

Security Management Practices

❖ *DigitalSherlock.com | SafeHack.com*

❖ *Date: 2005/05/27*

❖ *Document Name: security_management_practices.pdf*

❖ *GNU Free Documentation License*

❖ *Version 1.00, 2005-05-27*

❖ *Copyright © 2005 Adonis, MSc, Eng, CISSP, Security+, CEH, GSec, MCSE, etc.*

❖ *Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation.*

❖ Risk Management RM

➤ Objective

- **Main function is to mitigate Risk**
- **Mitigating risk means to reduce the risk until it reaches a level that is acceptable to an organization**
- **Risk management tries as much as possible to see the future and to lower the threats**

➤ Process

- **Performing a Risk Analysis [RA], including the cost benefit analysis of protections**
 - Quantify the impact of potential threats
 - To put price or value on the cost of a lost
 - Create clear COST-TO-Value ratio for security protections
 - Also influences the decision making process dealing with hardware and software configuration
 - Helps a company to focus its security resources where they are needed most
 - Quantitative Risk Analysis
 - Qualitative Risk Analysis
- **Implementing, reviewing, and maintaining protections**

➤ Terms and definitions

- **Asset**
 - An asset is a resource, process, product, computing infrastructure etc
 - The loss of the asset could affect C.I.A
 - The loss of the asset could affect the full organization
 - The Value \$ of an asset is composed of all the elements that are related to that asset
 - ◆ Creation
 - ◆ Development
 - ◆ Support
 - ◆ Replacement
 - ◆ Public credibility
 - ◆ Considered cost
- **Threat**
 - Any event that causes undesirable impact on the organization
 - Can be man-made or natural
- **Vulnerability**
 - The absence or weakness
 - Threat can become more frequent because of a vulnerability
 - Think of it as a threat that gets through a safeguard into the system
- **TRIPLE**
 - Combination of Asset + Threat + Vulnerability is called TRIPLE In risk management
- **Safeguard**
 - Is the control or countermeasure employed to reduce the risk associated with a specific

threat or group of threats

- **Exposure Factor [EF]**
 - % of asset loss caused by threat
 - The EF is needed to calculate Single Loss Expectancy [SLE]
- **Single Loss Expectancy [SLE]**
 - Is the dollar \$ figure that is assigned to a single event
 - $SLE = \text{Asset Value (\$)} \times \text{Exposure Factor (EF)}$
 - SLE is needed to calculate Annualized Loss Expectancy [ALE]
 - An asset valued \$100,000 that is subjected to an exposure factor of 30% would yield $SLE = 30,000$
- **Annualized Rate of Occurance [ARO]**
 - Is a number that represents the estimated frequency in which a threat is expected to occur
 - It is calculated based upon the LIKELIHOOD of the event and number of employees that could make that error occur
 - Frequency of threat occurrence per YEAR
 - Example if every 100000 year a meteorite will hit the earth the $ARO = 1/100000 = .00001$
 - Example if we have 100 data entry person that enter wrong data 6 times every year the $ARO = 6 \times 100 = 600$
- **Annualized Loss Expectancy [ALE]**
 - A \$ value derived from Single Loss Expectancy [SLE] X Annualized Rate of Occurance [ARO]
 - $\$ ALE = SLE \times ARO$

➤ **Quantitative Risk Analysis**

- **[PSE] Preliminary Security Examination**
 - Conducted before the actual quantitative RA
 - Helps to gather the elements that will be needed when the actual RA takes place
 - Elements that are defined in this phase:
 - ♦ Asset Cost
 - ♦ Listing of threats
 - ♦ Documentation of existing security measures
- **RA steps**
 - Estimate the potential losses to assets by determining their value
 - ♦ Exposure Factor [EF]
 - % of asset loss caused by threat
 - % of loss a realized threat would have on a specific asset
 - The EF is needed to calculate Single Loss Expectancy [SLE]
 - ♦ Single Loss Expectancy [SLE]
 - Is the dollar \$ figure that is assigned to a single event
 - $SLE = \text{Asset Value (\$)} \times \text{Exposure Factor (EF)}$
 - SLE is needed to calculate Annualized Loss Expectancy [ALE]
 - An asset valued \$100,000 that is subjected to an exposure factor of 30% would yield $SLE = 30,000$
 - Analyze potential threats to the assets
 - ♦ Annualized Rate of Occurance [ARO]
 - Is a number that represents the estimated frequency of the occurrence of an expected threat
 - It is calculated based upon the LIKELIHOOD of the event and number of employees that could make that error occur
 - Frequency of threat occurrence per YEAR
 - Example if every 100000 year a meteorite will hit the earth the $ARO = 1/100000 = .00001$

