Chapter 1

Prepare the Enterprise for Security

Preparing the enterprise for the necessary security changes is the first step of the Enterprise Security Plan (ESP) process. This most crucial step is, perhaps, the easiest to neglect because it involves managing more than technology. Step 1 shows how to build a foundation on the basis of the enterprise's need for security management, how to establish appropriately structured security organization to support the security systems, and how to ensure the entire enterprise is motivated to support security efforts.

Enterprises that are looking to improve their security must build, approve, and publish a security policy. Without a policy, full support for the mission cannot be generated and this support becomes crucial when the project is begun.

Before an enterprise can develop and market specific security projects, a strong base of support for the security mission among both the executive leadership and all end users must be established. This internal effort is not after-the-fact marketing based on telling IT customers what IT has to offer and trying to persuade them to like it. Instead, enterprises must conduct an internal market analysis of IT customers' business objectives to find out what they think they need. Security management then must package the enterprise security program so that it supports those objectives. To accomplish this analysis and packaging of results, IT must understand the needs of users and resource owners,

communicate with them clearly, and motivate them to support the enterprise security concepts.

In effect, marketing is a philosophical approach that infuses many different steps in the ESP process—gaining support from executives and users for the security *program* is the first marketing task. Successfully completing this first step and continuing to reinforce this support greatly enhances the security manager's ability to develop and market specific security projects. Security managers should refer to Step 6 for detailed information on marketing specific security projects.

Implementation of ESP also requires an effective organizational structure. If that structure does not exist, enterprises must develop such an organization in parallel with the ESP efforts. The responsibilities of resource owners, the vice president or director of security, security managers, and security administrators must be spelled out and made clear. This structural development will be discussed shortly.

The Enterprise Security Charter

A single, short document stands at the top of the hierarchy of all security activity within the enterprise: the enterprise security charter. It summarizes the organization's attitude and intent regarding security. It must be clear and concise. The top executive officer and possibly the board of directors should approve it. The enterprise security charter is the justification and approval for everything that is done to improve security. Without it, or with a poor one, every action taken in the name of security will require individual justification and approval, so almost nothing will get done. A policy that is too strong is just as ineffective.

Because perfect security is impossible, the enterprise security charter must define how the company will determine acceptable risk.

Many people need to understand the enterprise security charter:

- The CEO, to approve it
- Executive management, because they must enforce it
- Middle and lower management, to put the business processes in place that create the secure environment

Gaining CEO-level approval and communicating security needs to the staff are two aspects of the marketing skills that organizations require from security managers. In fact, the strong ability to communicate and

convince (that is, market) is now the primary differentiator between security managers and security administrators.

Ideally two to five pages long, the enterprise security charter should do the following:

- Identify the business need for security
- Define the scope of the policy
- List the job titles of the staff responsible for various security functions and their responsibilities
- Describe violation reporting and escalation
- Give the scope of contingency and disaster recovery
- Specify legal or regulatory requirements

On the following pages, the "Model for a Security Charter" provides a template that you can use as a model to create a security charter.

Model for a Security Charter

1. Business need for security

   Example 1. *X Company* owns significant assets in the form of information. Some of these assets lose significant value if they are improperly disclosed. Similar disclosure of other assets could result in significant harm to the corporation. Further, unauthorized changes to the information content of these assets can damage the corporation's ability to perform business. Even preventing authorized access to these assets can do significant harm.

   Example 2. *X Company* management has a fiduciary duty to preserve, improve, and account for company information and information systems, which are recognized as critical and important company assets. Management must ensure that information and information systems are properly protected from a variety of threats, including error, fraud, embezzlement, improper disclosure, sabotage, terrorism, extortion, industrial espionage, privacy violation, service interruption, and natural disaster.

Model for a Security Charter *(continued)*

2. Scope of the policy

   This policy covers all employees, contractors, part-time and temporary workers, and those employed by others to perform work on company premises or granted access to company information or systems. Any person not covered by this policy (for example, visitors) must be supervised by an employee at all times while they are on the company's premises. Information regarding this policy and its implementation must be made available to all affected staff by the *X Company* manager responsible for the performance of that staff member.

3. Job titles and duties of the staff responsible for various security functions

   All employees, contractors, and temporary and part-time workers are responsible for ensuring that company information assets are used only in proper pursuit of the company's business; information is not improperly disclosed, modified, or endangered; and access to company information resources is not made available to any unauthorized person.

   The Director (or Vice President) of Security is responsible for ensuring that appropriate security controls are in existence and in force throughout the company. The Security Administrator is responsible for ensuring that all authentication and authorization management systems are current and accurate. The Security Manager is responsible for determining methods of implementing and enforcing security policies and for advising resource owners on forming appropriate security policies.

   Application design and development staff members are responsible for ensuring that security policies are implemented effectively and efficiently within their applications and that those policies are administered.

   Any employee involved in selecting or purchasing computer system or application software is responsible for ensuring that this policy can be implemented effectively for that system or application.

