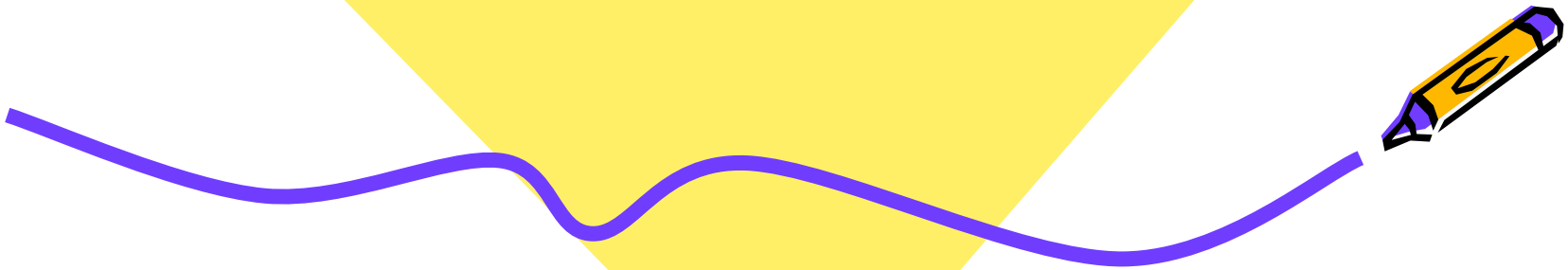
CHAPTER SIX: ADMINISTERING SECURITY & ORGANIZATIONAL SECURITY POLICIES



1. INTRODUCTION

Introduction:

- Security controls are classified as
  i. Technical
  ii. Administrative and
  iii. physical
- Thus Security is a combination of technical, administrative, and physical controls.
  - *What good is a firewall if there is no power to run it?*
  - *How effective is a public key infrastructure if someone can walk off with the certificate server? And*
  - *Why have elaborate access control mechanisms if your employee e-mails a sensitive document to a competitor?*
- The administrative and physical controls may be less glamorous than the technical ones, but they are surely as important.

1. INTRODUCTION Cont…

We consider administrative and physical aspects. We look at four related areas:

1. **Planning.**
   - *What advance preparation and study lets us know that our implementation meets our security needs for today and tomorrow?*
2. **Risk analysis.**
   - How do we weigh the benefits of controls against their costs, and how do we justify any controls?
3. **Policy.**
   - How do we establish a framework to see that our computer security needs continue to be met?
4. **Physical control;**
   - What aspects of the computing environment have an impact on security?

These four areas are just as important to achieving security as are the latest firewall or coding practice.

2. Security Planning Cont..

A security plan

- *is a document that describes how an organization will address its security needs.*
- *The plan is subject to periodic review and revision as the organization's security needs change.*
- is an official record of current security practices, plus a blueprint for orderly change to improve those practices.

- By following the plan,
  - developers and users can measure the effect of proposed changes, leading eventually to further improvements.
  - The impact of the security plan is important, too.
    - A carefully written plan, supported by management, notifies employees that security is important to management (and therefore to everyone).
    - Thus, the security plan has to have the appropriate content and produce the desired effects.

2. Security Planning Cont..

- In this section we study how to define and implement a security plan.
- We focus on three aspects of writing a security plan:
  - what it should contain,
  - who writes it, and
  - how to obtain support for it.
- Then, we address two specific cases of security plans:
  - business continuity plans,
    - to ensure that an organization continues to function in spite of a computer security incident, and
  - incident response plans,
    - to organize activity to deal with the crisis of an incident.
- **Contents of a Security Plan**

2. Security Planning Cont..

❑ Contents of a Security Plan

- A security plan identifies and organizes the security activities for a computing system.
  - The plan is both a description of the current situation and a plan for improvement.
- Every security plan must address seven issues.
  1. policy,
     - indicating the goals of a computer security effort and the willingness of the people involved to work to achieve those goals
  2. current state,
     - describing the status of security at the time of the plan
  3. requirements,
     - recommending ways to meet the security goals
  4. recommended controls,
     - mapping controls to the vulnerabilities identified in the policy and requirements
  5. accountability,
     - describing who is responsible for each security activity

2. Security Planning Cont..

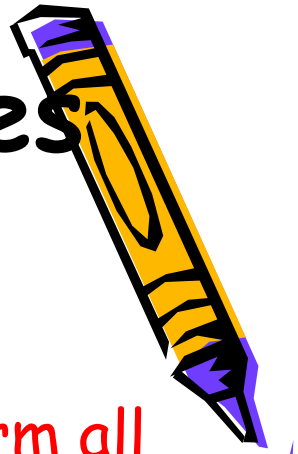
- **Contents of a Security Plan**
  6. timetable,
     - identifying when different security functions are to be done
  7. continuing attention,
     - specifying a structure for periodically updating the security plan
- NB
  - There are many approaches to creating and updating a security plan.
    - Some organizations have a formal, defined security planning process,
      - much as they might have a defined and accepted development or maintenance process.
  - Others look to security professionals for guidance on how to perform security planning.

