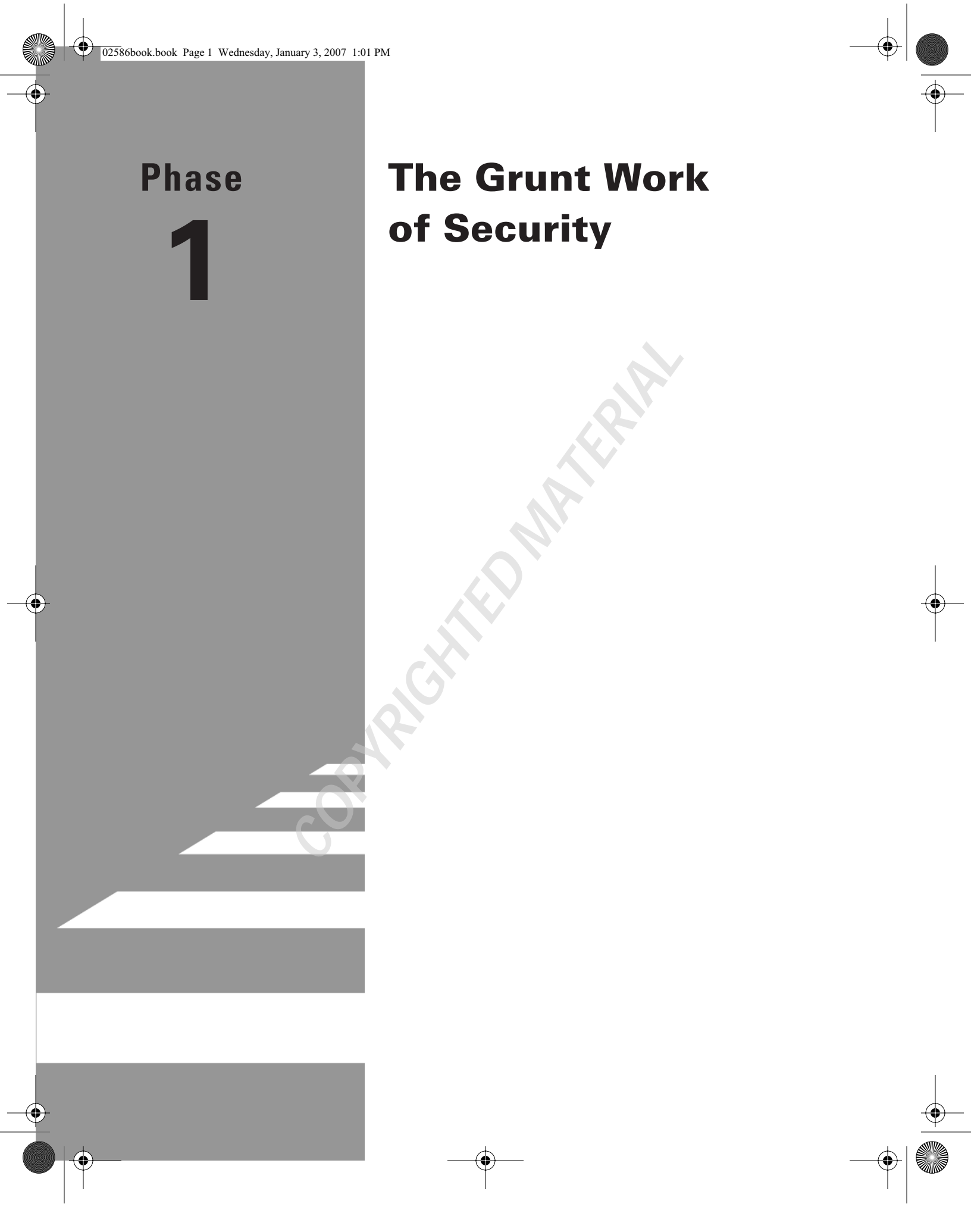


# Phase 1

# The Grunt Work of Security

COPYRIGHTED MATERIAL





There is an old saying that success is doing what's right at the right time. While the individual who created this quote may not have been thinking of security in particular, security professionals can most certainly learn from this saying. Security is about doing the right thing at the right time. Before you can run a password-cracking tool, perform penetration tests, or fire up a vulnerability scanner, you must cover some basic groundwork. That grunt work is the subject of this first phase.