Model for a Security Charter *(continued)*

X Company management must evaluate all stored information, applications, and information systems to determine the appropriate controls required to protect the information asset on the basis of its criticality to the business, value to *X Company*, and potential value to competitors. These evaluations will be documented and reviewed at least once annually. In addition, the *X Company* central Computer Security Department conducts ongoing reviews of risks to company information and systems.

Each organization unit director assigns one or more managers the responsibility for resource ownership of those information assets housed or managed within their divisions, as determined by the Computer Security Department.

4. Violation reporting and escalation

   Any person covered by this policy is obligated to report apparent violations of this policy to the responsible *X Company* manager. If the violation does not appear to be resolved in a timely manner, the Director of Security must be notified by the person observing the violation.

5. The scope of contingency and disaster recovery

   An inability to make use of information assets is as damaging to *X Company* as destruction of that asset. A plan for continuing business operations while information assets are unusable because of natural or man-made disasters must be documented and tested annually for all information assets identified as critical by the appropriate resource owner. The central Computer Security Department is responsible for assisting in the creation of such plans and in managing the testing process.

6. Legal or regulatory requirements

   Any external requirements that are specific to the company's industry or country should be referenced in this policy.

Building the Security Organization

The organization that administers ESP determines the project's success or failure. Two principles are crucial to success:

- The quality and security of data must be the responsibility of the business unit.
- The distinction between security management and security administration must be clear.

Today, as in the past, IT organizations often assume responsibility for the quality and security of enterprise data. Because they write the security code into some applications, programmers sometimes have responsibility for devising the security policies that govern access to data. This allocation of responsibility is not appropriate. Business unit managers should understand the rules that apply to their data better than anyone else. However, to express those rules in a usable form, they need guidance from managers who specialize in security.

A "best practice" model for an enterprise's security organization is built on defining four roles associated with security. Three of them are security department positions—*security director*, *security manager*, and *security administrator*. These roles are associated with different skill sets, training, responsibilities, and pay scales. The fourth role—*resource owner*—typically is not a full-time job. Resource owners are managers within the lines of business who have been assigned responsibility for setting security policy under the guidance of a security manager. These distinctions are important because, when job descriptions are not defined, crucial tasks are often left undone. For example, resource owners typically focus on customer service. As a result, this priority takes precedence over proper policy enforcement. Emphasizing customer service over security concerns can open holes in the security system. On the other hand, if the security staff members lack resource knowledge, they may define weak policies.

The actual staffing levels for the security organization can vary widely by enterprise. Staff size is determined primarily by the value that an enterprise associates with security, ranging from very high for some government installations to very low in noncompetitive industries, and by the level of success of its investment in automation.

Security Leadership

The person who leads the security department usually works at the level of a director or vice president. In addition to coordinating departmental activities, the director of security must perform some key leadership tasks. The marketing programs described later in this chapter are divided into two sections: upward (to executives) and outward (to business unit managers and other nonexecutive staff). The director has primary responsibility for the upward marketing program. The structure of domains created in the next chapter can have significant implications for staffing levels, job assignments, and even the success probability of ESP. The director of security must understand the implications of that structure before committing to it.

Security Management

Security managers work with the resource owners to ensure that technology is applied properly. Security managers understand how resources can be protected and how the lines of business operate. By applying technology to the business problem of resource security, they can design and implement secure systems. Security managers are advisers and trainers. Most resource owners are managers. To be effective, their advisers in the security organization (the security management staff) must be at a similar management level. Security managers develop the strategies and determine the policies that apply to the business units and the enterprise.

Security Administration

All organizations experience change. Keeping security systems synchronized with that change is imperative. Employee transfers and resignations must be reflected rapidly (ideally, within minutes) in enterprise-wide security authorization databases. Security administrators perform administrative tasks that implement policies, such as assigning authorization levels to individual users.

In a role-based authorization scheme, the constant remapping of individuals to their appropriate corporate roles creates a constant work volume as corporations adapt to new business environments.

Security administration systems based on the older, application security models, rather than role-based or data-centered models, are considerably more taxing to security administrators, as they simply cannot keep up with the level of change in the distributed environment.

For example, under the older model, when an employee is fired, the security staff must find every place that employee is defined and delete his permissions. In a company with 4,000 servers, each housing multiple applications, sometimes hundreds at each server, just finding those authorization records can take weeks. The same effort is needed when someone changes jobs or when a new person is hired. Many companies say that it takes them three weeks to add a new employee because of this work overload. Efforts to automate, or at least simplify, this area are a top concern for security product vendors.

Resource Ownership

Resource owners are not in the security organization; they work in the business departments. An enterprise secures resources to protect their business value. The knowledge of that value, and of changes in that value when the resource is used or updated, must come from the responsible business units. Most resource owners understand business value but have little understanding of the technology used to protect it. After security management has defined a resource classification scheme, the resource owners should determine the classification of each resource. Step 2 of this book presents more information on the classification of resources in detail.

Where Security Reports

Most enterprises categorize security organizations as an IT function—ideally as a chief information officer (CIO) staff function. The relationship between security and information technology must be strong, because IT personnel install and maintain the security staff's primary tools.

Most security organizations use existing staff to meet new demands whenever possible; therefore, they grow without an organizational strategy. As a result, job descriptions have expanded and become more heterogeneous and less uniform in the industry.

