DIPLOMA IN LAW ENFORCEMENT

DLE 2163: SECURITY RISK MANAGEMENT

Chapter 5

Identification of Assets

LEARNING OUTCOMES

Upon completion of the syllabus topics, students should be able to:

1. Identify the importance of risk management.
2. Demonstrate comprehension of various aspects of risk management.
3. Apply risk management techniques to risk management issues.
4. Demonstrate risk management skills in work.

TOPIC 5

Identification of Assets

Risk Identification

- **Assets are targets of various threats and threat agents.**
- Risk management involves identifying organization’s assets and identifying threats/ vulnerabilities.
- Risk identification begins with identifying organization’s assets and assessing their value.

Asset Identification AND Valuation

- Iterative process; begins with identification of assets, including all elements of an organizations system (people, procedures, data and information, software, hardware, networking).

- **Assets are then classified and categorized.**

Categorizing the Components of an Information System

Traditional system components	SecSDLC and risk management system components	
People	Employees	Trusted employees Other staff
	Nonemployees	People at trusted organizations Strangers
Procedures	Procedures	IT and business standard procedures IT and business sensitive procedures
Data	Information	Transmission Processing Storage
Software	Software	Applications Operating systems Security components
Hardware	System devices and peripherals	Systems and peripherals Security devices
	Networking components	Intranet components Internet or DMZ components

People, Procedures, and Data Asset Identification

- Human resources, documentation, and data information assets are more difficult to identify.
- People with knowledge, experience, and good judgment should be assigned this task.
- These assets should be recorded using reliable data-handling process.

People, Procedures, and Data Asset Identification (Continued)

- **Asset attributes for people:** position name/number/ID; supervisor; security clearance level; special skills.
- **Asset attributes for procedures:** description; intended purpose; what elements is it tied to; storage location for reference; storage location for update.

People, Procedures, and Data Asset Identification (continued)

- **Asset attributes for data:** classification; owner/creator/manager; data structure size; data structure used; online/offline; location; backup procedures employed.

Hardware, Software, and Network Asset Identification

What information attributes to track depends on:

i. Needs of organization/ risk management efforts.

ii. Management needs of information security/ information technology communities.

Hardware, Software, and Network Asset Identification (continued)

- Asset attributes to be considered are: name; IP address; element type; serial number; manufacturer name; model/part number; software version; physical or logical location; controlling entity.

Information Asset Classification

- Many organizations have data classification schemes (e.g., confidential, internal, public data).
- Classification of components must be specific to allow determination of priority levels.
- Categories must be comprehensive and mutually exclusive.

Information Asset Valuation

- Questions help develop criteria for asset valuation and which information asset;
  - Is most critical to organization’s success?
  - Generates the most revenue/ profitability?
  - Would be most expensive to replace or protect?
  - Would be the most embarrassing or cause greatest liability if revealed?

Listing Assets in Order of Importance

- Create weighting for each category based on the answers to questions.

- Calculate relative importance of each asset using weighted factor analysis.

- List the assets in order of importance using a weighted factor analysis worksheet.

Data Classification and Management

- Variety of classification schemes used by corporate and military organizations.
- Information owners responsible for classifying their information assets.
- Information classifications must be reviewed periodically.

Data Classification and Management (continued)

- Most organizations do not need detailed level of classification used by military or federal agencies; however, organizations may need to classify data to provide protection.

Security Clearances

- Security clearance structure: each data user assigned a single level of authorization indicating classification level.
- Before accessing specific set of data, employee must meet need-to-know requirement.
- Extra level of protection ensures information confidentiality is maintained.

Management of Classified Data

- Storage, distribution, portability, and destruction of classified data.
- Information not unclassified or public must be clearly marked.
- Clean desk policy requires all information be stored in appropriate storage container daily; unneeded copies of classified information are destroyed.
- Dumpster diving can compromise information security.

ASSET IDENTIFICATION

ASSET IDENTIFICATION

Many organizations have data classification schemes (e.g., confidential, internal, public data)

Classification of components must be specific to allow determination of priority levels

Categories must be comprehensive and mutually exclusive

ASSET IDENTIFICATION

ASSET IDENTIFICATION

Questions help develop criteria for asset valuation: - which information asset is most critical to organization’s success?
- generates the most revenue/profitability?
- would be most expensive to replace or protect?
- would be the most embarrassing or cause greatest liability if revealed?

ASSET IDENTIFICATION

ASSET IDENTIFICATION

Create weighting for each category based on the answers to questions

Calculate relative importance of each asset using weighted factor analysis

List the assets in order of importance using a weighted factor analysis worksheet

ASSET IDENTIFICATION

ASSET IDENTIFICATION

Most organizations do not need detailed level of classification used by military or federal agencies; however, organizations may need to classify data to provide protection.

ASSET IDENTIFICATION

ASSET IDENTIFICATION

Security clearance structure: each data user assigned a single level of authorization indicating classification level

Before accessing specific set of data, employee must meet need-to-know requirement

Extra level of protection ensures information confidentiality is maintained

ASSET IDENTIFICATION

ASSET IDENTIFICATION

Storage, distribution, portability, and destruction of classified data

Information not unclassified or public must be clearly marked as such

Clean desk policy requires all information be stored in appropriate storage container daily; unneeded copies of classified information are destroyed

Dumpster diving can compromise information security