- Example if we have 100 data entry person that enter wrong data 6 times every year the ARO = $6 \times 100 = 600$
- ◆ Threat type
 - Data classification
 - Data aggregation or concentration that results in data inference
 - Covert Channel manipulation
 - Malicious code/virus/trojan
 - Lack of separation of duties
 - Information warfare
 - Technology oriented terrorism
 - Malicious code or logic bomb
 - Emanation interception
 - Economic espionage
 - Personal
 - Unauthorized or uncontrolled system access
 - Misuse of technology by authorized users
 - Tampering by disgruntled employees
 - Falsified data input by disgruntled employees
 - Application
 - Ineffective security application result procedural error or incorrect data entry
 - Criminal
 - Physical destruction or vandalism
 - Theft of assets or information
 - Organized insider theft
 - Armed robbery
 - Physical harm to personnel
 - Environmental
 - Utility failure
 - Service outage
 - Natural disasters
 - Neighboring hazards
 - Computer Infrastructure
 - Hardware/equipment failure
 - Program errors
 - Operation system flaws
 - Communication system failure
 - Delayed processing
 - Reduced productivity
 - Delayed funds collection
 - Increased expenses
 - Late charges
- Define the annualized loss Expectancy [ALE]
 - ◆ The annual expected financial loss to an organization from a threat
 - ◆ A \$ value derived from Single Loss Expectancy [SLE] X Annualized Rate of Occurance [ARO]
 - ◆ $\$ ALE = SLE \times ARO$
- Results
 - ◆ Valuations of the critical assets in hard cost \$
 - ◆ Detailed listing of significant threats
 - ◆ Each threat's likelihood and its occurrence rate
 - ◆ Loss potential by threat. The \$ impact the threat will have on an asset
 - ◆ Recommended remedial measures

- Risk reduction
- Risk Transference
- Risk Acceptance
- ◆ Recommended Safeguard or countermeasures

➤ **Qualitative Risk Analysis**

- **Does NOT focus on \$ of the data but more on intangible values of a data loss**
- **Purely qualitative risk analysis is possible**
- **Threat frequency and impact data is required to do the analysis**
- **The seriousness of threats and the relative sensitivity of the assets are given a ranking using SCENARIO approach**
- **RA Steps**
 - Creation of threats listing
 - Define asset that need to be protected
 - Assign exposure level
 - Begin Qualitative Risk Assessment SCENARIO
- **Scenario Steps**
 - A scenario is written that addresses each major threat
 - The scenario is reviewed by business managers for a reality check
 - The RA team recommends and evaluates the various safeguards for each threat
 - The RA team works through each finalized scenario using a threat, asset, and safeguard
 - The RA team prepares their findings and submits them to management

➤ **Quantitative Vs Qualitative**

- **Quantitative**
 - Cost Benefit analysis = YES
 - Financial hard cost = YES
 - Can be automated = YES
 - Guesswork involved = LOW
 - Complex calculation = YES
 - Volume of information required = HIGH
 - Time / work involved = HIGH
 - Ease of communication = HIGH
- **Qualitative**
 - Cost Benefit analysis = NO
 - Financial hard cost = NO
 - Can be automated = NO
 - Guesswork involved = HIGH
 - Complex calculation = NO
 - Volume of information required = LOW
 - Time / work involved = LOW
 - Ease of communication = LOW

➤ **Asset valuation process**

- **To start we need both Quantitative and Qualitative procedures**
- **Is necessary to perform the cost/benefit analysis**
- **May be necessary for insurance reasons**
- **May be necessary to satisfy "Due care"**
- **3 elements used to determine value**
 - The initial and on-going cost of purchasing, licensing, developing, supporting
 - The asset's value to the organization's production operations R&D

- The asset's value established in the external marketplace and estimated value of the intellectual property (trade secret, copyright etc)