Consequently, replacing personnel is now more difficult. Selecting and scheduling training for security staff is also affected. The need to move to distributed security architectures has exacerbated the situation, as organizations have tried unsuccessfully to map significant retraining needs to existing job descriptions.

Using the current technology transition from centralized to distributed paradigms as an opportunity to reorganize the security organization offers the best solution. Enterprises can implement new structures

and new job descriptions as a part of adopting ESP. This transition can also drive structural changes in IT organizations. The traditional "stovepipe" IT organization shown in Figure 1.1 grew new legs as each new technology was added to enterprise environments. Organizations promoted technical specialists to management above their particular area of technology specialization.

New application paradigms such as client/server and Web-based design that distribute application components across many of these traditional applications have forced reassessment of this organizational style. In the stovepipe organization, security typically reports within the data center structure only because the data center is the most security-conscious organization in the enterprise.

A more-effective style of organization is shown in Figure 1.2. This function-oriented organizational structure integrates existing as well as new technologies, and the structure provides clear lines of responsibility for the success of business-oriented IT functions.

It also shows the security staff reporting directly to the CIO. This design is an important reporting structure. Security should be centralized in a single department that can make sure that policies are applied across the enterprise with no gaps between departments, branches, and user domains. In addition, it should report to the CIO rather than a senior-level IT manager, because the IT department is frequently the

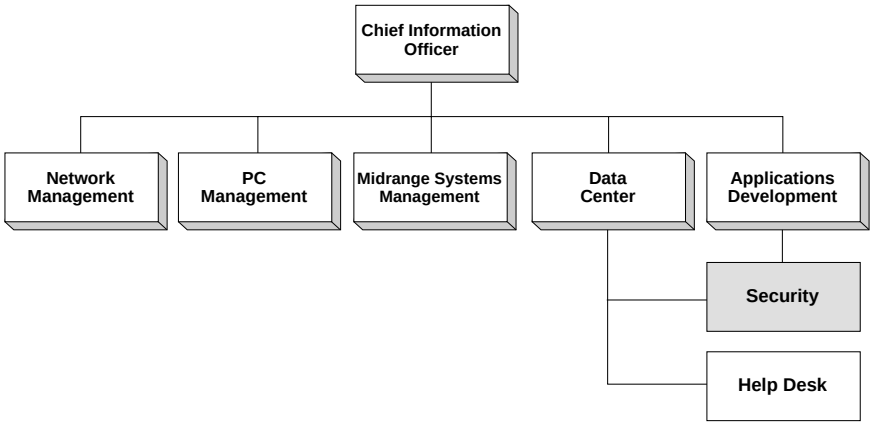

Figure 1.1 Traditional Stovepipe IT Organizational Structure

source of security compromises, so the security staff must be able to bypass IT staff to speak freely and directly to the CIO.

The ideal time to establish a centralized, technology-independent security department is during the transition to a function-oriented organizational structure.

Building Security Job Descriptions

The rate of technological change will continue to accelerate, and the jobs of today might have relatively short lives. Because of this factor, as many security functions as possible—in fact, all computer-support functions—should be automated.

The functions of a pure *security administrator* will soon disappear. As enterprises automate these functions, fully distribute them to their business units, and assimilate them into other job functions related to human resources, security administration will no longer be a separate business discipline. This projected change has significant implications for organizations that are now outsourcing their local administration functions. They may be locked into long-term outsourcing contracts at a time when they need to absorb these services into their business units.

Security management will continue as a required business discipline, but the number of practitioners will diminish as resource ownership becomes a more accepted part of management responsibility outside the security organization.

As with jobs, job descriptions developed now will have a shorter life than their predecessors and will continue to change as the technology

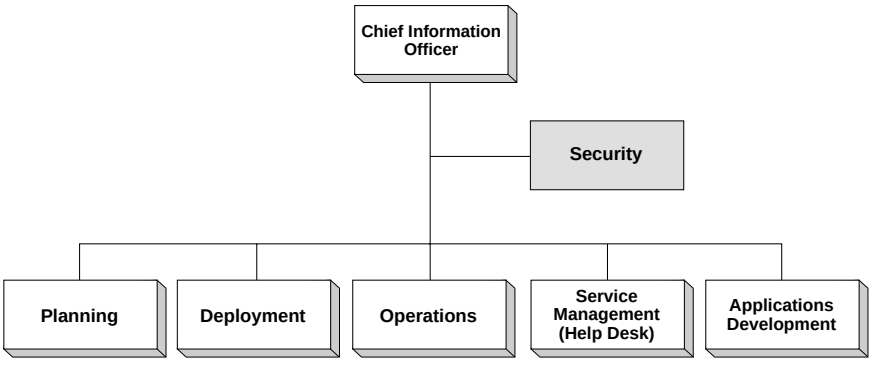

Figure 1.2 Function-Oriented Organizational Structure

changes. Thus, management should shorten the time invested in creating these descriptions. The templates that follow provide sample job descriptions.

Note

These templates aim to be comprehensive. Most organizations will select portions of the templates; very few will use them in their entirety.