Organizational Security Policies

1.0 Introduction

- A key element of any organization's security planning is an effective security policy.
- A security policy must answer three questions:
  - i. *Who should be allowed access?*
  - ii. *To what system and organizational resources should access be allowed?*
  - iii. *What types of access should each user be allowed for each resource?*
- A security plan must state the *organization's policy on security.*

Organizational Security Policies



- Definition
  - A security policy
    - is a high-level management document to inform all users of the goals of and constraints on using a system.
      - A policy document is written in broad enough terms that it does not change frequently.
      - The information security policy is the foundation upon which all protection efforts are built.
  - is a high-level statement of purpose and intent.
    - Initially, you might think that all policies would be the same:
      - to prevent security breaches.
        - But in fact the policy is one of the most difficult sections to write well.

Organizational Security Policies/definition cont…

The policy statement should specify the following:

1. **The organization's goals on security.**
   - *For example,*
     - *Should the system:*
       - *protect data from leakage to outsiders,*
       - *protect against loss of data due to physical disaster,*
       - *protect the data's integrity, or*
       - *protect against loss of business when computing resources fail?*
       - *What is the higher priority: serving customers or securing data?*
2. **Where the responsibility for security lies.**
   - *For example,*
     - *should the responsibility rest with a small computer security group(ICT), with each employee, or with relevant managers?*
3. **The organization's commitment to security.**
   - *For example,*
     - *who provides security support for staff, and where does security fit into the organization's structure?*

Organizational Security Policies/definition cont…..

- Security policy
  - should be a visible representation of priorities of the entire organization,
    - CLEARLY stating underlying assumptions that drive security activities.
  - should articulate senior management's decisions regarding security as well as asserting management's commitment to security.
    - To be effective,
      - the policy must be understood by everyone as the product of a directive from an authoritative and influential person at the top of the organization.
        - People sometimes issue other documents, called procedures or guidelines, to define how the policy translates into specific actions and controls.

2. Purpose of Security policy

Security policies are used for several purposes, including the following:

i. *recognizing sensitive information assets*
ii. *clarifying security responsibilities*
iii. *promoting awareness for existing employees*
iv. *guiding new employees*

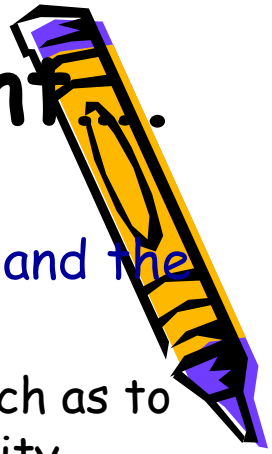
3. Audience of Security policy cont...

A security policy addresses several different audiences with different expectations.

- That is, each group *users*, *owners*, and *beneficiaries* uses the security policy in important but different ways.

1. ***Users***
   - Users legitimately expect a certain degree of confidentiality, integrity, and continuous availability in the computing resources provided to them.
     - Although the degree varies with the situation, a security policy should reaffirm a commitment to this requirement for service.
   - Users also need to know and appreciate what is considered acceptable use of their computers, data, and programs.
     - For users, a security policy should define acceptable use.

3. Audience of Security policy cont…



1. **Owners**
   - Each piece of computing equipment is owned by someone, and the owner may not be a system user.
     - An owner provides the equipment to users for a purpose, such as to further education, support commerce, or enhance productivity.
       - A security policy should also reflect the expectations and needs of owners.

3. **Beneficiaries**
   - A business has paying customers or clients;
     - *they are beneficiaries of the products and services offered by that business.*
   - At the same time, the general public may benefit in several ways: as a source of employment or by provision of infrastructure.
     - For example
       - a university's customers include its students and faculty;
       - other beneficiaries include the immediate community (which can take advantage of lectures and wifi on campus) and often the world population (enriched by the results of research and service).