The groundwork of security requires that you know what is worth securing. Companies don't have unlimited funds, so a big part of the security process is finding what is most critical to the organization and focusing your security efforts on these assets. Finding what's critical is only the first step. You will next need to write a policy that matches up to your findings. Is that enough? No. Policies have no meaning if users don't know they exist. That's where user awareness comes in. Finally, you can have great ideas but unless they are written down they have little value. In other words, documentation is important in everything you do. These are the tasks that we will examine in this phase of the security process. Let's get started by performing a basic risk assessment.



The tasks in this phase map to Domain 5 objectives in the CompTIA Security+ exam (<http://certification.comptia.org/security/default.aspx>).

## Task 1.1: Performing an Initial Risk Assessment

Risk assessment can be achieved by one of two methods: qualitative or quantitative. *Qualitative* assessment does not attempt to assign dollar values to components of the risk analysis. It ranks the seriousness of threats and sensitivity of assets into grades or classes, such as low, medium, or high.

*Quantitative* assessment deals with numbers and dollar amounts. It attempts to assign a cost (monetary value) to the elements of risk assessment and to the assets and threats of a risk analysis. The quantitative assessment process involves these three steps:

1. Estimate potential losses—Single Loss Expectance = Asset Value × Exposure Factor.

2. Conduct a threat analysis—The goal here is to estimate the Annual Rate of Occurrence (ARO). This numeric value represents how many times the event is expected to happen in one year.
3. Determine Annual Loss Expectancy (ALE)—This formula is calculated as follows:  $ALE = \text{Single Loss Expectancy (SLE)} \times \text{Annualized Rate of Occurrence (ARO)}$ .

The goal of this task is to conduct these three steps of the quantitative risk assessment process.

## Scenario

You have been asked to perform a quantitative risk assessment for a small startup web graphics firm.

## Scope of Task

### Duration

This task should take about 30 minutes.

### Setup

For this task you need access to a pen and paper. In real life, assessments require knowledge of assets, an analysis of threats and team of people to help in understanding what is truly important to the organization. These people should be from key departments of the company to get more rounded view. I think in this case, to make this differ from the Equipment Used section below, we need to also discuss some of the personal info that you would use. That is, do you need to interview anybody? Do you need other information—company assets, etc.—to make an informed risk assessment plan?

### Caveat

In real life, risk assessment is a complex process that is usually done with the aid of software tools that perform all the calculations.

## Procedure

In this task, you will learn how to perform a quantitative risk assessment.

### Equipment Used

For this task you must have:

- Paper
- Pen or pencil

## 4 Phase 1 • The Grunt Work of Security

**Details**

This task will introduce you to the risk assessment process. This is a critical step in the security process since an organization must determine what is most critical and apply cost-effective countermeasures to protect those assets. A quantitative risk assessment attempts to put dollar amounts on those risks, which makes it a valuable tool when working with management to justify the purchase of countermeasures.

**Estimating Potential Loss**

Your first step in the risk assessment process is to estimate potential loss. This is performed by multiplying the asset value times the exposure factor. The asset value is what the asset is worth. The exposure factor is the cost of the asset lost or damaged in one single attack. For example, if the threat was a computer virus and the asset was a server valued at \$32,000 with an exposure factor of .25, the formula would be as follows: Single Loss Expectance = Asset Value  $\times$  Exposure Factor, or  $\$32,000 \times .25 = \$8,000$ . The SLE, which represents what one computer virus attack would cost, is \$8,000.

Now that you have a better idea of how the process works, take a look at Table 1.1.1, which shows a variety of threats and their corresponding exposure factors.