➤ **Safeguard selection Criteria**

• **Steps**

- **Cost/Benefit Analysis** We should consider:
 - ♦ The purchase, DEV, and licensing costs of the safeguard
 - ♦ The physical installation costs and the disruption to normal production during the installation
 - ♦ Normal operating costs, resource allocation, maintenance and repair costs
 - ♦ $ALE \text{ before safeguard} - ALE \text{ after safeguard} - \text{annual safeguard cost} = \text{Value of safeguard to the organization}$
 - ♦ **Where**
 - **Single Loss Expectancy [SLE]**
 - Is the dollar \$ figure that is assigned to a single event
 - $SLE = \text{Asset Value (\$)} \times \text{Exposure Factor (EF)}$
 - SLE is needed to calculate Annualized Loss Expectancy [ALE]
 - An asset valued \$100,000 that is subjected to an exposure factor of 30% would yield $SLE = 30,000$
 - **Annualized Rate of Occurrence [ARO]**
 - It is calculated based upon the LIKELIHOOD of the event and number of employees that could make that error occur
 - Frequency of threat occurrence per YEAR
 - Example if every 100000 year a meteorite will hit the earth the $ARO = 1/100000 = .00001$
 - Example if we have 100 data entry person that enter wrong data 6 times every year the $ARO = 6 \times 100 = 600$
 - **Define the annualized loss Expectancy [ALE]**
 - A \$ value derived from Single Loss Expectancy [SLE] X Annualized Rate of Occurrence [ARO]
 - $\$ ALE = SLE \times ARO$
- **Level of Manual Operations**
 - ♦ The amount of manual intervention required to operate the safeguard
 - ♦ The more automated a process is, the more sustainable and reliable that process will be.
 - ♦ The safeguard should not unreasonably interfere with the normal operations of production
- **Auditability & Accountability Feature**
 - ♦ The safeguard **MUST** allow auditing and accounting functions
 - ♦ The safeguard **MUST** have the ability to be audited and tested by the auditors
- **Recovery Ability**
 - ♦ During Reset and after reset the safeguard must provide the followings
 - ♦ No asset destruction during activation or reset
 - ♦ No covert channel access to or through the control during reset
 - ♦ No security loss or increase in exposure after activation or reset
 - ♦ Defaults to a state that does **NOT ENABLE** any operator access or rights until the controls are fully operational
- **Vendor Relations**
 - ♦ The credibility , reliability and past performance of the safeguard vendor must be examined
 - ♦ The openness (open source) should also be known in order to avoid design secrecy that prevent later modifications or allow backdoors
 - ♦ Vendor support and documentation should also be considered

❖ **Management Concepts**

➤ **The big three**

• **Confidentiality**

- Prevent the intentional or unintentional unauthorized disclosure of a message's contents

- Can occur intentional release of private information
- Can occur through a misapplication of network rights
- Violation of confidentiality allows attackers to access data without authorization
- **Integrity**
 - ENSURE modifications are not made to data by unauthorized personnel or processes
 - ENSURE Unauthorized modifications are not made to data by authorized personnel or processes
 - ENSURE The data internally and externally consistent
 - Integrity violation allows the (unauthorized) attacker to change the system state or any data residing on or passing through a system
- **Availability**
 - ENSURE the reliable and timely access to data or computing
 - Guarantees that the system are up and running when they are needed.
- **Concept of**
 - **Identification**
 - Means in which users claim their identities to a system
 - User identification enables accountability.
 - **Authentication**
 - Is what you are authorized to perform, access, or do.
 - The testing of evidence of a users identity
 - Authentication is a means of verifying the eligibility of an entity to receive specific categories of information
 - Authentication is typically based upon something you know, something you have, or something you are
 - ♦ Something you KNOW password or pass phrase
 - ♦ Something you HAVE a key, a smart card, a disk
 - ♦ Fingerprint, voice, or retinal scans
 - The authenticating item should be difficult to duplicate
 - The rights and permissions granted to an individual to access a computer
 - **Accountability**
 - Ability to determine the actions and behavior of a single individual within a system
 - Audit trails and logs support accountability
 - It is a principle by which specific action can be traced back to an individual
 - Means of linking individuals to their interactions with an IT product
 - The property that enables activities on a system to be traced to individuals who may then be held responsible for their actions
 - **Authorization**
 - The rights and permissions granted to an individual or process which enable access to a computer resource
 - Authorization determines who is trusted for a given purpose
 - **Privacy**
 - Guarantees the fundamental of confidentiality of a company's data
 - Guarantees the data's level of privacy which is being used by the operator
- **Objectives of security control**
 - **Risk Management ROLE To reduce the effects of security threats and vulnerabilities to a level that is tolerable**
 - **RA Risk Analysis is the process that analyzes the threat and produces a representative value of the estimated potential loss**
 - **Risk can never be eliminated**

