ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 1, Issue 10, December 2012

FUNDAMENTAL ISSUES FOR DEVELOPING INFORMATION SECURITY POLICIES

Mr. Hardeep Singh Sidhu (M.Sc., M.Phil., M.Tech. IT)
(Research scholar Dravidian University)

***Abstract*—** In this paper fundamental issues for developing information security policies are proposed. Information security is an important issue in today's organization from the business point of view. Information security management can no more be done by merely a set of hardware and software.
The top-level information security policy is a key component of the organizations overall information security management framework. It should be considered as detailed information security documentation including, system level security policies, security guidance and protocols or procedures. The development of information security policy for an organization is a huge task, because it shall be based on mutually agreed visible signs, practices and images, values, basic assumptions and functions. Developing a policy for an organization is an engineering approach just like a software development. This strategy is used by Security Development System Engineers (SDSE) to effectively engineer and integrate information security into a target system as it progresses through the security development life cycle (SDLC).

I. INTRODUCTION

Security policy is the behavior in an organization that contributes to the protection of information and knowledge within and outside the system boundaries. Interest in the security of information and knowledge management systems has been increasing together with the developments of ICT (Information and Communication Technology). An organization from the security point of view has to secure both information and knowledge. Besides information management, attempts to cover both information and knowledge security have often been discussed under the title of "information security awareness" and more recently under the title of "information security culture" in literature survey. The concept of information security policy and apply this concept to an enterprise is the main issue for information security in an organization. Information and especially knowledge are considered to be the critical success factors of business activities. An increasing amount of effective information and knowledge is currently available on internet due to developments in ICT services. Current approaches to secure information and knowledge in an organization include information security management, information system security management, information risk management and security evaluation. In these current approaches the emphasis is given to the information security not to the knowledge.

Definition: Information security policy is a set of rules, regulations, laws and practices that manage how assets in the system including sensitive information are managed, protected, shared and distributed accurately without any type of loss within an organization.

II. SOME GENERAL FACTS ABOUT INFORMATION SECURITY POLICY:

Implementable

The policy that cannot put into practice is of no use to an organization. Analyzing the chosen controls, as well as their implementation and management, should clearly indicate whether the resulting policy will be reasonable.

Enforceable

Any written policy must have mechanisms that will control its enforcement, whether that is a management mechanism such as review and oversight or an automated function of a particular system.

Responsible

The policy must clearly define that who is responsible for the implementation of the policy and it must consistently ensure that the responsibility is handled.

Communicable

Information security policy serve a variety of critical purposes in the enterprise. They are documented business rules for how the organization will protect critical information. Policy form the foundation of the information protection program, establishing the overall information architecture and translating requirements for more detailed standards and procedures. The role of written policy as a business communication tool both within the organization and with the rest of the business world. Information security policy provide the written contract between management, employees, and from the third party point of view on how the organization will protect information.

Documental

The policy must be formally documented, distributed, and understood by all affected personnel within the organization. This is most time-consuming and most

critical part of the entire ISMS. The detail documentation describes that how the ISMS works in a specific organization. There are number of different possible approaches to this, from using external consultants to tackling it yourself. One can do it with more depth and awareness who are much more familiar with the organization security framework. By doing this you can avoid, or reduce, consultancy costs. Development of all the documentation required can be a daunting task, unless you deploy a pre-completed, template documentation toolkit.

III. INFORMATION SECURITY POLICY OBJECTIVES

Information security has long been considered to consist of three main objectives; the preservation of the information's confidentiality, integrity, and availability.

Confidentiality

The prevention of unauthorized disclosure of the information, has been the primary security objective. The Trusted Computer Security Evaluation Criteria (TCSEC) have confidentiality as their primary concern. Unauthorized disclosure may be accomplished through

- Unauthorized access to the information by unauthorized users, such as authorized users accessing information to which they are not concerned with or authorized.
- Hardcopy of sensitive information sent to unattended hardcopy device such as printers, fax machines etc. in public areas.
- Large amounts of information leaving the organization on a floppy disk / flash drives. Having a detailed policy about required technical controls to forestall hackers will not adequately protect the organization.

Integrity

Is an another information security objective. There is no accepted single definition of what integrity encompasses. A multipart definition of integrity has been formulated as follows:

- A subgoal of information security which pertains to ensuring that information processes continue to perform correct processing operations.
- A subgoal of information security which pertains to ensuring that information retains its original level of accuracy.
- A subgoal of information security which pertains to ensuring that information in sound, unimpaired, and perfect condition.