With a list of exposure values, you are now ready to calculate the SLE for some common systems. These are shown in Table 1.1.2. Complete the table using the information provided by Table 1.1.1.



Answers to SLE values in Table 1.1.2 can be found in Table 1.1.4

**TABLE 1.1** Threat Level and Exposure Factor (EF)

Threat Level or Vulnerability	Exposure Value
5=STOLEN or COMPROMISED DATA	.90
4=HARDWARE FAILURE	.25
3=VIRUS or MALWARE	.50
2=DoS ATTACK	.25
1=SHORT-TERM OUTAGE	.05

**TABLE 1.2** Calculating Single Loss Expectancies (SLE)

IT Asset Name	Asset Value	Threat	EV	SLE Value
Symantec's Enterprise Firewall	\$25,000	2	.25	
WAN Circuits (3 remote call centers)	\$25,000	4	.25	
Cisco 6500 Switch/Router	\$160,000	4	.25	
LAN Connectivity	\$100,000	4	.25	
LAN VPN Connectivity	\$25,000	4	.25	
Dell Servers—Pentium 4's	\$32,000	2	.25	
Linux Servers	\$20,000	2	.25	
End-User Workstations (HW & SW)	\$300,000	1	.05	
Microsoft SQL Server	\$20,000	3	.50	
Oracle SQL Data (Customer Data)	\$500,000	5	.90	

### Conducting a Threat Analysis

With the calculations completed for SLE, the next step is to determine the ARO. This is the average number of times you might expect this to happen in a year. Here's an example: Galveston typically gets hit with a hurricane at least once every ten years. Therefore, the chance for a hurricane is .10.

Take a moment to review Table 1.1.3. You will need to complete this table based on the following information:

**Stolen equipment** Based on information provided by actuary tables, there is the possibility that your organization will lose equipment, or have its equipment compromised, once in a five-year period.

**Hardware failure** By examining past failure rates of equipment, you have determined that it has happened twice in the last eight years.

**Computer virus** Historical data shows that the company has been seriously affected only once in the last two years.

## 6 Phase 1 • The Grunt Work of Security

**DoS attack** Your research has shown that the average company in your field is affected by denial of service (DoS) up to three times every 12 years.

**Short-term outage** Trouble tickets from the help desk indicate that three-fourths of all trouble tickets in one year are related to some type of outage.

**TABLE 1.3** Annualized Rate of Occurrence (ARO)

Threat Level or Vulnerability	ARO Value
5=STOLEN or COMPROMISED DATA	.2
4=HARDWARE FAILURE	.25
3=VIRUS or MALWARE	.5
2=DoS ATTACK	.25
1=SHORT-TERM OUTAGE	.75

### Determining the Annual Loss Expectancy

Armed with SLE values and ARO values, you are now ready to complete the final steps of the risk assessment process:

1. To calculate ALE you will use the following formula:  $ALE = \text{Single Loss Expectancy (SLE)} \times \text{Annualized Rate of Occurrence (ARO)}$ . As an example, if the SLE is \$1,000 and the ARO is .25, the formula would be  $\$1000 \times .25 = \$250$  ALE.
2. Using the information gathered earlier in this task, complete Table 1.1.4.



Given the risk calculated for Table 1.1.5, note that the customer's database has the largest ALE.

The answers for Table 1.1.4 can be found in Table 1.1.5.