❖ Security Awareness

➤ Awareness

- **Objective**
 - Indoctrinate system users and support personnel
 - Tell them what they are expected to do, why, and the possible repercussions to the company
 - Specify the security requirements including
 - ♦ Mode of operation
 - ♦ Access requirements
 - ♦ Information handling
 - ♦ Reporting procedures
 - ♦ Unauthorized actions
 - Conduct Periodic reviews of the information (maintain the indoctrination)
 - It is important to have periodic awareness sessions to orient new employees and refresh senior employees
- **Suggested topics for awareness**
 - Policies, procedures and standards
 - Errors, accidents and omissions
 - Physical and environmental hazards
 - Information warfare
 - Malicious code/logic
 - Intrusions
- **Benefit**
 - Make a measurable reduction in the unauthorized actions attempted by personnel
 - Significantly increase the effectiveness of the protection controls
 - Help to avoid the fraud waste and abuse of computing resources
 - Personnel are considered to be security aware when they clearly understand the need for security
- **Ways to improve security awareness without a lot of expense**
 - Live interactive presentations
 - Lectures
 - Video
 - Computer Based training CBT
 - Publishing, newsletters, bulletins and intranet
 - Incentives. Awards and recognition for security related achievement
 - Reminders. Login banner, Mugs pens, sticky notes mouse pads etc

➤ Training & Education

- **Suggested topics for training**
 - Policies
 - Standards
 - Guidelines
 - Procedures
 - Environmental hazards discussion
 - Physical and environmental hazards
- **InfoSec Training Related Topics**
 - Security related job training for operators and specific users
 - Awareness training for specific departments or personnel
 - Technical security training for IT support personnel and sys admins

- Advanced InfoSec training for security practitioners and Information systems auditors
- Security training for senior managers and business unit managers

❖ Security Policy Implementation

➤ Policy

- **Policies Role**
 - Policies are considered the first and HIGHEST level of documentation
 - Can provide protection from liability due to an exemployee's actions
 - It is an essential fundamental element of SOUND Security Practice
- **FLOW Of Policy**
 - Senior Management Statment Of Policy
 - General Organizational Policies
 - Functional Policies
 - Mandatory Standards
 - ◆ Baselines
 - Recommanded Guidelines
 - Detailed Procedures
- **Policy Types**
 - Senior Management Statment Of Policy
 - ◆ The first policy of any policy creation
 - ◆ CONTAIN an acknowledgment of the importance of the computing resources to the business model
 - ◆ CONTAIN a statement of support for information security
 - ◆ CONTAIN a commitment to authorize and manage the definition of the lower level standards, procedures, guidelines
 - Regulatory
 - ◆ Policies that an organization is REQUIRED to implement
 - ◆ These policies are very DETAILED and are specific to the industry in which the organization operates
 - ◆ ENSURE that an organization is following the standard procedures in its specific industry
 - ◆ GIVE an organization the confidence that they are following the standard
 - Advisory
 - ◆ Security policies that are NOT MANDATORY but are suggested
 - Informative
 - ◆ Policies that simply to inform the reader they are NOT MANDATORY
 - ◆ There are not IMPLIED or specified requirements

➤ Standards

- **Specify the use of specific technologies in a uniform way**
- **Standard are Compulsory or MANDATORY**
- **Are often expensive to administer and therefore should be used judiciously**

➤ Guideline

- **They refer to the methodologies of securing systems (Like Standards) but they are NOT MANDATORY**
- **A Guideline is a more general statement of how to achieve the policies objectives**
- **They are more flexible then standards**
- **They can be used to specify the way standards should be developed.**