Availability

The availability objective is generally seen as ensuring that the information is available to authorized users when they needed it. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks. In law, non-repudiation implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.

IV. DEVELOPMENT LIFE CYCLE FOR INFORMATION SECURITY POLICY:

A security policy is a document specify rules and adds structure to the organization's procedures. It gives guidance regarding how one should act and respond to given events or situations in an organization. Generally this process is classified in following phases;

Initiation phase:

In the initiation phase of the SDLC, the primary activity is to determine the need for the information system. The system sponsor is identified, the system is linked to one or more organizational goals, and an initial definition of a problem that can be solved by an information system is documented. Steps in this phase include establishing the basic system idea, preliminary requirements definition, feasibility assessment, technology assessment, and management signoff to continue to the next phases.

Design phase:

In this phase, system requirements are gathered and verified. Some system components may be acquired from vendors and some components may be built in-house. The bulk of security planning takes place at this phase.

Implementation phase:

In the implementation phase, the new information system is tested and put into initial production mode.

Operations/Maintenance phase:

In the operations and maintenance phase, the information system is running in normal production, and changes and updates to the system are managed.

Replacement/Disposition phase:

Finally, in the disposition phase, the information system is removed from production and retired; it also can be replaced with another one.

V. SOME BASIC ACTIVITIES IN DEVELOPMENT OF INFORMATION SECURITY POLICY:

Defining scope and system boundaries;

This provide general guidance on the commonly accepted goals of information security management. The control objectives are intended to be implemented to meet the requirements identified by a risk assessment. This practical guideline for developing organizational security standards and effective security management practices and to help build confidence in inter-organizational activities. Beside this boundaries of integrated parts of an organization is defined. An organization should identify all assets and document the importance of these assets. The asset inventory should include all information necessary in order to recover from a disaster, including type of asset, format, location, backup information, license information, and a business value.

Security Requirements;

1. One source is derived from assessing risks to the organization, taking into account the organization's overall business strategy and objectives. Through a risk assessment, threats to assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated.
2. Another source is the legal, statutory, regulatory, and contractual requirements that an organization, its trading partners, contractors, and service providers have to satisfy in the organization.
3. A further source is the particular set of principles, objectives and business requirements for information processing that an organization has developed to support its operations and overall control in the organization.

Overall access control;

A policy can affect few or many users in an organization. Policies may intend to apply to all users and may apply only to a specific application or type of information. For single-user systems or systems dedicated to a specific task, the coarsest control may be sufficient. In multi-user systems running several applications, a finer level of control is probably required. Centralized versus decentralized control is another aspect of access control. With centralized control, a single authority controls all security aspects of the system. In decentralized control, the responsibility for many security functions are in the hands of individuals, users who are probably most familiar with the particular requirements of the information.

Authorization;

Authority: An important part of defining the information security policy is defining the authority for the policies and providing for the delegation of authority. The strength, scope, and controls depend on the authority of the person or organization that makes the rules and maintains the information and rules used by the system. The level of authority is delegated as the policy is refined, and at some point, we reach the boundary between the administrative controls among people and the technical controls within the information system. Defining this hierarchy of controls is part of determining authority. Another aspect of defining levels of authority in a system involves clearly defining the different types of users and the responsibilities and authority of each. Many systems support the concept of groups and roles. The policy should also address related issues such as who defines group membership, when the use of groups is appropriate, whether a user can belong to more than one group, what the individual accountability requirements are within the groups, and how to resolve conflicts between individual user and group privileges. As an example, a system may define four types of users:

User: One who has authorized access to information in an organization. Authorizations may include the ability to read, write, delete, append, execute, and grant / rescind permissions to some objects.

Owner: That individual manager or representative of management who has the responsibility for making and communicating judgments and decisions on behalf of the organization with regard to the use, identification, classification, and protection of a specific information asset. For example, the owner of the information may be the only one authorized to grant/rescind user privileges to access the information.

Custodian: One having authorized possession of the information and entrusted by the owner to provide proper protection in an ongoing operational environment.

Security administrator: The person responsible for the security of a system. Functions that the security administrator is expected to perform include auditing, initializing, and maintaining the security parameters of the system.

Vulnerability analysis

Vulnerability analysis is to identify specific threats to system assets. For each asset, starting with the largest, list all known threats to the asset and eliminate threats from the list that are not relevant to the organization.

