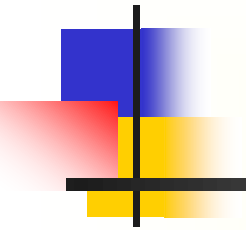

Chapter 6 – Information Security Policies and Procedures

“Quality information security program begins and ends with policy”

“…policies are important reference documents for internal audits and for the resolution of legal disputes about Management’s due diligence and policy documents can act as a clear statement of Management’s intent …”

Charles C. Wood

6.1 Information Security Policy

- Policies are used to express views of communities which then become the basis of planning, management and maintenance of the information security profile
- Policies are set of rules that dictate acceptable and unacceptable behavior within an organization
- Policies represent the formal statement of the organization's managerial philosophy (in case of our focus, the organization's information security philosophy)
- Policies should not go into detail like specifying the proper operation of equipment or software (Standards & Procedures)
- Policies must specify the penalties for unacceptable behavior and define an appeals process

- The objective of information security is to protect the
  - integrity,
  - confidentiality, and
  - availability of information
- Information protection should be part of an overall asset protection program
- Security techniques are available to minimize security risks; however, human factor is a major concern
- Organizations need to ensure that their information is protected irrespective of the employees they may have
- They achieve this objective through Policies, Standards and Procedures

- The success of any information security program lies in policy development
  - Policy is the essential foundation of an effective information security program
  - The centrality of information security polices is to virtually everything that happens in the information security field
  - An effective information security training and awareness effort cannot be initiated without having information security policies

- According to NIST (National Institute for Standards and Technology) - Executive guide to the protection of information resources
  - The primary responsibility of the policy maker is to set the information resource security policy for the organization within the objectives of
    - Reduced risk
    - Compliance with laws and regulations
    - Assurance of CIA - confidentiality, integrity and availability

- Basic Rules in Building Policy
  - Policy should never conflict with law
  - Policy must be able to stand up in court, if challenged
  - Policy must be properly supported and administered
- Guidelines for IT policy
  - All policies must contribute to the success of the organization
  - Management must ensure the adequate sharing of responsibility for proper use of information systems
  - End users of information systems should be involved in the steps of policy formulation

- A policy is a high-level statement of the enterprise's beliefs, goals, and procedures; and the general means for their attainment
- Standards are mandatory requirements that support individual policies
- Procedures are mandatory step-by-step detailed actions required to complete a task successfully
- Guidelines are similar to standards but are not mandatory
- Information security policies, standards and procedures enable organizations to
  - Ensure that their security concerns are properly addressed
  - Every employee knows what s/he needs to do to ensure the information security of the company
  - Similar response is given for every problem

6.1.1 Developing Policies

- A Good Policy should
  - Be easy to understand: by all people who will have to read the policy
  - Be applicable: don't copy others' policy word by word since it may not be applicable to you
  - Be doable: the restrictions should not stop work!
  - Be enforceable: if it cannot be enforced, it will probably remain on paper
  - Be phased in: organizations need time to digest policy
  - Be proactive: say what needs to be done rather than what is not allowed
  - Avoid absoluteness: be diplomatic
  - Meet business objectives: should lower the security risks to a level acceptable by the organization without hampering the work of the organization to unacceptable level

- There are three types of policies
  - Global policies (Tier 1)
    - Used to create the organization's overall vision and direction
    - Examples
      - Employment Practices: such as hiring practices and new employee orientation (introduce them about information security, nondisclosure and confidentiality agreement, etc.)
      - Conflict of Interest
      - Employee Discipline, etc.
  - Topic-specific policies (Tier 2)
    - Address particular subject of concern
    - They require more frequent revisions as changes in technology and other factors dictate
    - e.g., Antivirus, E-mail usage, Internet usage

- Application-specific policies (Tier 3)
  - Decisions taken by Management to control particular applications
  - Focuses on one particular system or application
    - e.g., Accounting system
  - It addresses issues such as
    - Who has the authority to read or modify data?
    - Under what conditions can data be read or modified?
    - How is remote access controlled?

- Components of a Policy
  - The components of a policy typically include
    - Scope
      - Global or specific
    - Responsibilities
      - Who is responsible for what
    - Compliance or consequences
      - What will happen if you are not compliant
  - Writing a policy requires multiple skills and attention
  - A global policy, for example, is developed by a steering committee established for the purpose

- Example of Policy Statements
  - "Exchanges of information and software between the Company and any other organization shall be controlled in accordance with its classification"
  - "To ensure protection of corporate information, the owner shall use a formal review process to classify information into one of the following three: Public, Internal-use and Confidential."
- Information Classification Policy
  - Why classify?
    - Among the information available in an enterprise there are (approx.)
      - 10% confidential information
      - 80% internal use information
      - 10% public information
    - It would be a big waste of resources to give the same level of security for all the information
    - You don't put everything you own in a safe (כזכף)!