3. Audience of Security policy cont….

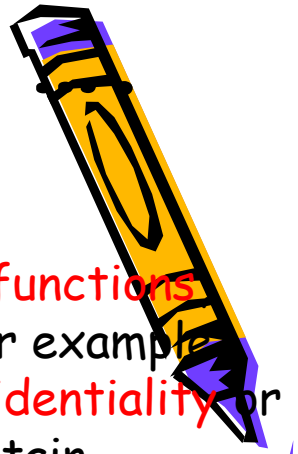
3. Beneficiaries cont…

- To varying degrees, these beneficiaries depend, directly or indirectly, on the existence of or access to computers, their data and programs, and their computational power. For this set of beneficiaries, continuity and integrity of computing are very important. Thus, the interests of beneficiaries of a system must be reflected in the system's security policy.

Balance Among All Parties

- A security policy must relate to the **needs of users, owners, and beneficiaries.** Unfortunately, the needs of these groups may conflict.
- A beneficiary might require immediate access to data, but owners or users might not want to bear the expense or inconvenience of providing access at all hours. Continuous availability may be a goal for users, but that goal is inconsistent with a need to perform preventive or emergency maintenance.
- Thus, the security policy must balance the priorities of all affected communities.

4. Contents of Security policy



1. the purpose of the computing system,

- The policy should state the purpose of the organization's security functions reflecting the requirements of beneficiaries, users, and owners. For example, the policy may state that the system will "protect customers' confidentiality or preserve a trust relationship," "ensure continual usability," or "maintain profitability."
- **There are typically three to five goals, such as:**
  - i. *Promote efficient business operation.*
  - ii. *Facilitate sharing of information throughout the organization.*
  - iii. *Safeguard business and personal information.*
  - iv. *Ensure that accurate information is available to support business processes.*
  - v. *Ensure a safe and productive place to work.*
  - vi. *Comply with applicable laws and regulations.*

The security goals should be related to the overall goal or nature of the organization. It is important that the system's purpose be stated clearly and completely because subsequent sections of the policy will relate back to these goals, making the policy a goal-driven product.

4. Contents of Security policy

2. Protected Resources

- A risk analysis will have identified the assets that are to be protected. These assets should be listed in the policy, in the sense that the policy lays out which items it addresses.
  - **For example,**
    - *will the policy apply to all computers or only to those on the network?*
    - *Will it apply to all data or only to client or management data?*
    - *Will security be provided to all programs or only the ones that interact with customers?*
    - *If the degree of protection varies from one service, product, or data type to another, the policy should state the differences.*
      - **For example,**
        - *data that uniquely identify clients may be protected more carefully than the names of cities in which clients reside.*

4. Contents of Security policy cont

3. Nature of the Protection

- The asset list tells us what should be protected.
- The policy should also indicate who should have access to the protected items.
- It may also indicate how that access will be ensured and how unauthorized people will be denied access.

❑ All the mechanisms described are at your disposal in deciding which controls should protect which objects. In particular, the security policy should state what degree of protection should be provided to which kinds of resources.

5.Characteristics of a Good Security Policy

Characteristics of a Good Security Policy

- If a security policy is written poorly, it cannot guide the developers and users in providing appropriate security mechanisms to protect important assets. Certain characteristics make a security policy a good one.

1. **Coverage**
   - A security policy must be comprehensive:
     - It must either apply to or explicitly exclude all possible situations. Furthermore, a security policy may not be updated as each new situation arises, so it must be general enough to apply naturally to new cases that occur as the system is used in unusual or unexpected ways.
2. **Durability**

- A security policy must grow and adapt well.
  - In large measure, it will survive the system's growth and expansion without change. If written in a flexible way, the existing policy will be applicable to new situations. However, there are times when the policy must change (such as when government regulations mandate new security constraints), so the policy must be changeable when it needs to be.

5.Characteristics of a Good Security Policy

Characteristics of a Good Security Policy.

3. Realism

The policy must be realistic.

- That is, it must be possible to implement the stated security requirements with existing technology.
- Moreover, the implementation must be beneficial in terms of time, cost, and convenience; the policy should not recommend a control that works but prevents the system or its users from performing their activities and functions. It is important to make economically worthwhile investments in security, just as for any other careful business investment.

4. Usefulness

An obscure or incomplete security policy will not be implemented properly, if at all.

The policy must be written in language that can be read, understood, and followed by anyone who must implement it or is affected by it.

- For this reason, the policy should be succinct, clear, and direct.

5.Characteristics of a Good Security Policy

Remark

- Organizations develop computer security policies along the lines just described.
- Generally the policies lead to the familiar assets, vulnerabilities, and controls.
- But sometimes you have to start with existing policies which may be formal documents or informal understandings and consider how they apply in new situations.
- Is this action consistent with the goals of the policy and therefore acceptable?
- Applying policies can be like being a judge. As security professionals, we should often focus on security policy without remembering the context in which we are making policy decisions.

The End

Question

&

Answers

THANKS