Vulnerability is assessed from an operations, development, and security perspective to determine if it is a false positive, caused by a required operations configuration, or needs to be fixed. The false positives are documented and removed from further consideration. The remaining vulnerabilities are assigned a qualitative value indicating potential damage or consequences to the system. The values are shown in the Table below;

Table: 1

Vulnerability Level	Consequence / Damage
0	The impact is negligible
1	The impact is slight. At this value, the impact is so slight that the analyst may recommend that the manager consider accepting the risk.
2	The impact is moderate. An impact of this magnitude must be accounted for in the overall security solution.
3	The impact is great. If this vulnerability is exploited, an impact to the system's mission will occur. This impact must be accommodated by proper controls.
4	The impact would be catastrophic. It is imperative that this impact be specifically accommodated in system security processes and controls

Risk Analysis

Risk assessments: It identifies and prioritizes risks against criteria for risk acceptance and objectives relevant to the organization. The results should guide and determine the appropriate management action and priorities for managing information security risks.

Risk assessment should include the systematic approach of estimating the magnitude of risks (risk analysis) and the process of comparing the estimated risks against risk criteria to determine the significance of the risks (risk evaluation).

To provide management direction and support for information security management should set a clear policy direction for organization objectives and demonstrate support for information security through the issue and maintenance of an information security policy across the organization.

It should be kept in mind that no set of controls can achieve complete security, and that additional management action should be implemented to monitor, evaluate, and improve the efficiency and effectiveness of security controls lo support the organization's aims. Risk assessments should also be performed periodically to address changes in the security requirements and in the risk situation.

Risk calculation: performed to identify relevant assets, threats, and vulnerabilities, comprehensively and qualitatively. The Security Risk Assessment is reviewed on a schedule set by the Information System Security Officer.

The general Risk Calculation equation is:

Risk = Probability * Assets

Based on the above equation, table given below provide examples of scales to quantify harm.

Table: 2

Probability of Event Scale	Frequency	Rating
Negligible	Unlikely to occur	0
Very Low	2 – 3 times every 5 years	1
Low	< = Once per year	2
Medium	< = Once every 6 months	3
High	< = Once per month	4
Very High	= > Once per month	5
Extreme	= > Once per day	6

Table: 3

Risk calculation (Probability x Assets)	Definition	Rating
0	The threat is not viable.	None
1-5	The threat is viable but is not likely to occur.	Low
6-10	This threat is not only viable but likely to occur.	Medium
11-15	The threat is significant, and it is imperative that it be considered in the risk analysis.	High
16-20	The threat is certain to occur. This threat must be accommodated in the security controls.	Critical
21-25	The threat must occur. This threat must be accommodated in the security controls.	Extreme

Once the risks have been evaluated a prioritized list of the risks for further action should be produced using the revised level of risk that reflects existing treatments. The purpose is to identify the risks that are acceptable and those that are not in accordance with the risk evaluation criteria.

Information security architecture

Security architecture provides a framework of procedures, technology and processes. It ensures coherent, consistent, cost effective and secure implementation, use and maintenance of safeguards throughout an agency. It should:

- minimize the variety of technology;
- provide consistent security functionality across all information assets;
- integrate safeguards;
- segregate different domains and control the flow of information between them;
- apply consistent security methods, techniques and naming conventions.

Policy Design

According to the literature survey, the design phase usually consists of two steps. First, the preliminary design and second is the critical design. In the preliminary design, Information security requirements and the synthesized functional specification (from the previous step) are mapped onto specific security controls, standards, (low-level) policy, and procedures to formulate a preliminary design. The elements of the preliminary design are defined below.

- Countermeasures: also know as security measures and safeguards are devices or mechanisms used to regulate or guide the operation of a system.
- Standards: cover details such as implementation steps, system design concepts, software interface mechanisms, software algorithms, and other technical requirements.
- Procedures: are specific operational steps or manual methods that workers must employ to achieve a certain goal

In the second step, the critical design are defined, may be based on the preliminary design. Decisions are made at strategic, tactical and operational level in the organization.

At the end of the critical design phase another series of design reviews will be held with similar goals but with much more detail and implementation planning information.

Implementation

During the implementation phase, security controls are developed or procured, installed, configured and tested in organization. Standards, low-level policy, and procedures are documented and tested. As the security controls are implemented in the system test environment, policy and procedures are adapted. In most cases, security controls must be integrated or interfaced with system components in other organizational units. At the implementation end, limitations of existing systems may not allow for precise implementations of the defined organization policy. Some security mechanisms developed to support many other information security policies in other government agencies and the private sectors are adopted.