- What is confidential information?
  - It is information, if disclosed, could
    - Violate privacy of individuals
    - Reduce company's competitive advantage
    - Cause damage to the organization
- Many organizations classify information into different classes of security
  - Part of the asset classification policy
- An information or asset classification process is a business decision process. Examples of information classification could be
  - Top Secret, Confidential, Restricted, Internal-Use, Public
  - Company confidential Red, Company confidential Yellow, Company confidential Green, Company Public

- How to develop classification levels
  - Discuss with other organizations' specialists and learn from their experiences (learn from best practices)
  - Discuss with Management of the organization
  - Prepare a draft and discuss it with Management
  - Avoid the temptation of having too many levels
- The information classification policy defines the department's policy with regards to classification, declassification and reclassification of information

- Employee responsibilities
  - Three kinds of employees
  - Owner
    - Has been given the organization's property right
    - Should identify the classification level
    - Should identify the appropriate safeguards to ensure the security of the information
    - Decides on who should be authorized to access the information
  - Custodian
    - Responsible for overseeing and implementing the necessary safeguards to protect the assets
  - User
    - Views, amends or updates the information if authorized

6.1.2 Developing Standards and Procedures

- Developing Standards
  - Standards define what is to be accomplished in specific terms
  - Every industry has standards that try to ensure some quality of product or service, or enable interoperability
  - Many industry standards have information security issues
    - e.g., Banking, Healthcare
  - Some of the standards become national regulations where organizations will have to follow
  - Organizations can also develop their own standards (enterprise standards)
  - Standards are easier to update than global policies
  - Standards have to be reviewed regularly (every year, for example)

- Standards must be
  - Reasonable
  - Flexible
  - Practical/Applicable
  - Up-to-date/Reviewed regularly
- Standards should enable the enterprise to fulfill its business objectives while minimizing the security risks
- Examples of standard statements
  - “Where a facility is available, unattended terminals must enforce a timeout not exceeding 15 minutes.”
  - “When it becomes known that permanent, contract, or temporary staff are to leave the organization, the relevant Manager must immediately inform Information Security Administration of the fact providing expected date of leaving.”
  - “All visitors must be supervised by authorized personnel at all time while within controlled areas.”

- Developing Procedures
  - Developing a procedure should be faster than developing a policy since it does not need to be approved by Management
  - Policies change rarely, but procedures (implementation details) can vary from department to department and are modified over time
  - Procedure writing process
    - Interview with SME (Subject Matter Expert)
    - Prepare a draft
    - Review of the draft by the SME
    - Update of the procedures based on the comments
    - Final review by SME
    - Update of the procedures based on the comments
    - Test the procedures
    - Publish the procedures
  - Procedures should also be reviewed regularly

- Selling Policies, Standards, and Procedures
  - If you write policies, standards, and procedures, publish them and do nothing else, it is very probable that nobody will use them
  - You should therefore ensure acceptance of the policies, standards, and procedures at all levels
  - Selling points
    - Formal risk analysis to show Management how important it is to avoid the risks using your policies, standards, and procedures
    - Showing examples of security problems
    - Showing how policies, standards, and procedures facilitate the work but not making it more difficult

- You need support from Management; to achieve that
  - You need to involve them right from the beginning so that they understand and support your work
  - You should make sure that Management is aware of the stake at hand
  - You should show them that it is up to their needs
- Employees should be in the process; to achieve that
  - You should educate the employees about the policies, standards, and procedures in an ‘interesting’ way
  - You should be a good communicator

- Next Steps: Post policies
  - Develop revised user ID issuance forms
  - Develop agreement to comply with information security policies
  - Assign and train information security coordinators
  - Prepare and deliver a basic information security training course
  - Develop tests to determine if workers understand policies
  - Develop application-specific information security policies
  - Develop a conceptual hierarchy of information security requirements
  - Assign information ownership and custodianship
  - Establish an information security management committee
  - Develop an information security architecture document
  - Automate policy enforcement through policy servers
  - Develop a self-assessment questionnaire