**TABLE 1.4** Calculating Single Loss Expectancies

IT Asset Name	SLE Value	Threat	ARO Value	ALE Value
Symantec's Enterprise Firewall	\$6,250	2=DoS ATTACK	.25	
WAN Circuits (3 remote call centers)	\$6,250	4=HARDWARE FAILURE	.25	

**TABLE 1.4** Calculating Single Loss Expectancies (*continued*)

IT Asset Name	SLE Value	Threat	ARO Value	ALE Value
Cisco 6500 Switch/Router	\$40,000	4=HARDWARE FAILURE	.25	
LAN Connectivity	\$25,000	4=HARDWARE FAILURE	.25	
LAN VPN Connectivity	\$6,250	4=HARDWARE FAILURE	.25	
Dell Servers—Pentium 4's	\$8,000	2=DoS ATTACK	.25	
Linux Servers	\$5,000	2=DoS ATTACK	.25	
End-User Workstations (HW & SW)	\$15,000	1=SHORT-TERM OUTAGE	.75	
Microsoft SQL Server	\$10,000	3=VIRUS or MALWARE	.5	
Oracle SQL Data (Customer Data)	\$450,000	5=STOLEN or COMPROMISED DATA	.2	

**TABLE 1.5** Calculating Single Loss Expectancies Results

IT Asset Name	SLE Value	Threat	ARO Value	ALE Value
Symantec's Enterprise Firewall	\$6,250	2=DoS ATTACK	.25	\$1,562.50
WAN Circuits (3 remote call centers)	\$6,250	4=HARDWARE FAILURE	.25	\$1,562.50
Cisco 6500 Switch/Router	\$40,000	4=HARDWARE FAILURE	.25	\$10,000
LAN Connectivity	\$25,000	4=HARDWARE FAILURE	.25	\$6,250
LAN VPN Connectivity	\$6,250	4=HARDWARE FAILURE	.25	\$1,562.50
Dell Servers—Pentium 4's	\$8,000	2=DoS ATTACK	.25	\$2,000
Linux Servers	\$5,000	2=DoS ATTACK	.25	\$1,250
End-User Workstations (HW & SW)	\$15,000	1=SHORT-TERM OUTAGE	.75	\$11,250

## 8 Phase 1 • The Grunt Work of Security

**TABLE 1.5** Calculating Single Loss Expectancies Results (*continued*)

IT Asset Name	SLE Value	Threat	ARO Value	ALE Value
Microsoft SQL Server	\$10,000	3=VIRUS or MALWARE	.5	5,000
Oracle SQL Data (Customer Data)	\$450,000	5=STOLEN or COMPROMISED DATA	.2	\$90,000

### Criteria for Completion

You have completed this task when you have calculated the SLEs, ALEs, and AROs for a range of IT products.

## Task 1.2: Determining Which Security Policy Is Most Important

Security policies are the lifeblood of any organization. Once you've performed a risk assessment, you can begin to lock in these findings in the security policy. The policy should spell out what should be protected, how it should be protected, and what value it has to senior management. Be sure to specify these concerns in *written* documents. You must also verify that the policies comply with all federal, state, and local laws.

Policies play such an important role because they put everyone on the same page and make it clear where senior management stands on specific issues. Policies help define how security is perceived by those within an organization. Policies must flow from the *top* of the organization because senior management is ultimately responsible.

### Scenario

Management was pleased with your recent risk assessment, and you have been asked to make some basic security policy recommendations. Any given company only has a limited amount of funds so your real task is to determine when the funds you can spend on security will have the most benefit. The risk assessment process discussed previously is one way to place a value to assets and to the threats those assets face.

## Scope of Task

### Duration

This task should take about 10 minutes.

### Setup

For this task you only need read through the scenario and determine what you think is the best solution.

### Caveat

Well-written policies should spell out who's responsible for security, what needs to be protected, and what's an acceptable level of risk. When writing policies you should make sure that what is written is something that users can really do. For example you may want policy to state that users must select complex passwords but will the operating system support that feature?

## Procedure

In this task, you will learn to write and assess the security of an organization and determine where to start in the security policy process.

### Equipment Used

For this task you must have:

- A pen or pencil

### Details

This task will introduce you to basic policy design and help you understand the importance of specific policies to the organization. The following organization and company profile will be used to complete this task.

### Company Profile

Your company has all of its future potential pinned to the fact that it has several unique products in FDA-approved trials. If the products are approved for use, the company will be able to obtain additional funding. Recently, a sensitive internal document was found posted on the Internet. The company is worried that some of this information may have ended up in the hands of a competitor. If key proprietary information was leaked, it could endanger the future of the company.