Verification and validation

The purpose of the Verification and Validation (V&V) phase is to verify that the delivered system's security controls, standards, policies, and procedures meet the security requirements and that the security requirements were necessary and sufficient to meet organization's information security expectations.

Verification is the process of determining whether or not the products of a given phase of development fulfill the requirements established during the previous phase.

Validation means evaluation of information security requirements against organization's needs, expectations, and evaluation of the system to meet organization's operational needs.

Refinement & maintenance

Most safeguards will require maintenance to ensure that they continue to function correctly and meet evolving risks. Maintenance is continuous improvement to the information security system which involves corrective, preventative, adaptive and perfective changes to the ISMS.

The information protection objectives of many organizations looks same at a top level, e.g. sensitive information processed by the organization's resources shall be properly safeguarded against accidental or malicious disclosure, alteration, destruction.

The process of refining an organization's high-level policy into an implemental security policy involves many choices and decisions, from top-level decisions concerning organization objectives to hardware implementation choices. Through this refinement process, there will be many representations of the policy. At the higher levels, the policy is likely to be documented in a natural language, which is easy to understand, consistent and concise.

Risk Mitigation

The risk mitigation was produced from the information and documents created during the previous phase. The correct implementation of

safeguards relies on a well-structured and documented Risk mitigation plan approved by executive management. Implementing the risk mitigation plan must include arrangements to measure the effectiveness, the extent to which objectives are achieved, of the ISMS. The risk mitigation is either a minor configuration change that will eliminate the vulnerability, a lien that when completed will eliminate / reduce the risk, or a waiver that leaves the vulnerability and the risk in place. For the high and medium risk vulnerabilities, the planned risk mitigation must be reviewed with technical and management personnel from the development, operations, and security of the organizational unit. Agreement must be achieved on a test and deployment schedule for minor configuration changes. Upon agreement, commitment of resources and scheduled deployment the vulnerability value goes to 0, along with the risk value. Liens must be approved by the Central authority and management of the organizational unit. The approving authority must have budget and schedule responsibility and authority over the entire organizational unit. Liens require a commitment of resources, scheduled deployment, and priority from development and operations of the organizational unit.

VI. LITRATURE SERVEY:

- Governing for Enterprise Security Implementation Guide of the Carnegie Mellon University Software Engineering Institute CERT is designed to help business leaders implement an effective program to govern information technology (IT) and information security.
- A Capability Maturity Model for system security engineering was standardized in ISO/IEC_21827.
- Information Security Management Maturity Model (known as ISM-cubed or ISM3) is another form of ISMS. ISM3 builds on standards such as ISO 20000, ISO 9001, CMM, ISO/IEC 27001, and general information governance and security concepts. ISM3 can be used as a template for an ISO 9001-compliant ISMS. While ISO/IEC 27001 is controls based, ISM3 is process based and includes process metrics. ISM3 is a standard for security management (how to achieve the organizations mission despite of errors, attacks and accidents with a given budget). The difference between ISM3 and ISO/IEC 21827 is that ISM3 is focused on management, ISO 21287 on Engineering.
- Yang yue jiang Yu yong xia (2009) Behavioral science-based information security research: Paper discovers that the security problem in fact is person's behavior question. Formerly each kind of security model's flaw had neglected to person's factor consideration, in the information security question, human's factor is more important then any factor.

VII. REFERENCES:

1. Knowledge Based Model for Holistic Information Security Risk Analysis, 2008 Wen Huang, Yong Sheng Ding, Zhi-Hua Hu, Jing-Wen Huang, 2008 International Symposium on Computer Science and Computational Technology, IEEE.
2. A Security Management Assurance Model to holistically assess the Information Security posture Igli Tashi, Solange Ghernaouti 2009 International Conference on Availability, Reliability and Security.
3. Information Security Management – A Practical Approach, 2007 Manik Dey, IEEE.
4. Knowledge Based Framework for Real-Time Risk Assessment of Information Security Inspired by Danger Model, Zhi-Hua Hu, Yong-Sheng Ding, Jing-Wen Huang, 2008 International symposium on Intelligent Information Technology Application Wrokshops, IEEE
5. Behavioral science-based information security research, Yang yue jiang Yu yong xia, 2009, First International Workshop on Education Technology and Computer Science IEEE.