

Security Management Practices

Ed Crowley CISSP
Spring '05

1

Topics

- ◆ Security Management Concepts and Goals
- ◆ Threats, Vulnerabilities, and Risk
- ◆ Security Models
- ◆ Risk Management
 - Information Classifications
 - Risk Analysis
 - Risk Response
- ◆ Security Policy
 - Standards, Guidelines, and Procedures
 - Roles and Responsibilities

2

Security Management Principles

- ◆ Security provides assurance that the enterprise can accomplish its mission
 - Based upon an INFOSEC assessment that includes information criticality matrix.
- ◆ Develops, implements, and maintains relevant:
 - Policies and related entities.
 - Standards, Guidelines, and Procedures
 - Facilitates cost effective countermeasures (controls)

3

Risk

- ◆ Risk
 - Can be managed.
 - Cannot be eliminated.
- ◆ Perfect security isn't attainable.
- ◆ Trust based upon external evidence (assurance) is attainable.

4

Baseline INFOSEC Categories

- ◆ Management
- ◆ Technical
- ◆ Operational
- ◆ Each category has preventative, detective, and reactive aspects.

csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

5

NSA Baseline INFOSEC Classes

Management

- ◆ INFOSEC Documentation
- ◆ INFOSEC roles and responsibilities
- ◆ Contingency planning
- ◆ Configuration management

Operational

- ◆ Media controls
- ◆ Labeling
- ◆ Physical environment
- ◆ Personnel security
- ◆ Education training and awareness

Technical

- ◆ Identification and authentication
- ◆ Account management
- ◆ Session controls
- ◆ Audit
- ◆ Malicious code protection
- ◆ Maintenance
- ◆ System assurance
- ◆ Networking/connectivity
- ◆ Communications security

6

Risk Management Process

Risk management process

- Understand enterprise mission
- Identify and classify informational assets
- Rate and prioritize vulnerabilities
- Identify threats
 - Impact and Likelihood.
- Estimate potential damage
- Review/implement Controls

Includes:

- Policy
- Training and education.

7

Risk Management Objectives

- ◆ Identify and reduce risk to an acceptable level.
- ◆ Facilitate implementation of appropriate, cost effective countermeasures
- ◆ Create/embrace a security model that provides informational assurance.

8

Risk Management Primitives

- Informational assets.
- Vulnerabilities
- Threats
- Controls

9

Security Model *One*

- ◆ Describes important security aspects and their relationship to system behavior.
- ◆ Provides the necessary level of understanding for successful implementation of key security requirements.
 - *Rainbow Series Aqua Book.*

10

Security Model *Two*

- ◆ Layered framework consisting of:
 - Protection mechanisms
 - Logical and physical components
 - Policies, guidelines, and procedures
 - Configurations
 - aka Defense in Depth
- ◆ Provides a means for accreditation and certification testing.
- ◆ Dependent upon an organization's mission and business requirements.

11

Goals

- ◆ Primary Security Goals
 - Confidentiality (privacy)
 - Integrity
 - Availability
 - Authentication and Nonrepudiation
- ◆ Ancillary goals and services:
 - Identification, accountability, and authorization.
- ◆ Security provides confidence that the organization can accomplish its mission

12

Confidentiality

- ◆ Prevents unauthorized information disclosure.
- ◆ Intentional or unintentional
- ◆ Deals with reading data.

Note

When applied to individuals, this is referred to as privacy i.e. organizations need confidentiality while individuals need privacy.

13

Integrity

- ◆ Prevents unauthorized modifications.
 - By unauthorized personnel or processes.
 - Also ensures that unauthorized modifications are not made by authorized personnel or processes that are exceeding their authorization.
- ◆ Includes the maintenance of consistency between internal and external data.
- ◆ May refer to data or to systems.

14

Two Integrity Dimensions

- ◆ Data Integrity
 - Deals with information.
- ◆ System Integrity
 - Deals with systems and components.
- ◆ If you lose the later, in time, you lose the former.

15

Availability

- ◆ Ensures that appropriate personnel have reliable and timely access to informational resources.
- ◆ Impacted by:
 - System malfunction.
 - DOS and DDOS Attacks

16

Ancillary Goals *One*

- ◆ Identification
 - Means by which a user claims their identify to a system.
- ◆ Authentication
 - Testing or reconciliation of evidence of a user's identify.
- ◆ Accountability
 - The property that enables activities on a system to be traced to individuals who may then be held responsible for their actions.
 - *Aqua Book (NCSC-TG-004-88)*

17

Ancillary Goals *Two*

- ◆ Authorization
 - Granting rights or permissions to an individual or process which enable access to a computer resource.
- ◆ Privacy
 - Level of confidentiality that a user is given in a system.
- ◆ Nonrepudiation
 - Quality that ensures that a sender cannot deny sending the message at a later date.