### Company Overview

Your talks with senior management revealed the following. The company is betting everything on the success of these products. Most of its key employees have been stolen away from competing firms. These employees were originally attracted by the promise of huge stock options. HR has all these records and they have to keep track of any payouts if they occur.

The company has been lucky—venture capital has poured in. All of this capital has been invested in research and development (R&D). Once a design is pulled together, the company locks in the documentation. It doesn't actually build the product in the United States; a subsidiary in South Korea assembles the design. The finished product returns to the United States for final tests, and then the product is submitted for FDA trials.

Because the company is new and poised for growth, the rented office and lab space is full. There are several entrances to the building, and people can come and go through any of them. Employees often work from home. Employees connect to the office from home via virtual private networks (VPNs). They have been required to sign an acceptable-use policy that specifies for what purposes they can use the network and its resources.

There is no full-time network administrator; those responsibilities fall on a research assistant that has experience managing systems in a college environment (but not in a high-security environment). The network consists of one large local area network (LAN) connected to the Internet through a firewall appliance—except for the VPNs, where the firewall still has its factory-default configuration. Employees must use two-factor authentication to log into local computers, and laptops have biometric authentication.

Because a storm last year wiped out a competitor, the company called in a disaster recovery expert and backup policies were developed. It also contracted with a service bureau for its backup services, should the network go down because of a disaster. This led the company to set up policy templates for other major areas, but policies have not been completed.

### Policy Development Overview

Once an organization has decided to develop security policies, the question that usually comes to mind is “What's next?” The best place to start is to frame the policies within some type of existing framework.

Two examples of such a framework are ISO 17799 and BS7799. BS7799 is a recognized standard that breaks security policy into ten categories. These include the following:

**Business continuity planning** Addresses business continuity and disaster recovery

**System access control** Addresses control of information, protection of network resources, and the ability to detect unauthorized access

**System development and maintenance** Addresses the protections of application data and the safeguards associated with confidentiality, integrity, and availability of operational systems

**Physical and environmental security** Addresses the physical protection of assets and the prevention of theft

**Compliance** Addresses the controls used to prevent the breach of any federal, state, or local law

## Task 1.2: Determining Which Security Policy Is Most Important 11

**Personal security** Addresses the protection of individuals and the protection from human error, theft, fraud, or misuse of facilities

**Security organization** Addresses the need to manage information within the company

**Computer and network management** Addresses the need to minimize the risk of system failure and protect network systems

**Asset classification and control** Addresses the need to protect company assets

**Security policy** Addresses the need for adequate policies to maintain security

Based on the information provided in the Details section of this task and the BS7799 categories, you should complete Table 1.2.1. In the table you will find a listing for each of the BS7799 categories. Beside each category, list the level of importance of each of these items. Use the following scale:

- 1—Low importance, should not be an immediate concern
- 2—Medium importance, requires attention
- 3—High importance, should be a priority

Answers for Table 1.2.1 can be found in Table 1.2.2.

**TABLE 1.6** Policy Action Items

Category	Level of Concern
Business Continuity Planning	
System Access Control	
System Development and Maintenance	
Physical and Environmental Security	
Compliance	
Personal Security	
Security Organization	
Computer and Network Management	
Asset Classification and Control	
Security Policy	



Answers will vary but should be similar to what is found in Table 1.2.2.

**TABLE 1.7** Policy Action Items

Category	Level of Concern
Business Continuity Planning	1
System Access Control	3
System Development and Maintenance	1
Physical and Environmental Security	3
Compliance	3
Personal Security	3
Security Organization	2
Computer and Network Management	2
Asset Classification and Control	3
Security Policy	2



The SANS Institute has a great resource that can be used to develop specific policies. You'll find it at <http://www.sans.org/resources/policies/>. Best of all, it's free!

## Criteria for Completion

You have completed this task when you have completed Table 1.2.1 determined which security concerns are most important.