Sample Templates of Security Job Descriptions

Director (or Vice President) of Security

Summary: Leads company in adopting and accepting appropriate security procedures. Manages department that ensures appropriate security controls are in existence and in force throughout the company.

Duties and Responsibilities:

- Works with executive management to determine acceptable levels of risk for the company.
- Works with business unit management to ensure that resource owner responsibilities are accepted and appropriately staffed.
- Consults with Information Technology management to facilitate selection and use of realistic enforcement mechanisms.
- Helps peer managers understand and respond to security audit failures reported by internal and external auditing departments.
- Supervises security management staff and security administration staff.
- Reviews and approves security policies and resource classification scheme.
- Presents security status and project status to executive management and the Board of Directors.

Director (or Vice President) of Security *(continued)*

Required skills, experience, and competencies: Bachelor's degree plus six years of information security experience or a minimum of eight years of information security experience. Ability to relate business requirements and risks to technology implementation for security-related issues. Knowledge of risk assessment procedures, policy formation, role-based authorization methodologies, authentication technologies, and security attack pathologies. Strong communications and public-speaking abilities. Demonstrated skills in budget management, personnel management, and contention management. Knowledge of current company business functions and operations.

Additional desired qualifications: CISSP or CISA preferred. Knowledge of distributed systems technology and client/server application design is beneficial. Second-level management experience strongly preferred.

Security Manager

Summary: Determines methods of implementing and enforcing security policies. Advises resource owners on forming appropriate security policies.

Duties and responsibilities:

- Identifies existence of securable resources and helps business unit management select appropriate resource owner.
- Works with resource owners in business units to determine appropriate security policies for securable resources.
- Consults with Information Technology Technical Services staff to evaluate, select, install, and configure hardware and software systems that provide appropriate security functions.
- Helps resource owners and Information Technology staff understand and respond to security audit failures reported by internal and external auditing departments. May review operational logs and event console activity to determine cause of security-related events or to identify potential security-related events.

Security Manager *(continued)*

- Advises security administration staff on normal and exception processing of security authorization requests.
- Documents security policies; maintains resource classification scheme; and presents information on security status, project status, and security training to audiences from top executive level to field staff as appropriate.

Required skills, experience, and competencies: Bachelor's degree plus three years of information security experience or a minimum of five years of information security experience. Ability to relate business requirements and risks to technology implementation for security-related issues. Knowledge of risk assessment procedures, policy formation, role-based authorization methodologies, authentication technologies, and security attack pathologies. Strong communications and public-speaking abilities.

Additional desired qualifications: CISSP or CISA preferred. Knowledge of distributed systems technology and client/server application design is beneficial. Experience as an IT auditor is highly valuable.

Security Administrator

Summary: Ensures the currency and accuracy of all authentication and authorization management systems.

Duties and responsibilities:

- Accepts requests for change in authentication and authorization systems. Validates requestor and determines authorization of requestor.
- Modifies authentication and authorization systems to match change requests.
- Helps security managers determine "reasonableness" of policies requested by resource owners. Defines process for implementing new policies.
- Identifies unauthorized changes to authentication and authorization systems and notifies Director of Security.

Security Administrator *(continued)*

Required skills, experience, and competencies: Two-year college degree and two years' experience in office administration environment. Ability to see patterns and identify exceptions. Strong telephone and communications skills.

Additional desired qualifications: Knowledge of security procedures and technology. Understanding of audit processes.

Centralizing and Decentralizing Security Functions

Frequently, security administration is centrally managed and located. Many other systems management disciplines are becoming more centralized, as skill shortages and economies of scale dominate organizational decisions. Security administration does not follow this pattern. Instead, the trend is toward further distribution of the responsibility to lines of business. This trend will accelerate as vendors deliver better tools.

The authority exercised by a security administrator in assigning roles and rights to individuals is a direct expression of the policies set by resource owners under the guidance of, and perhaps as executed by, the security manager. Basic security and audit rules require that some degree of separation exist within this triumvirate. As previously stated, the resource owners should be local to—that is, report within—the business units. As long as this condition is met, either but not both security administration or security management can also report within the business unit.

Consistent policy is also an audit requirement. Because security management staff manages policy, the security managers must be centralized. A new generation of tools that provide consistent policy enforcement through a delegation of administration mechanism makes possible the distribution of security administration.

Unfortunately, many organizations have achieved fully distributed security administration without the tools to enforce consistent policy and reduce administrative duplication. As a result, the least-secure system at the least-secure site is the hacker's port of entry into the entire enterprise's computing environment.

Centralized security management maintains effectiveness by controlling tools that provide delegation management and through internal audit procedures. The auditing process comprises three separate activities:

- Static policy audit
- Real-time event detection
- Attack simulation

Chapter 9 describes the tools to support all these activities.

Marketing the Mission within the Enterprise

Unconvinced that the success of a security program hinges on buy-in from affected groups, the security organization at many companies pays little attention to managing its relationship and image with executives and other end users. However, without proper marketing, the best-designed security program is doomed to failure; and if the program does not have the proper support from its customers, specific security projects are destined to fail before they are even developed.