18

Vulnerability and Threats

- ◆ Vulnerability
 - A weakness in system security procedures, system design, implementation, internal controls, etc., that can be exploited to violate system security policy.
 - *Aqua Book (NCSC-TG-004)*.
- ◆ Threat
 - Any circumstance or event with potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service.
 - Likely involves a threat agent.

19

Risk and Risk Analysis

- ◆ Risk is:
 - The probability that a particular threat will exploit a particular vulnerability of the system.
 - *Aqua Book*
- ◆ Risk Analysis:
 - Analyzes threat scenarios
 - Accesses possible damage
 - Determines value of potential loss.
 - ARO & SLE

20

Information Classification

- ◆ Not all data has the same value.
 - Without classification (valuation), cost/benefit analysis is impossible.
 - At a minimum, information should be prioritized into an INFOSEC criticality matrix.
- ◆ Information classification may also:
 - Demonstrate compliance with privacy laws
 - Facilitate regulatory compliance.

21

Organizational Information Classification

- ◆ Organizational information can be classified according to sensitivity to its:
 - loss or
 - disclosure.
- ◆ Information classification program must address a security awareness program and how the classification and handling of information will be provided to employees.

22

Sample Information Classification Criteria

- ◆ Value (mission impact)
- ◆ Age
- ◆ Useful Life
- ◆ Personal Association

23

Design Principles *One*

- ◆ Draw on the ideas of simplicity and restriction.
- ◆ Simplicity makes designs and mechanisms easy to understand.
 - Reduces the potential for inconsistencies within a policy.
- ◆ Restriction minimizes the power of an entity. The entity can access only information it needs.
- ◆ Principle of Fail-Safe Defaults
 - Unless a subject is given explicit access to an object, it should be denied access to that object.

24

Design Principles *Two*

- ◆ Need To Know
 - No need to know, no access.
- ◆ Least Privilege
 - A subject should be given only those privileges that it needs to complete its task.
- ◆ Separation of Duties (Privileges)
 - People involved in checking for inappropriate use should not be capable of making inappropriate use.
 - For example, separate:
 - Development/production
 - Security/audit
 - Accounts payable/accounts receivable

25

Design Principles *Three*

- ◆ Principle of complete mediation
 - All accesses to objects be checked to ensure that they are allowed.
- ◆ Principle of Least Common Mechanism
 - Mechanisms used to access resources should not be shared
- ◆ Principle of Psychological Acceptability
 - Security mechanisms should not make the resource more difficult to access than if the security mechanism were not present.

26

DOD Information Classification Levels

- ◆ Top Secret
- ◆ Secret
- ◆ Confidential
- ◆ Sensitive but Unclassified (*New!*)
- ◆ Unclassified

27

Sample Private Sector Classifications

- ◆ Confidential
- ◆ Private
- ◆ Sensitive
- ◆ Public

28

Information Classification Benefits

- ◆ Appropriate enterprise controls help assure confidentiality, integrity, and availability.
- ◆ As quality of data upon which security decisions are made is improved, decision quality is also improved.
- ◆ Demonstrates, in cost/benefit terms, that information is appropriately protected.

29

Classified Information Distribution

- ◆ External factors may force distribution.
 - Court or regulatory processes.
- ◆ Inherent security vulnerabilities need to be addressed. Situations may include:
 - Court Orders
 - Government Contracts
 - Senior level approvals

30

Information Roles

- ◆ Owner
 - Officer or manager
- ◆ Custodian
 - Day to day responsibility, IT personnel
- ◆ User
 - Uses information in job

31

Information Owner

- ◆ Person responsible for informational asset.
 - Dictates who can access data
 - Usually senior exec
- ◆ Has final corporate data protection responsibility.
- ◆ Under due care, failure to protect this data may result in the owner being held legally liable for negligence.

32

Information Custodian

- ◆ Delegated, by its owner, the responsibility of protecting information.
- ◆ Custodian duties may include:
 - Backup
 - Restore
 - Record maintenance with the established information classification policy.

33

Information User

- ◆ Anyone routinely using the information in their job.
- ◆ Information Users must:
 - Follow operating policy.
 - Take due care.
 - Use only for company purposes.

34

Other Roles

- ◆ Senior Manager
 - Ultimate security responsibility.
- ◆ InfoSec Officer
 - Functional security responsibility.
- ◆ Auditor
 - Examines security.

