CSE 543

Information Assurance and Security

IA Policies

Professor Stephen S. Yau

Fall 2022

What Is an IA Policy?

- ***High level statements*** of ***goals*** of ***procedures for information assurance***
  - Define what actions are ***required***, and which are ***permitted***
  - Not guidelines
  - 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***

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 a training session
  - Enforcement mechanism may be technological (e.g., firewall), or a process (e.g., 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 controls
  - Dictate configuration of control mechanisms (e.g., firewall, and IDS)
- Guide product selection (e.g., laptops not permitted)
- Demonstrate management support

Importance of IA Policies *(Cont.)*

- Clearly define appropriate behavior of employees
- Can achieve higher level security than with the IA policies
- ***Avoid liability*** for company and management

Threats Countered

- IA policies indicating the organization is ***aware*** of 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 why the organization needs the proposed IA policy
- Cross reference with HR policies

Establishing IA Policies *(cont.)*

Step 5: Perform risk assessment/analysis or audit.

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

What else need to be done in order to establish an IA policy after Step 6?

Establishing IA Policies *(cont.)*

- Number of IA policies
  - ***Number of areas*** identified in your ***objectives***
  - One policy document for each system and subsystem within your business objectives, e.g. email, anti-virus protection, and Internet usage.
  - No limit on length of a policy, ***clarity*** of policy definition is most important

Establishing IA Policies (cont.)

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

Policy Areas *(cont.)*

- ***Integrity*** Policies
  - 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
  - Typically exist before a system development process
  - 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
  - Essential when something bad happened since 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 system

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 laws and to comply with various statutes and policies ***protecting rights and privacy of individuals***

Policy Areas (cont.)

- ***Personnel Security*** Policies
  - Define rules to do ***background checking and screening*** before hiring
  - Make ***agreement*** with employees ***before*** they start working
  - Reduce ***risks of human errors, theft, fraud or misuse of facilities***
  - Ensure that users are ***aware of information security threats and concerns,*** and are equipped to ***support organization's security policies in their normal work***

An IA Policy Example

A small start-up company has a new product X in the market and needs to have a policy to protect the product information.

Policy for access control of product X information.

IA Policy Example *(cont.)*

Access control policy (for product information):

"***All non-commercial information*** related to product X is *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 accesses this information, he/she must have ***the written permission from his/her supervisor."***

Some Research Topics Related to IA Policies (including security policies)

- Automated ***consistency check*** of IA policies (including security policies)
- Resolution of ***conflict*** of IA policies
- Effective mechanisms for ***enforcing*** IA policies (including security policies)
- Effective ***implementation*** of IA policies

For both static and ***dynamic (situation awareness)***

References

- Mandal, D. and Mazumdar, C. Towards an Ontology for Enterprise Level Information Security Policy Analysis. DOI: 10.5220/0010248004920499 In Proceedings of the 7th International Conference on Information Systems Security and Privacy (ICISSP 2021), pages 492-499 ISBN: 978-989-758-491-6
- N. Kobayashi, A. Nakamoto, M. Kawase, M. Ioki and S. Shirasaka, "A Proposal of Information Security Policy Agreement Method for Merger and Acquisition Using Assurance Case and ISO 27001," 2019 8th International Congress on Advanced Applied Informatics (IIAI-AAI), 2019, pp. 727-733, doi: 10.1109/IIAI-AAI.2019.00150.

References (cont.)

- Michael E. Whitman, Herbert J. Mattord , Principles of Information Security, Thomson Course Technology, 6th edition, 2018.
- Robert Johnson, Security Policies And Implementation Issues, 2014
- Mark Stamp, *Information Security: Principles and Practice*, 2nd edition, 2011
- Corey Schou, Steven Hernandez, *Information Assurance Handbook: Effective Computer Security and Risk Management Strategies*, 2014
- Alan Mclennan, *Information Governance and Assurance: Reduing Risk, Promoting Policy*, 2014