➤ Procedures

- **Detail the steps that are followed to perform a specific task.**
- **They are detailed actions that personnel are REQUIRED to follow**

- Provide the detailed steps for implementing the policies, standards, guidelines.
- A procedure is a description of tasks that must be executed in a specific order
- Are step-by-step instructions for compliance with mandatory standards

➤ **Baselines**

- They are similar to standards and they are **COMPULSORY** or **MANDATORY**
- Once a consistent baseline has been created standard can then be developed.
- They take in consideration the difference between various operating systems.
- Guidelines for policies recommendations

❖ **Roles and Responsibilities**

➤ **Senior Management**

- Management is responsible for protecting all assets that are directly or indirectly under their control
- They are viewed as the end of the food chain when liability is concerned
- They may delegate the function of security

➤ **IT Information Systems Security Professionals**

- Are delegated the responsibility for implementing and maintaining security by Senior Level
- Responsible for conducting the Security awareness training
- Providing risk analysis services and investigating computer security incidents
- Provide coordination with internal or external auditors during an EDP audit
- Organizations may have someone who is responsible for the development of the policies and procedures while IS provides input

➤ **Owners**

- Management is responsible for protecting all assets that are directly or indirectly under their control
- Executive or manager of an organization
- This person is responsible for the asset of information
- Has the final corporate responsibility of data protection
- Liable for negligence
- Responsibilities include
 - Responsible for determining the sensitivity and criticality of the information.
 - Periodically reviews that classification to ensure that it still meets the business needs.
 - Ensures that security controls are in place commensurate with the classification.
 - Reviews and ensures currency of the previously granted access rights.
 - Delegating the responsibility of the data protection to custodian

➤ **Custodian**

- Custodian is delegated the responsibility of protecting the information by its owner
- This role is commonly executed by IT system personnel
- Responsibilities include
 - Running regular backups and testing the validity of the backup
 - Performing data restoration from the backups when necessary
 - Maintain Records In Accordance with (IAW) the established information classification policy

➤ **User**

- Any employees
- Contractors

- **External party**
- **Responsibilities include**
 - Users must follow the operating procedures defined by organization
 - They must adhere to the published guidelines
 - Users must take "DUE CARE" to preserve the information's security during their work
 - They must prevent OPEN VIEW
 - They must use company computing resources only for company purposes.
- **Information Systems Auditors**
 - **Responsible for providing reports to the senior management on the effectiveness of the security**
 - **They examine security policies standards guidelines to see if they are effectively complying with the company objectives**

❖ **Information Classification**

- **Objectives**
 - **We classify information in order to determine the appropriate level of protection required**
 - **Has a higher enterprise level benefit**
 - **Primary purpose to enhance confidentiality, integrity, and availability**
 - **There shouldn't be too many categories as this will make it hard for the person classifying the information**
 - **Classified information is generally government information**
 - **Labels are used to identify the classification/categorization that is attached to an object or subject**
- **Benefit**
 - **Demonstrates an organization's commitment to security protections**
 - **Help identify which information is the most sensitive or vital to an organization**
 - **Supports the tenets confidentiality, integrity, and availability**
 - **Help identify which protections apply to which information**
 - **May be required for regulatory, compliance, or legal reasons.**
- **Concept**
 - **GOV Sector**
 - **Unclassified**
 - ◆ Data is not sensitive or classified
 - ◆ The public release of this information DOES NOT violate confidentiality
 - ◆ Example
 - Computer manual
 - Warranty information
 - Recruiting information
 - **Sensitive but Unclassified (SBU)**
 - ◆ Minor secret
 - ◆ Unauthorized disclosure COULD cause SERIOUSE damage
 - ◆ May NOT create serious damage if diclosed
 - ◆ Example
 - Health care data
 - Answers to test scores
 - **Confidential**
 - ◆ Information designated confidential nature
 - ◆ Unauthorized disclosure COULD cause some damage to the COUNTRY