35

Security Policy

- ◆ Conceptually, a general statement governed by senior executive(s) defining security's organizational role.
 - Provides foundation for an organization's security program.
 - Facilitates a top down approach
- ◆ Rainbow series definition:
 - The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

36

Security Policy Basis

- ◆ Based upon a hierarchy of:
 - Policies
 - Top down
 - Standards
 - Specific technologies applied uniformly.
 - Procedures
 - Steps to perform a specific task.
 - Guidelines
 - Recommended, but not compulsory, actions.

37

Security Policy Management's Role

- ◆ Without management support, an organization doesn't have a security policy.
- ◆ Without a security policy, an organization doesn't have security.

38

Security Policy -- Strategic

- ◆ Policies are the first and highest level of documentation.
 - All the lower level elements, standards, procedures, and guidelines flow from policy.
- ◆ Facilitates “Top Down” implementations.

39

Security Policy Scope

- ◆ Should:
 - Include scope. (What is and what isn't covered by the policy.)
 - Be job position independent
 - Be a high level document
- ◆ Should not include:
 - Procedures
 - Techniques
 - Methods
- ◆ Should be distributed appropriately.
 - Optimum to have employees sign statements that they know and understand the policy
 - Improper distribution, may have legal implication.

40

Security Policy Levels

- ◆ Senior – Strategic
- ◆ Regulatory – Assures legal compliance
- ◆ Advisory – Not mandatory
- ◆ Informative – Facilitates awareness

41

Organizational Security Policy

- ◆ In an organizational security policy, management establishes:
 - How a security program will be set up
 - Program's goals
 - Individual responsibilities
 - Strategic and tactical value of security
 - Enforcement.
 - If policy is not enforced, courts may rule that the policy is not valid.

42

Issue Specific Security Policy

- ◆ Addresses specific security issues that need more detailed explanation and attention to make sure a comprehensive structure is built and all employees understand how they are to comply to these security issues.

43

System Specific Security Policy

- ◆ Presents specific management decisions concerning:
 - Actual computers
 - Networks
 - Systems
 - Applications
 - Data.

44

Regulatory Policies

- ◆ Ensure that organizations follow specific industry:
 - Standards and/or law(s).
 - Standard procedures or base operational practices

45

Advisory Policies

- ◆ Strongly suggest certain behaviors or activities.
- ◆ A company with such policies may want its employees to consider these policies mandatory.

46

Informative Policies

- ◆ Informative policy is written to inform employees of certain topics.

47

Standards, Guidelines, and Procedures

- ◆ Separate from but linked to general policies.
- ◆ Standards – Mandatory requirements
 - Standards specify application of specific technologies in specific ways.
- ◆ Guidelines –Recommended
 - Guidelines refer to the methodologies of securing systems.
- ◆ Procedures – Steps to implement policy

48

Procedures and Baselines

- ◆ Procedures contain detailed steps necessary to perform specific tasks.
- ◆ Baselines define a minimum level of security.
 - Includes specific implementation methods
 - Platform unique

49

Risk Management (RM)

Aqua Book defines risk as the probability that a particular threat will exploit a particular vulnerability.

Risk management:

1. Identifies and assesses risk
 1. Asset valuation and threat identification
2. Deals with risk by mitigating, accepting, or transferring it.
 1. Mitigation involves appropriate mechanisms to maintain an acceptable level of risk.

Note total risk elimination is impossible.

50

Risk Management *Rainbow Series*

Risk Management is:

The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review.

From the Rainbow Series

51

Major Risk Areas

- ◆ Physical damage
- ◆ Human Error
- ◆ Equipment malfunction
- ◆ Attacks
 - Internal
 - External
- ◆ Data loss or misuse
- ◆ Application error

52

Risk Analysis

- ◆ Rainbow Series defines risk analysis as the process of:
 - Identifying security risks
 - Determining their magnitude
 - Identifying areas needing safeguards.
- ◆ Helps integrate security program objectives with business objectives and requirements.

53

Risk Analysis Goals

- ◆ Identify Risks
- ◆ Quantify impact
- ◆ Facilitate cost benefit studies.

54

Risk Assessment

- ◆ Undefined entities cannot be protected from undefined risks.
- ◆ A risk assessment:
 - Identifies assets
 - Identifies threats
 - Calculates risks
- ◆ Synonymous with risk analysis.

55

Risk Management Terms

- ◆ Asset
 - A resource, process, product, or infrastructure component, that an organization has determined must be protected.
- ◆ Threat
 - Any circumstance or event with potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service.