Computer security competes with other business issues for attention and investment within an enterprise. At the same time, advances in technology increase the threat to computer security and augment the need for investment in better protection. Executives and other end users are primarily concerned with running their business efficiently and growing it where they can. To get them to buy into an overall security plan, IT must illustrate how failure in security will threaten their ability to run their businesses. To do so, IT should use the results of any security audit to demonstrate the dangers that currently exist and their possible impact on specific business units.

By applying marketing strategies, the security organization can communicate the nature of this relationship upward to executive management and outward to the rest of the enterprise staff—thereby speeding acceptance and compliance in the end-user communities and easing the work of security staff. Chapter 11 shows how this upward marketing was done recently at a large company.

Security managers typically do not have a lot of experience or training in marketing. Because marketing is crucial to implementing ESP, this chapter includes considerable detail on applying marketing strategies to establish a firm base of support for security concepts.

Developing a Security Marketing Program

Marketing efforts must be scaled to achievable levels. The information provided here gives a perspective on the role and application of marketing strategies to security management. Because of resource constraints, IT will probably not be able to develop perfect, detailed security marketing programs. However, to be successful, the security program must consider, plan, and implement practical upward and outward security marketing programs.

A typical marketing program includes the following:

- *Market identification*—To identify the target audiences of marketing programs at a detailed level
- *Market research and analysis*—To understand the business issues, needs, and focus of the target audience
- *Product packaging*—To define the overall security plan and the related messages that communicate benefits in a way that can be accepted by the audience
- *Marketing communications*—To create and deliver ongoing messages about security

Ideally, marketing involves effective two-way communication. The security manager must identify the audience, understand their needs, package solutions, and then communicate the solution.

Marketing begins in the first step of ESP and continues through the last. The first step of ESP illustrates how to plan upward and outward marketing programs designed to establish enterprise support for security efforts, and it begins implementing the upward marketing program. In the last step of the ESP process, when the security projects to be implemented have been determined and the messages that must be delivered are understood, the plans for the upward and outward marketing programs can be completed. The rest of this chapter explains how to use basic marketing tasks to market ESP within the enterprise. First, the basic tasks, which apply to both the outward and upward audiences, are discussed. Then the chapter examines how to tailor the tasks to each of these audiences. Table 1.1 shows the differences in marketing to the upward and outward audiences.

Market Identification. During this first step in the ESP process, security management needs to identify the audiences that must accept or may interfere with implementing a security system. End users, business unit managers, IT managers, and enterprise executives must accept the

security systems in varying degrees, and the types of people that constitute these markets are substantially different.

Market Research and Analysis. Market research involves collecting background and historical information, typically through surveys. Market research should result in an internal working document that consolidates all the research.

The security organization gathers some marketing information in the course of developing the enterprise security charter, identifying the target audiences, and implementing Steps 2 through 4 of ESP. The rest of this research involves additional effort, such as interviewing the identified market participants, which include executives and operational managers.

Security management should use the material gathered as part of the market identification phase to build a set of surveys—one for the upward market and one for the outward market. These surveys should become the basis for an ongoing survey program on target-audience satisfaction. The surveys should test the assumptions used during market identification, determine current attitudes toward IT security, and test the acceptability of potential solutions to known problems. Asking participants the following questions is appropriate in a formal or informal survey:

- What is your position?
- What is your background?
- What are your security concerns?
- How have you responded in the past to security initiatives?
- What other programs have elicited your positive reaction?
- What other programs are currently competing for funding and attention?

Good systems analysts often have the skills to ask the right questions and document requirements. In addition, enterprise help desk employees frequently are skilled in gathering information on end-user perceptions. Because of their involvement in managing service-level agreements, they may also have experience in conducting surveys. IT should interview help desk employees about their perspective on security issues and should solicit their help in gathering survey information.

One critical person to identify is a high-level sponsor for the marketing program. Security is an enterprise and executive concern. Perfect marketing will not erase all objections to an effective security imple-

Table 1.1 Different Approaches in Marketing to Upward and Outward Audiences

Marketing Task	Both Audiences	Upward Audience	Outward Audience
Identifying the target audiences.		Specify the individual executives who are the key players in making decisions about investments in security.	Identify groups most affected by the security program. Audience is usually too large to specify individuals, except in the case of business unit managers in smaller organizations; the target of outward marketing is all nonexecutive staff.
Analyzing markets.	Get information from audiences to develop marketing program.	Conduct interviews; use surveys when the target audience is large.	Use surveys. Develop the market analysis on the basis of the groups most affected by the program. Identify key players at this level who can affect group response.
	Determine what marketing methodology has succeeded in the past.	Determine how executives have reacted to other, similar nonsecurity plans, how much they supported past security initiatives, and their personal perspectives on security.	Determine groups' pattern of behavior in relation to security; if no history of security plans exists, determine behavior toward other types of projects and proposals.
		Identify nonsecurity programs that are competing for resources.	Determine potential or perceived threats and benefits.