- Secret
 - ♦ Unauthorized disclosure COULD cause SERIOUSE damage to the country
 - ♦ Example
 - Troops deployment plans
 - Nuclear bomb placement
- Top Secret
 - ♦ The highest level of information
 - ♦ Unauthorized disclosure cause EXCEPTIONALLY GRAVE damage to the country
 - ♦ Example
 - Blueprint of new wartime weapons
 - Spy satellite information
 - Espionage Data
- President Of USA
 - ♦ The president of USA has a level only for him
- **Public Sector**
 - Proprietary
 - ♦ If disclosed it could reduce competitive edge
 - ♦ Example
 - Recipe to soft drink or trade secret
 - Technical specifications
 - Public
 - ♦ All data that does not fit into previous classes
 - ♦ Disclosure is not welcome, but it would not cause an adverse impact to company or personnel
 - ♦ Example
 - Upcoming Event
 - Upcoming Projects
 - How many peoples are workingon a specific project
 - Private
 - ♦ Information considered of a personal nature
 - ♦ Intended for company use only
 - ♦ Disclosure COULD Adversely affect the company or personnel
 - ♦ Example
 - Example Salary, Medical information
 - Confidential
 - ♦ Information very sensitive
 - ♦ Intened for INTERNAL use only
 - ♦ Exempt from disclosure under the Freedom of Information Act
 - ♦ Disclosure COULD SERIOUSLY affect the company
 - ♦ Example Info about new product, Trade secrets, merger negotiations
 - Sensitive
 - ♦ Require higher level of classification than normal data
 - ♦ This information is protected from a loss of confidentiality as well as integrity

➤ **Classifications criteria**

- **Value**
 - Number ONE commonly used to classify data in PUBLIC sector
 - If the information is valuable it need to be classified
 - What is this information worth to the company?
 - How much would it cost to reproduce if it was lost?
- **Age**
 - The classification may be lowered if the information value decreases over time
 - How old is this information?

- When will it's useful lifetime be reached?
- **Useful Life**
 - The information made obsolete due to new information
 - Example: Substantial change in the company
- **Personal Associations**
 - If information is personally associated with specific individuals
 - Example: Investigation information that reveals names may need to remain classified
- **Authorization**
 - Who is authorized to see this information?
 - Who is authorized to allow declassification?
- **Custody**
 - Who will have custody of this information?
 - How will they determine if the requesting user is entitled access?
- **Reproduction**
 - Can this material be copied?
 - If so, how will distribution be controlled?
- **Logging Should records be kept regarding**
 - Who has the material
 - Was it returned or destroyed?
 - Was it copied?
- **Marking and Labeling**
 - How will the classified information be labeled and marked to show the classification?
 - How will the information be protected in storage?
 - Does it requires the use of encryption or special locking mechanisms?
- **Filing and Safekeeping**
- **Classifications Procedures**
 - **Identify the administrator/Custodian**
 - **Specify the criteria of how the information will be classified and labeled**
 - **Classifiy the data by its owner**
 - **Specify and document any exceptions to the classification level**
 - **Specify the controls that will be applied to each classification level**
 - **Specify the termination procedures for declassifying the information**
 - **Create an entreprise awareness program about classification controls**
- **Roles**
 - **Owners**
 - Management is responsible for protecting all assets that are directly or indirectly under their control
 - Executive or manger of an organization
 - This person is responsible for the asset of information
 - Has the final corporate responsibility of data protection
 - Liable for negligence
 - Responsibilities include
 - ◆ Responsible for determining the sensitivity and criticality of the information.
 - ◆ Periodically reviews that classification to ensure that it still meets the business needs.
 - ◆ Ensures that security controls are in place commensurate with the classification.
 - ◆ Reviews and ensures currency of the previously granted access rights.
 - ◆ Delegating the responsibility of the data protection to custodian
 - **Custodian**

- Custodian is delegated the responsibility of protecting the information by its owner
- This role is commonly executed by IT system personnel
- Responsibilities include
 - ♦ Running regular backups and testing the validity of the backup
 - ♦ Performing data restoration from the backups when necessary
 - ♦ Maintain Records In Accordance with (IAW) the established information classification policy
- **User**
 - Any employees
 - Contractors
 - External party
 - Responsibilities include
 - ♦ Users must follow the operating procedures defined by organization
 - ♦ They must adhere to the published guidelines
 - ♦ Users must take "DUE CARE" to preserve the information's security during their work
 - ♦ They must prevent OPEN VIEW
 - ♦ They must use company computing resources only for company purposes.