56

Risk Management Terms

- ◆ Vulnerability
 - Absence or weakness of a safeguard
- ◆ Safeguard
 - A control or countermeasure employed to reduce the risk associated with a specific threat, or group of threats.
- ◆ Exposure Factor (EF)
 - The percentage of loss a realized threat event would have on a specific asset.

57

Single Loss Expectancy (SLE)

- ◆ Single Loss Expectancy (SLE)
 - Dollar figure that is assigned to a single event.
- ◆ Asset Value X Exposure Factor = SLE
$$AV \times EF = SLE$$

58

Annualized Loss Expectancy

- ◆ Annualized Rate of Occurrence (ARO)
 - A number that represents the estimated frequency with which a threat is expected to occur.

Annualized Loss Expectancy

- ◆ A dollar value derived from:
$$SLE \times ARO = ALE$$

59

Risk Analysis Elements

- ◆ Quantitative or Qualitative
- ◆ Threat Identification
- ◆ Vulnerability Analysis
- ◆ Asset Valuation Process
- ◆ Safeguard Selection

60

Quantitative Risk Analysis

- ◆ Assigns objective numeric values to risk assessment components and to potential losses.
 - Helps an organization better understand its vulnerabilities.
 - Provides a basis for cost/benefit assessment.
 - Supports budget decisions.

61

Qualitative Risk Analysis

- ◆ Utilizes different scenarios to rank seriousness of the threats
 - Based on judgment, intuition, and experience. (Subjective)
 - Does not attempt to assign hard costs to loss elements.
 - Calculations are simple and readily understood.
 - A general indication of significant areas of risk that should be addressed is provided
- ◆ Scenario orientated. During a scenario description , various threats are matched to assets.

62

Scenario

- ◆ A scenario describes the type of threat and the potential loss to assets, and selects safeguards to mitigate the risk.

63

Preliminary Security Examination

- ◆ Often, conducted prior to quantitative RA.
- ◆ Facilitates gathering of elements needed when the actual RA takes place.
- ◆ Defines asset costs and values.
- ◆ Produces a threat list

64

Risk Analysis Steps

1. Identify assets
2. Analyze vulnerabilities
3. Analyze threats
4. Calculate risk
5. Define Annualized Loss Expectancy (ALE).

65

Asset Valuation Process

- ◆ Both quantitative and qualitative RA procedures require a valuation made of the asset's worth to the organization.

66

Elements that Determine an Asset's Value

- ◆ Initial and ongoing cost.
- ◆ Assets value to the organization's production operations, research and development, and business model viability.
- ◆ Asset's value established in the external marketplace, and the estimated value of the intellectual property.
- ◆ Value is dynamic

67

Potential Threat Categories

- ◆ Data Classification
- ◆ Information Warfare
- ◆ Personnel
- ◆ Application/Operational
- ◆ Criminal
- ◆ Environmental
- ◆ Computer Infrastructure
- ◆ Delayed Processing

68

Risk Analysis Product

- ◆ Detailed significant event listing.
- ◆ Hard cost critical to asset valuation
- ◆ Threat model.
- ◆ Possible threat occurrence rate
- ◆ Loss potential by a threat -- dollar impact
- ◆ Recommended remedial measures and countermeasures

69

Possible Risk Responses

- ◆ Risk Mitigation
 - Implement countermeasures
- ◆ Risk Transference
 - Insurance
- ◆ Risk Acceptance
 - Minimum response
- ◆ Risk Rejection (Ignorance?)
 - You can't have a response to a risk that you are not aware of. (Risk Rejection?)

70

Safeguard Selection Criteria

- ◆ Number one safeguard selection criteria is the cost effectiveness of the control.
 - Safeguard cost of vs. risk exposure
- ◆ The amount of manual intervention required to operate the safeguard.
- ◆ Safeguards should not unreasonably interfere with the normal operations.

71

Safeguard Selection Issues

- ◆ Must allow for the inclusion of auditing and accounting functions.
- ◆ Should be evaluated in regard to its functioning state after activation or reset.
- ◆ Credibility, reliability, and past performance of the safeguard vendor.

72

Security Awareness

- ◆ Often, people are the weakest link in a security chain.
- ◆ All employees need:
 - Education in the basic concepts of security and its benefits to an organization.
 - To know and understand an organization's security policy.

73

Security Awareness

When are personnel are considered security aware?

When they clearly understand the need for security and how security impacts the organization.

74

Training and Education

- ◆ Training is different from awareness in that it utilizes specific classroom or one on one training.

75

Questions?

76