## Task 1.3: Establishing a User Awareness Program

Policies are not enough to protect an organization. Employees must develop user awareness programs so that other employees know about specific policies and are trained to carry out actions specified in security policies. The overall process to accomplish this task is usually referred to as security education, training, and awareness (SETA).

Take, for example, a policy dictating that employees should access the Internet for business use only. Management can dictate this as a policy, but how are end users going to know? That's where employee awareness comes in. Employee awareness could include asking employees to sign an acceptable-use statement when they are hired; it might also include periodic training, and could even include warning banners that are displayed each time an employee accesses the Internet. Awareness is about making sure that employees know security policies exist, what they are, and what their purpose is.

### Scenario

Your company has established basic security policies based on BS7799 standards. They have now turned to you for help in developing an awareness program.

### Scope of Task

#### Duration

This task should take about 10 minutes.

#### Setup

For this task you will need to have performed a risk assessment and developed policies. Once policies are in place you can then start the training process.

#### Caveat

A study conducted by Ernst and Young found that more than 70 percent of companies polled failed to list security awareness and training as top company initiatives. These same companies reported that 72 percent of them had been affected by infected e-mails and computer viruses. Good training and awareness would have reduced these numbers. You can read more about this at: [http://www.ey.com/global/download.nsf/UK/Survey\\_-\\_Global\\_Information\\_Security\\_04/\\$file/EY\\_GISS\\_%202004\\_EYG.pdf](http://www.ey.com/global/download.nsf/UK/Survey_-_Global_Information_Security_04/$file/EY_GISS_%202004_EYG.pdf).

## Procedure

In this task, you will be required to categorize and design a basic user awareness program.

### Equipment Used

For this task you must have:

- A pen or pencil

### Details

This task will provide you with details on how a security awareness program is developed and give you the opportunity to develop key portions of the procedure.

### User Awareness

It is sad but true that one of the least implemented and yet most useful parts of a security policy is user awareness. Security must be kept at the forefront of employees' minds for a security program to work. This overall program is typically referred to as security education, training, and awareness (SETA).

SETA is the responsibility of the chief security officer and consists of three elements: education, training, and awareness. While these items can be categorized in many ways, The National Institute of Standards and Technology (NIST) has developed some benchmark procedures that perform such services. One such document is NIST 800-12. Table 1.3.1 contains the information found in that document.

Based on the information provided in Table 1.3.1, identify the following items shown in Table 1.3.2 and place them into the proper category of education, training, or awareness.

**TABLE 1.8** Security Awareness, Training, and Education

Item	Education	Training	Awareness
Trinkets printed with security slogans			
Newsletters			
Security + certification			
Bachelor's degree in Computer Security			
SANS 3- day seminar			
CISSP certification			
T-shirts provided for good security practices			

**TABLE 1.8** Security Awareness, Training, and Education *(continued)*

Item	Education	Training	Awareness
1- day security seminar at the local college			
Quarterly security quiz with prize			
2 -year degree in Associates of Security			

Based on Table 1.3.2, which of the items do you feel would be most useful to keep security awareness at the forefront of users' minds as they work day to day?

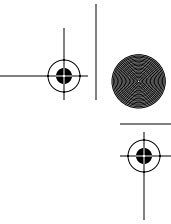


Answers may vary but may include anything that keeps people focused on security, such as mousepads printed with security slogans, coffee cups, T-shirts, pens, or other objects that would be used during the workday.

Answers to questions in Table 1.3.2 can be seen in Table 1.3.3.

**TABLE 1.9** Security Awareness, Training, and Education

Item	Education	Training	Awareness
Trinkets printed with security slogans			X
Newsletters			X
Security + certification		X	
Bachelor's degree in Computer Security	X		
SANS 3- day seminar		X	
CISSP certification		X	
T-shirts provided for good security practices			X
1- day security seminar at the local college		X	
Quarterly security quiz with prize			X
2- year degree in Associates of Security	X		



## Criteria for Completion

You have completed this task when you have analyzed the items needed for a SETA program and determined which are most useful for a user awareness program.