- Final Note
  - Policies are a countermeasure to protect assets from threats
  - Policies exist to inform employees of acceptable and unacceptable behavior
  - Policies are meant to improve employee productivity and prevent potentially embarrassing situations
  - Communicate penalties for non-compliance

6.2 Legal Issues and Information Security

- Information security and privacy often become major issues for law makers since it can touch fundamental rights of individuals
- You must understand the scope of an organization's legal and ethical responsibilities
- To minimize liabilities (reduce risks), the information security practitioner must
  - Understand the current legal environment
  - Stay up-to-date with laws and regulations
  - Watch for new issues that emerge
- Laws: rules that mandate or prohibit certain societal behaviour
- Ethics: define socially acceptable behaviour
- Cultural Norms: fixed moral attitudes or customs of a particular group; ethics is based on these
- Laws carry sanctions of a governing authority; ethics do not

- Types of Laws
  - Civil: governs nation or state; manages relationships or conflicts between organizational entities and people
  - Criminal: addresses violations harmful to society; actively enforced by the state
  - Private: regulates relationships between individuals and organizations
  - Public: regulates structure/administration of government agencies and relationships with citizens, employees, and other governments

- Policies versus Laws
  - Policies: expectations that describe acceptable and unacceptable employee behaviours in the workplace
  - Policies function as laws within an organization; must be crafted carefully to ensure they are complete, appropriate, and fairly applied to everyone
  - Difference between policy and law: ignorance of a policy is acceptable defense
- Relevant U.S. Laws
  - United States has been a leader in the development and implementation of information security legislation
  - Implementation of information security legislation contributes to a more reliable business environment and a stable economy
  - The U.S. has demonstrated understanding of problems facing the information security field; has specified penalties for individuals and organizations failing to follow requirements set forth in U.S. civil statutes

- Computer Fraud and Abuse Act of 1986 (CFA Act): cornerstone of many computer-related federal laws and enforcement efforts
- National Information Infrastructure Protection Act of 1996
  - Modified several sections of the previous act and increased the penalties for selected crimes
  - Severity of penalties judged on the purpose
    - For purposes of commercial advantage
    - For private financial gain
    - In furtherance of a criminal act

- European Council Cyber-Crime Convention
  - Establishes international task force overseeing Internet security functions for standardized international technology laws
  - Attempts to improve effectiveness of international investigations into breaches of technology law
  - Well received by intellectual property rights advocates due to emphasis on copyright infringement prosecution
  - Lacks realistic provisions for enforcement

- International Laws and Legal Bodies
  - When organizations do business on the Internet, they do business globally
  - Professionals must be sensitive to laws and ethical values of many different cultures, societies, and countries
  - Because of political complexities of relationships among nations and differences in culture, there are few international laws relating to privacy and information security
  - These international laws are important but are limited in their enforceability

- Ethics and Information Security
  - Many professional groups have explicit rules governing ethical behavior in the workplace
  - Professional associations and certification agencies work to establish codes of ethics
    - Can prescribe ethical conduct (Code of conduct and code of practice)
    - Do not always have the ability to ban violators from practice in field

- Ethical Differences Across Cultures
  - Cultural differences create difficulty in determining what is and what is not ethical
  - Difficulties arise when one nationality's ethical behaviour conflicts with ethics of another national group
  - Scenarios are grouped into
    - Software License Infringement
    - Illicit (illegal) Use
    - Misuse of Corporate Resources
  - Cultures have different views on the scenarios
- Ethics and Education
  - Overriding factor in levelling ethical perceptions within a population is education
  - Employees must be trained in expected behaviours of an ethical employee, especially in areas of information security
  - Proper ethical training is vital to creating informed, well prepared, and low-risk system user

- Deterring Unethical and Illegal Behavior
  - Three general causes of unethical and illegal behaviour: ignorance, accident, intent
  - Deterrence: best method for preventing an illegal or unethical activity; e.g., laws, policies, technical controls
  - Laws and policies only deter if three conditions are present
    - Fear of penalty
    - Probability of being caught
    - Probability of penalty being administered

- Evidential Issues
  - There is still no consensus on whether computer evidences are admissible in court
    - Some countries admit computer evidences
    - Some others admit them conditionally (e.g., the computer should be accompanied with a certificate that says that it is working properly)
  - Reliability of evidence
    - When a computer is taken as an evidence, law enforcement officers generally mirror the hard disk for subsequent examination
    - However, since today's operating systems and application software products are very complex, the interpretation can be complex
    - More and more countries are now accepting electronic signatures and contracts as evidences
- Read about Computer Forensics