Table 1.1 Different Approaches in Marketing to Upward and Outward Audiences *(Continued)*

Marketing Task	Both Audiences	Upward Audience	Outward Audience
Developing product packages.	Bundle palatable functions with less-palatable functions to please the end user while advancing security.	Develop product packages that reduce risk to reasonable levels.	Develop product packages that improve, or at least do not interfere with, business units' ability to do business.
Developing marketing communications.	Develop ongoing communication. Develop a marketing communication plan. Include marketing materials and a production schedule for the presentations.	A schedule for follow-up meetings with executives.	A certification process. A schedule for measuring yourself and the effectiveness of your program.
	Develop message media: Presentations and supporting materials.		White papers (tailored to different outward marketing audiences). Briefing documents. Brochures. Posters. Desk cards. Telephone stick-ons. E-mail. Internal mail.

mentation. Executive fiat should be a last resort, but the threat implicit in the existence of executive sponsorship makes the marketing efforts more effective.

An internal working document that consolidates the information gathered from the market research should be produced. Because some of the information is sensitive, it should be used for internal security management purposes only. As an internal document, it is less likely to cause controversy. This report should include the results of the research

and be organized on the basis of the security organization's strengths, weaknesses, opportunities, and threats (commonly known as SWOT analysis). Separate sections on the strengths and weaknesses of the security organization's political position within the enterprise (its friends, its enemies) should be included, along with the most significant threats to successful implementation and the greatest opportunities for maximizing success.

A history of support for security within the enterprise and a reputation for excellent end-user support are typical strengths. The broad implementation of a recently developed client/server application system without security considerations is a common weakness. Opportunities are the benefits that could result from the proper security implementation. Threats may include political issues for some enterprises, which is one reason this document is an internal working document only.

Product Packaging. When security management has identified the market and researched its concerns and needs, the next step is to package the overall security plan so that it attracts support and minimizes opposition. Most likely, the audience has expressed diverse and conflicting needs and concerns. In marketing the overall mission, common issues and goals should be paramount. The mission should include broad, general suggestions to satisfy conflicting needs; these concepts should be disseminated clearly in the marketing communication efforts.

Security management should use market research to identify two or three security issues that are critical to all the business units in the enterprise, emphasizing these common concerns in presentations, briefing documents, white papers, posters, newsletter articles, and e-mail. Concentration on similarities rather than differences will facilitate buy-in.

Unfortunately, business units may have critical needs that conflict with the needs of other units; to successfully market the security program to the enterprise, these conflicts cannot be ignored. Security management should develop suggestions for addressing these conflicts in the overall security plan and promote them through marketing communications. However, not every conflict should get equal time and attention. Only issues critical to the unit's success should be given special attention. The other issues can be addressed and resolved as various security projects are developed, marketed, and implemented.

Marketing Communications. An effective marketing program requires a marketing communication plan to describe what, how, and when to communicate to the audience. The plan should identify the

basic messages to communicate. The basic messages are only the simple statements that the affected audience must understand to believe in the importance of the project.

Communication is the process of imparting information in such a way that another person willingly listens to and absorbs what is being said; skilled communication is the core of successful marketing. Security management needs to communicate the essence of the enterprise security mission so that the audience will listen to, absorb, and act on the information.

Messages should be simple! Whenever two people in different knowledge domains try to communicate, the communication must take a simple form. Therefore, low-level detail should be omitted. Messages should contain only words and phrases that others can immediately understand and accept. Again, clarity and simplicity are the goal.

The marketing should take the concept of the overall security program, add the common concerns and needs the market research identified, and develop from these some relatively simple statements that communicate the ways the security program will alleviate or mitigate those concerns. It should then discuss any conflicting needs and solutions that require mention in this early marketing strategy. These statements and the words in them should be short—no more than 10 to 15 words per statement, with words of no more than three syllables whenever possible.

Because this is a presentation put on by a security expert trying to communicate with people who are focused on business, the presenter must learn to communicate in business terms.

A marketing communication plan includes messages for each target audience and media for delivering the messages. The following media could be useful in conveying the marketing message, depending on the audience:

- Presentations
- Security briefing documents
- Brochures
- White papers
- Posters
- Newsletter articles
- E-mail

Memos are not appropriate for delivery of marketing messages. While they can create a paper trail of marketing activities, in many organizations, employees are flooded by memos and tend to pay little attention to them, if they read them at all.

Presentations are the most effective marketing medium. Security project presentations should include war stories (tales of what happened to companies that did not do what is being proposed). These stories are located in newspapers and archives, as well as through Internet searches.

This marketing communication effort will help to build end users' understanding of how the IT security staff is meeting the differing, even conflicting, needs of the various audiences. It also provides an opportunity to communicate the professionalism, and business and service orientations, of the IT security staff. Professional trainers are the ideal people to develop and implement this communication plan unless security management has access to a professional marketing department.

Marketing Upward

Simply getting signatures on the enterprise security charter is not sufficient to ensure that upper management will make the proper investment in security. In fact, the security organization needs an ongoing, two-way communication program with upper management to accomplish the following:

- Anticipate changing business needs
- Evaluate the perceived effectiveness of current programs
- Inform executives of security management actions designed to meet existing needs, the methods used to accomplish tasks, the projected cost, and the importance of projects

Identifying the Targets of Upward Marketing. In upward marketing programs for midsize and large enterprises, security management must be specific about who the target audience is—the key players in making decisions about investments in security. They should know the five or ten individual executives who have the power to approve or reject a project.

