, and REFOG Keylogger. (You can also click on the desktop shortcut.)
13. Click Buy Later if prompted.
14. Click Next, Next, Next, Next, Next, and Finish.
15. Click the green Play button to start monitoring.
16. Press the Hide button. (It has a little eye on it.)
17. Click OK. (Note that you will need to run "runrefog," or press Ctrl+Shift+Alt+K to get to the Refog screen again.)
18. Make a Word document or Send yourself an email with the words "YourName, Credit card number, SSN, and Secret Stuff." (Replace "YourName" with your first and last name.)
19. Open a Web browser and visit a couple of websites.

20. Click Start and, in the Run box, type "runrefog" to get the Refog Keylogger window to show again. (You may also be able to press Shift+Ctrl+Alt+K or Ctrl+ Shift+Alt+K to get the program to show again. Students have had mixed success with the keystroke shortcuts.)
21. Click on Program Activity under your username.
22. Take a screenshot.
23. Click on Keystrokes Typed under your username.
24. Take a screenshot.
25. Scroll through the bottom window to see all the words you just typed.
26. Click on Websites Visited.
27. Take a screenshot.
28. Click on the Report button at the top of the screen.
29. Take a screenshot.
30. Click the Clear Logs button.
31. Select Clear all logs.
32. Click Clear, and Yes.
33. Uninstall Refog if you do not want to keep monitoring activity on your computer.

Student screenshots will vary.

Project Thought Questions

1. Where does SANS get all of the information about attacks that are occurring?

   SANS gets information from more than 165,000 IT security professionals at universities, government agencies, corporations, and private consultants.

2. Who contributes to the SANS Reading Room?

   Various security professionals can submit papers to be posted in the SANS Reading Room. You could submit a paper for review if you chose to do so.

3. What type of training or certification does SANS provide?

   SANS provides a wide variety of IT security training including introductory classes, hacker techniques, computer forensics, intrusion detection, wireless security, etc.

4. What does the SANS Top-20 list tell you?

   It tells you about the top 20 most important security concerns for IT security professionals today.

5. Does your employer/spouse/roommate monitor your activities with a keylogger? Are you sure?

   If you work at a publicly traded company, it's highly likely that your employer does monitor your activities. Parents are becoming increasingly aware of monitoring software and are using it at home to watch their children's activities. Spouses worried about infidelity are also interested in monitoring software.

6. What would happen if your employer/spouse/roommate finds out you were using a keylogger to monitor their activities?

   They would likely be upset. While it's legal for an employer to monitor business-related activities, most employees don't like it.

7. Why would someone want to install a keylogger on their own computer?

   A keylogger on your own machine will tell you if anyone else uses your computer and what they do on your computer. If other people have physical access to your computer, they might also try to access your data.

8. How would you know if you had a keylogger on your computer? How would you get rid of it?

   Some anti-virus programs will recognize some of the keyloggers available today. You need to restrict other users from installing software on your machine. You can also look at each process running on your machine to ensure you don't have a rogue process running.

Case Discussion Questions

1. Why was the navigational data on the Japanese Coast Guard vessel not securely deleted?
   It may not have been perceived as a potential source of data loss. The responsible party may not have considered the navigational data when selling the ship. They also may not have considered the national security implications.
2. How could the lost navigational data compromise national security?
   The lost navigational data may be recovered and sold to another nation-state. Another nation may use the navigational data to see when and where the Japanese Coast Guard is utilizing its fleet. It may give the nation an operational advantage if a conflict were to break out.
3. How could the Japanese Coast Guard write an effective data disposal policy?
   The Japanese Coast Guard could write an effective data disposal policy by first enumerating all possible forms of digital data stored on a vessel. This would include navigational data. The policy could then outline how the data are to be securely disposed.
4. Is a self-assessment of effective security policy a good predictor of actual security? Why or why not?
   Not necessarily. It depends on the ability of the evaluator to critically look at his or her own corporate systems without bias. Most people tend to think they are "good" and "honest," but these terms are highly subjective. The same is true of IT security. It's much better to have an external entity assess the effectiveness of an organization's security policy at arm's length.
5. How might broad economic concerns make an organization's information systems less secure?
   Generally speaking, as economic conditions deteriorate, crime tends to increase. This is likely true for cybercrime as well. If broad economic conditions deteriorate, it may be possible that we see a jump in cybercrime.

6. How might widespread adoption of new technology affect an organization's security efforts?
   Rapid and widespread adoption of a new technology may adversely affect an organization's ability to effectively protect itself. The organization's internal IT security staff may not be able to respond quickly enough to the use of new innovations within the organization. These new innovations (e.g., a smart phone) may circumvent existing security measures (e.g., a firewall).

Perspective Questions

1. What was the most surprising thing you learned in this chapter?
   Student answers will differ.
2. What was the most difficult material in this chapter for you?
   Student answers will differ.