# Task 1.4: Reviewing a Physical Security Checklist

The value of physical security cannot be overstated. Physical security is also the oldest aspect of security. Even in ancient times, physical security was a primary concern of those who had assets to protect. Just consider the entire concept of castles, walls, and moats. While primitive, these controls were clearly designed to delay attackers. Physical security is a vital component of any overall security program. Without physical security you can have no security at all. Any time someone can touch an asset, there is a good chance they can control it. Usually, when you think of physical security items such as locks, doors, and guards come to mind, but physical security is also about employees. What can they bring to work—iPods, USB thumb drives, camera phones? Even these items can pose a threat to security. One good way to start building effective physical security is by creating a checklist of items employees are allowed (or not allowed) to bring with them to work.

## Scenario

Your organization may soon be subject to a security audit. Your manager would like to get ahead of this process and have you investigate the current physical security practices.

## Scope of Task

### Duration

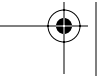
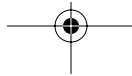
This task should take about 20 minutes.

### Setup

In real life security audits don't happen in a void. They occur with the support and under the direction of senior management. End users may or may not be informed ahead of time. Either way you would most like have a memo or letter of authorization authorizing you to perform such activities.

### Caveat

Physical security is sometimes overlooked in the mostly logical world of IT. That can have catastrophic consequences.



## Procedure

In this task, you will learn how to go through a physical security checklist.

### Equipment Used

For this task you must have:

- A pen or pencil

### Details

This task will step you through a physical security checklist. It will highlight the value of physical security. Physical security is different from the security controls focused on hackers and crackers. Logical security addresses controls designed to prevent disclosure, denial, or alteration of information. Both are important and, when combined, a holistic view of security can be adopted.

### Reviewing a Physical Security Checklist

One of the best ways to check the physical security of your network infrastructure is to conduct a physical security review.

Use Table 1.4.1 to measure your company's level of security. For each item that is present, note a score of 1. If the control is not present, rate that item a 0.

**TABLE 1.10** Physical Security Checklist

Item	Score (Yes=1 / No=0)
Is there perimeter security?	
Is a security fence is present?	
Is exterior lighting used to deter intruders?	
Is CCTV being used?	
Are exterior doors secured?	
Is access control in use at building entries?	
Are dumpsters in an area where the public can access?	
Are sensitive items shredded or destroyed before being discarded?	

## 18 Phase 1 • The Grunt Work of Security

**TABLE 1.10** Physical Security Checklist (*continued*)

Item	Score (Yes=1 / No=0)
Do interior areas have access control?	
Are the servers in a secure location?	
Does the server room have protection on all six sides?	
Is access to the server room controlled?	
Are network cables the lines protected from tapping, cutting, or damage from digging?	
Are there “deadman” doors at each of the entrances to prevent piggybacking?	
Is old media degaussed, shredded, and destroyed?	
Are confidential documents marked?	
Is visitor access controlled?	
Are UPS, surge protectors, and generators user?	
Are visitor badges different than regular employees?	
Are end-users allowed uncontrolled access to USB ports or CD/DVD burners?	
<b>Total Score</b>	

After filling in Table 1.4.1, add up the score and compute the total:

- A score of 18 or higher is good.
- A score of 16 to 17 is fair.
- A score of 15 or below is poor.



In real life, physical security takes much more work. This rating system doesn't take into account the issue of reliability or assurance but should give you an idea of the types of items you will want to examine.

## Criteria for Completion

You have completed this task when you have reviewed a physical security checklist.

# Task 1.5: Understanding the Value of Documents

Identifying the value of the documents your company has is an important task. Documents have value—some more than others. You might lose a quote from a vendor for the new server you have requested and have little to worry about. But what if you lost a client list that had credit card and other personal information? Clearly, some documents and the information they contain are more valuable than others. Factors that impact organizations and how they handle information include:

Government regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act hold corporations accountable for the privacy, integrity, and security of information.