The largest of enterprises may have as many as 100 key players. Gathering information for this number of individuals is unreasonable. In this case, it is preferable to employ the same techniques for targeting this audience as were used for targeting an outward audience.

Analyzing Upward Markets. The following information is needed concerning all the identified executives:

- How they reacted to security initiatives in the past—whether they gave effective support and promoted such projects to other executives or just gave vocal support but failed to provide any substantial enactment
- How they reacted to similar (in terms of scope, purpose, and intent) *nonsecurity* initiatives that affected their departments in the past—their general attitudes on change

The Executives' Personal Perspectives on Security. In addition, knowing the following information about the executives can be very helpful:

- Where their focus is
- What they see as the direction of the business
- What they see as the needs of the business
- How they would like to see the enterprise grow and flourish

At the same time, noting their personal interests is potentially useful. This information might aid in developing the communication plan.

In some cases, IT can garner this information through interviews. Understanding how the executives feel about security as a process and a priority within the organization is important.

Gathering data on other nonsecurity programs competing for the same dollars, time, and staff as the security program is equally important. Success will hinge on knowing which other projects might compete for resources. By identifying the competition, security management can find ways to make the programs work together and perhaps augment each other or develop methods to keep the programs from interfering with each other's resource requirements.

Developing Product Packages for Upward Markets. Security managers should use the approach described earlier of packaging the security mission to both upward and outward markets.

Developing Upward Marketing Communications. Although the product packaging will be the same for both upward and outward markets, the messages employed to market the package will differ for each market.

Creating Marketing Messages for the Upward Audience. Enterprise executives require that the security functions reduce risk to reasonable levels; therefore, marketing messages to upper management should speak to this concern. The marketing messages should say nothing about firewalls or most other technical issues.

The plan may well install firewalls and additional servers and add some administrative overhead to manage those elements. All of that information goes in the proposal but not necessarily in the marketing messages. It certainly does not belong in marketing communication messages for the upward audience.

The Internet may be the one exception in keeping language nontechnical, since most computer users, and even nonusers, are familiar with this technology. Generally, executives do not have the technical background to appreciate these issues or they are just too busy to want that level of detail. They are more likely to want to see the bottom line—how security affects business. The marketing messages for a branch office security program might be as follows:

- Allow dispersed employees to work from home without endangering corporate resources.
- Stop as soon as possible all unsecured access that endangers corporate resources through branch office facilities.

The sequence is important in these statements: first it enables beneficial practices, and then it disables harmful practices. Putting the "stop" statement first would be a serious mistake, because the executives would perceive that they are supposed to stop a practice that provides a business function.

Using Media in Upward Marketing Communications. Typically, security management communicates to upper management through white papers and memos. However, those media are the two worst for marketing to this audience. A white paper provides detailed technical analysis, and executives will not read it. The number of memos to executives in most organizations is overwhelming. While memos do provide an audit trail, most quickly end up in the circular file.

The best medium to use in communicating with executives is a presentation. If the project lead—generally, the security manager—does not have good presentation skills, he should enlist someone who does. The security manager does not have to be the one to give the security presentation to upper management. Another possible presenter is the person to whom the security manager reports. Either way, the material

must be presented effectively. To make it effective, the presenter should hand out copies of the presentation materials to the executives at the beginning of the presentation. Table 1.2 shows a scheduling grid for marketing.

Along with war stories, the presenter should include alternative approaches and their impacts in the presentation to executives. When presenting the security plan to upper management, the speaker should provide multiple solutions. Upper management's role in the organization is to decide how to solve problems, frequently by choosing among several options. Although the best solution may seem obvious to the presenter, upper management should receive all reasonable solutions. The presenter certainly can give recommendations regarding the preferred solutions. However, because upper management's support for the overall philosophy of the security program is crucial, providing alternative approaches and an impact analysis for the alternatives is a necessary part of the marketing strategy.

Scheduling Production. The marketing communication plan should include the production schedule for:

- The presentation itself
- Any supporting material
- Any subsequent meetings with the executives about the plan
- It is important to get on the calendar of the executives so that they can be prepared. This way they know the presentation is coming and they can plan to attend.

Security management should plan follow-up meetings with the executives to discuss the following:

- Their reactions to the plan
- How they would like to see this type of material presented in the future
- Their decisions about the plan

Marketing Outward

For security to be effective, technology users—including end users and their managers—must buy into the program. Thus, security management must develop an internal marketing program for nonexecutive staff.

Table 1.2 A Scheduling Grid for Marketing

	11/23	11/24	11/25
Presentation	X		
Follow-up meeting			X
Expected approval			

Marketing is a tool for influencing people. The need to market does not detract from the legitimate authority of the security staff. Real security depends upon the willingness of end users to follow proper procedures and appropriately protect resources. The investment in marketing generates a return through lower training and enforcement costs. Willing participation is more efficient (and more secure) than grudging compliance.

