CSE 465
Information Assurance

IA Policies

Professor Stephen S. Yau

What Is an IA Policy?

- ***High-level statements*** of ***goals*** of the ***procedures for information assurance***
  - Define which actions are ***require***d, and which are ***permitted***
  - Not guidelines, procedures or controls
  - Top level policies are often determined by ***management*** with significant input from ***IT personnel***, and represent ***corporate goals and principles***
  - Important to ***distribute*** policies to those responsible for following the policies and/or implement the policy enforcement method

What Is an IA Policy? (cont.)

- Policy and enforcement mechanism
  - Every IA policy statement should have an ***enforcement mechanism***
    - Critical to make ***employees aware of policies*** affecting their actions, and their violations may result in reprimand, suspension, or dismissal
    - The fact that individual employees have been made aware of should be ***documented***.
      - Example: An employee signs a statement that the employee has attended XX training session
  - Enforcement mechanism may be technological, such as firewall, or a process, such as security audit.

What Is a Security Policy?

- A statement that partitions the states of the system into ***a set of authorized, or secure states*** and ***a set of unauthorized or unsecure states.***
- IA policies include security policies
- A security policy sets ***the context*** in which we can ***define a secure system***. What is secure under a policy may not be secure under a different policy.

Importance of IA Policies

- Assure proper implementation of ***control***s
  - Dictate configuration of control mechanisms, such as firewall and IDS
- Guide ***product selection***, such as product from foreign company not allowed in certain projects
- Demonstrate ***management support***
- Clearly define ***appropriate behavior of employees***
- Achieve higher level security
- Avoid ***liability*** for company and management

Threats Countered

- IA policies indicating that the organization has proper operations ***against***
  - ***Disregard for public laws,*** such as institutional violation of copyright laws, and violation of privacy laws
  - ***Negligence***
  - ***Failure to use measures commonly found*** in other "like" organizations
  - ***Failure to exercise due diligence*** by computer professionals (computer malpractice)
  - ***Failure to enforce policies***

An Example

- Acceptable Use Policy (AUP) for employees to ***access Internet on corporate systems***
  - Defines which employees can and which employees cannot use corporate systems for accessing Internet
  - Define penalties for violations
  - Enforcement: website blocking, activity logging and audit, individual workstation audit, etc.

Establishing IA Policies

Step 1: Secure strong ***management support***

Step 2: Gather ***key data***

- Relevant policies
- Relevant statutes
- Research on what other organizations are doing

Step 3: Define ***framework***

- Determine ***overall goal*** of policy statement
- List ***areas to be covered***
- Start with basic essentials and add additional areas as required

Establishing IA Policies (cont.)

Step 4: Structure effective ***review, approval, implementation, and enforcement procedures***

- Determine who need to ***coordinate*** and get them ***involved early***
- Know who are going to ***approve*** the policy and ensure they understand that information is an asset
- ***Cross reference with HR policies***

Step 5: Perform ***risk assessment/analysis*** or ***audit***

Step 6: Make sure each policy is written in ***same style*** as existing policies

Guidelines for IA Policies

- Number of IA policies
  - ***Number of areas*** identified in your ***objectives***
  - One policy document ***for each system or subsystem within your business objectives***, such as e-mail, and Internet usage.
  - No limit on length of a policy, ***clarity*** of policy definition is most important
- IA policies must be ***coherent*** and ***enforceable***
  - In 1991 National Research Council Report on "Computers at Risk", the prosecutors stated they ***turn down many cases because it is not clear what is allowed and what is not***

Policy Areas

- ***Confidentiality*** Policies
  - Deal only with confidentiality
  - ***Prevent unauthorized disclosure of information***
  - ***Identify those states in which information leaks*** to those not authorized to receive it. of rights.
  - Must handle ***dynamic changes of authorization***, and hence it includes a ***temporal element***.

Policy Areas (cont.)

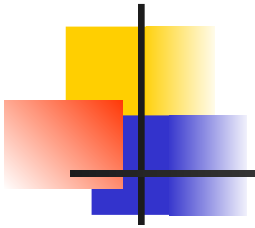
- ***Integrity*** Policies
  - Deal only with integrity
  - Identify ***authorized ways*** in which ***information may be altered and entities authorized to alter it***.
  - Describe conditions and manner in which data can be altered

Policy Areas (cont.)

- ***Administrative Security*** Policies
  - Policies related to ***administration of information systems***
  - Typically exist before a system development process begins
  - Usually focus on ***responsibilities of all members within IA team***, and have legal implications.
- ***Access Control*** Policies
  - Decide who can access what information under what conditions
  - Authorize a group of users to perform a set of actions on a set of resources
  - Ensure "***separation of duty***" and "***least privilege***"

Policy Areas (cont.)

- ***Audit Trails and Logging*** Policies
  - Define rules on how the system behavior will be recorded
  - ***Audit trails*** are usually continuous record about routine activities
  - ***Logs*** are usually event-oriented record
  - Objective: To record proper nformation of the system so that when something bad happens, these records will help staff know who/what caused the problem



Policy Areas (cont.)

- ***Documentation*** Policies
  - Define rules about
    - What kinds of information should be documented?
    - Who can modify the documents?
    - Under what situations can some of the documents be disclosed and to whom?
  - Important to ensure privacy and integrity of the system

Policy Areas (cont.)

- ***Evidence Collection and Preservation*** Policies
  - Define rules about computer incident investigation:
    - What information should be collected and how to collect it?
    - How to store collected information to best present it later in a court?
  - Computer forensics always conflict with personal privacy and the policies should clearly draw the line

Policy Areas (cont.)

- ***Information Security*** Policies
  - Set forth mechanisms by ***which information*** stored on organization's information systems and utilized by organization's employees is ***secured and protected***
  - State ***rights and obligations*** of organization to manage, protect, secure, and control various information that could be accessed through organization's information systems

Policy Areas (cont.)

- ***Information Security*** Policies (cont.)
  - Help maintain ***data integrity and accuracy***, and provide authorized individuals ***timely and reliable access to needed data***. Also ensure that unauthorized individuals are ***denied access*** to computing resources or other means to retrieve, modify or transfer information
  - Ensure organization to meet its ***record-keeping and reporting obligations*** as required by state and federal laws simultaneously, comply with various statutes and policies ***protecting rights and privacy of individuals***

An IA Policy Example

Scenario:

A company will have a new product X in the market and needs to have a policy to protect the access to the product information. Following is the ***access policy*** for accessing the product X's information.

IA Policy Example (cont.)

Access policy (for product information):

"The company considers ***all non-commercial information*** related to the product X as *proprietary*, which must be under the control of the company. Only people working directly on X may access X's non-commercial information. The persons, who can access this information should be at least at the manager level, and before such a person exercises such access to this information, he/she must have the written permission from his/her supervisor."

References

- Michael E. Whitman, Herbert J. Mattord , *Principles of Information Security*, Course Technology, 2011
- Matt Bishop, *Introduction to Computer Security*, *Addison- Wesley*, 2004
- Matt Bishop, *Computer Security: Art and Science*, *Addison- Wesley*, 2002,
- M. Merkow, J. Breithaupt, *Information Security: Principles and Practices*, Prentice Hall, August 2005
- R. J. Anderson, *Computer Engineering: A Guide to Building Dependable Distributed Systems*, Wiley, 2008