- Industry is more dependent than ever on the Internet. Many organizations use it for critical and sensitive communications.
- Identity theft and loss of personal information is at an all-time reported high.

These issues are affecting businesses and placing an increased emphasis on how they handle information.

## Scenario

Your organization recently lost a laptop with sensitive company information. The data on the drive was not encrypted. This has started a big debate at work on the value of documentation and data. Your boss has asked you to investigate a system that could be used to value documents and the information they hold. You will be asked to make recommendations at the next staff meeting.

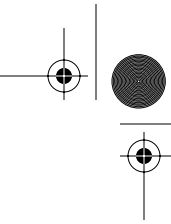
## Scope of Task

### Duration

This task should take about 15 minutes.

### Setup

For this task you need a group of people from throughout the organization working with you. While you may be an expert on IT systems, you may not know the value of documents or



## 20 Phase 1 • The Grunt Work of Security

information in the HR department. Gathering data from different people in different departments will provide better results.

### **Caveat**

Documents and data, whether in paper or electronic form, need adequate protection. Sometimes this fact is grossly overlooked.

### **Procedure**

In this task, you will learn how to categorize and place a value on documents and data.

### **Equipment Used**

For this task you must have:

- A pen or pencil

### **Details**

This task will introduce you to some of the methods of information classification. You will be required to take specific documents and determine which category they belong in. This will allow you to specify the level of protection needed.

### **Information Classification**

All companies must take steps to protect the integrity and confidentiality of their information assets. An information classification system is one way to do this. Information classification helps identify sensitive information and can assist an organization in meeting government regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), and other regulatory requirements. Such a system also helps prevent identity theft.

Two systems are primarily used to classify information:

- Governmental classification
- Commercial classification

This task will look at commercial classification, which is broken into the following four categories:

**Confidential** This is the most sensitive rating. This is the information that keeps a company competitive. This information is for internal use, and its release or alteration could seriously affect or damage the corporation.

**Private** This category of restricted information is considered of a personal nature and might include medical records or human resource information.

**Sensitive** This information requires controls to prevent its release to unauthorized parties. Damage could result from its loss of confidentiality or its loss of integrity.

**Public** Disclosure or release of information in this category would cause no damage to the corporation.



By using the categories as described in Table 1.5.1, place the following items in Table 1.5.2 into their proper categories.

After completing Table 1.5.1, compare it to the results shown in Table 1.5.2.

**TABLE 1.11** Commercial Information Classification

Item	Classification
Employee Medical Records	
Trade Secrets	
Prototypes of Next Year's Products	
Schedule of Public Events	
Customer Database	
Pending Sales Events	
Salesmen Call List	
Monthly Customer Profit Reports	
Router Configuration	
Network Diagrams and Schematics	

**TABLE 1.12** Commercial Information Classification

Item	Classification
Employee Medical Records	Private
Trade Secrets	Confidential
Prototypes of Next Year's Products	Confidential
Schedule of Public Events	Public
Customer Database	Confidential
Pending Sales Events	Sensitive
Salesmen Call List	Sensitive

## 22 Phase 1 • The Grunt Work of Security

**TABLE 1.12** Commercial Information Classification (*continued*)

Item	Classification
Monthly Customer Profit Reports	Confidential
Router Configuration	Sensitive
Network Diagrams and Schematics	Sensitive

Did the answers agree with what you felt was the adequate level of protection? Were you more conservative than the answers shown in Table 1.5.2? Although your answers may vary from the chart, the goal is to see how certain documents, data, and information have more value than others. Part of the job of a security professional is to determine that value and work with management to develop adequate protection.



Computer security is not just about networks. It also encompasses the technological and managerial procedures applied to protect the confidentiality, integrity, and availability of information.

## Criteria for Completion

You have completed this task when you have placed the various documents into their proper categories.