Identifying the Targets of Outward Marketing. In outward marketing, market identification cannot consist of descriptions of individuals, except business unit managers in smaller organizations. In other cases, the organization is simply too large to target individuals. Instead, security management should develop a list of affected organizational groups and staff.

Analyzing Outward Markets. Once the affected population has been determined, security management bases the market analysis, as well as the entire outward marketing program, on that population.

It is useful to determine whether the groups identified as the target audience have a pattern of behavior regarding security. If they do, what is it and why? Understanding why previous programs failed or succeeded is important. What were the reactions of management and other staff to the program?

If the enterprise has no history of security programs, other types of projects and proposals make good substitutes. Has the organization shown itself to be receptive to change? Can this acceptance be demonstrated by listing specific things that have happened over the course of the last two to three years that showed that the organization was receptive and able to deal with some level of change? This change might have involved new technologies.

Security management should identify key players at this level if program information is available from the recent past. Those key players become influencers who either support or undermine any program in the organization. When they have been key players in technology

upgrading, they can be extremely important to the success or failure of the security mission. Identifying the pattern of behavior and the key players is crucial.

Having identified the patterns, security management should consider the threats and benefits this program creates. Individuals react first to threat or a perception of threat. Therefore, security management must determine how these groups will perceive the security program in terms of threat. Then, from the perspective of the target audience, the positive aspects of the security program should be identified.

Finally, security management should use any theme or historical precedent or pattern of past behavior to communicate with these groups. What have they been receptive to, what caused them to take action or make commitments, and what is the most effective way to communicate with them?

Developing Product Packages for Outward Markets. Product packaging for upward and outward markets is the same.

Developing Outward Marketing Communications. Outward marketing augments the traditional task of training. Traditional training involves educating staff on security procedures and their importance. Although training is a necessary part of any security implementation, it is usually merely a presentation of information.

Outward marketing, on the other hand, is a two-way communication process of researching, analyzing, convincing, influencing, and presenting information. Using the term "outward marketing" instead of "training" is important, because "outward marketing" stresses that communications is one of the most important skills for a security management professional.

Creating Messages for the Outward Audience. As in upward marketing, in outward marketing, marketing messages must be kept straightforward, simple, and generally nontechnical. Business unit managers do not want security to interfere with their ability to do business; when speaking to these managers, marketing messages should address this concern. The following are examples of marketing messages for the outward audience:

- Compliance with security policy is a condition of employment.
- The central security department exists to help you understand and comply with policy.

- Through technology, your competition can access your data and hackers can access your customers' data. Security protects them.
- The last of these three messages is directed specifically toward managers.

Using Media in Outward Marketing Communications. In outward marketing, an 8- to 10-page white paper that outlines the background material and justification for the security plan may be appropriate. But because separate audiences have different needs, the audiences should be addressed separately through white papers composed specifically for them.

Here again, presentations are important. These presentations should include war stories. And, again, memos should be avoided.

Security managers can serve the more detailed needs of nonexecutives by creating an extended briefing document. This document, which is generally 10 to 15 pages long, is used in employee and management training. It becomes a standard part of the new employee training program and a part of the message delivery process for every security project. The briefing document must be kept up-to-date, be written in plain English, and have everything in it that a first-line manager needs to know about security. It needs to contain basic policy statements, including how to assign resources to various security classifications. It should have all the basic information that a line manager needs to make decisions regarding security:

- How to handle a problem—when to escalate, how to escalate, who to escalate to, and what to expect as a result of that escalation
- The basic components of the enterprise security policy—why security is important, how all the security issues are going to be handled, and who is responsible for what in every step along the way

The marketing communication plan for outward marketing also needs other materials. The importance of security must be continuously communicated to the target audience. Any or all of the following tools and techniques can be useful in this endeavor:

- Posters that are suitable for hanging in cubicles
- Desk cards
- Telephone stick-ons that help people remember that they must pay attention to security

- E-mail (perhaps humorous)
- Internal mail that communicates a single coherent concept

Such regular communication can increase expenses, but the increases may be minimal. Security managers can use desktop publishing, desktop color printers, and quick-run color printing at local print shops to build inexpensive communication vehicles.

As in upward marketing, a marketing communication plan that includes a production schedule is key. In circumstances where certification is appropriate, it should be part of the plan and the schedule. Certification is the process by which first-line managers certify they have read a specific component of the marketing communication deliverables. Frequently, the briefing document includes a sign-off form. As the document is updated each year, all managers must review it and certify that they did so by signing the form. The appropriateness of this process is entirely a cultural issue.

Evaluating the Security Program. The last piece of the outward marketing communication plan is a schedule for measuring the effectiveness of the marketing communication program. It is desirable to have a way of auditing and measuring compliance with the policies implemented. Therefore, the marketing program should express the expected compliance levels, including reasonable time periods in which to expect compliance and to achieve the plan's objectives. Month by month, the security manager records the expected compliance levels as a result of the marketing communication plan. And again, managers should use marketing tools to remind end users to comply with policy.

This chapter developed an enterprise security charter that strengthens and clarifies the security organizational structure. It also shows how to market the security plan both to senior management who approve the investment of resources and to the users. The next chapter examines ways to organize corporate resources into domains so that security managers can establish the exact security needs to address.