Chapter 15: Information Security Management

Asset Protection

- Protecting assets is at the core of information security
- Asset protection involves asset management and change management

Asset Management

- An **asset** is any item that has a positive economic value
- In an enterprise, assets have the following qualities:
  - They provide value to the enterprise
  - They cannot easily be replaced without a significant investment in expense, time, worker skill, and/or resources
  - They can form part of the enterprise’s corporate identity

Asset Management

Asset	Description	Example	High value?
Data	Data that has been collected, classified, organized, and stored in various forms	Customer, personnel, production, sales, marketing, and finance databases	Yes: Extremely difficult to replace
Customized business software	Software that supports the business processes of the enterprise	Customized order transaction application	Yes: Unique and customized for the enterprise
System software	Software that provides the foundation for application software	Operating system	No: Can be easily replaced
Physical items	Computer equipment, communications equipment, storage media, furniture, and fixtures	Servers, routers, and power supplies	No: Can be easily replaced
Services	Outsourced computing services	Voice and data communications	No: Can be easily replaced

Asset Management

- **Asset management** is the coordinated activity of an organization to realize value from its assets
- To generate value from assets there must be a systematic approach to the governance of the assets and proper utilization of the assets in a cost-effective fashion

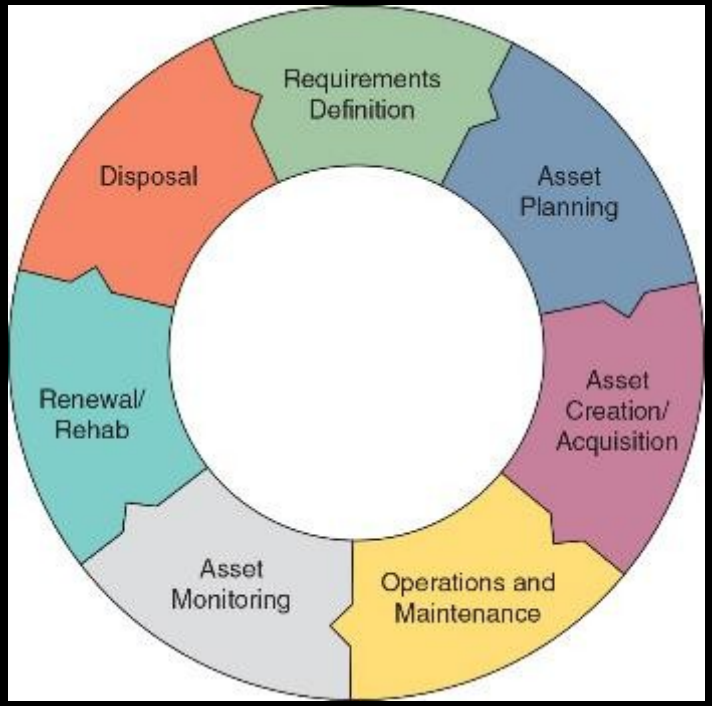
Asset Management

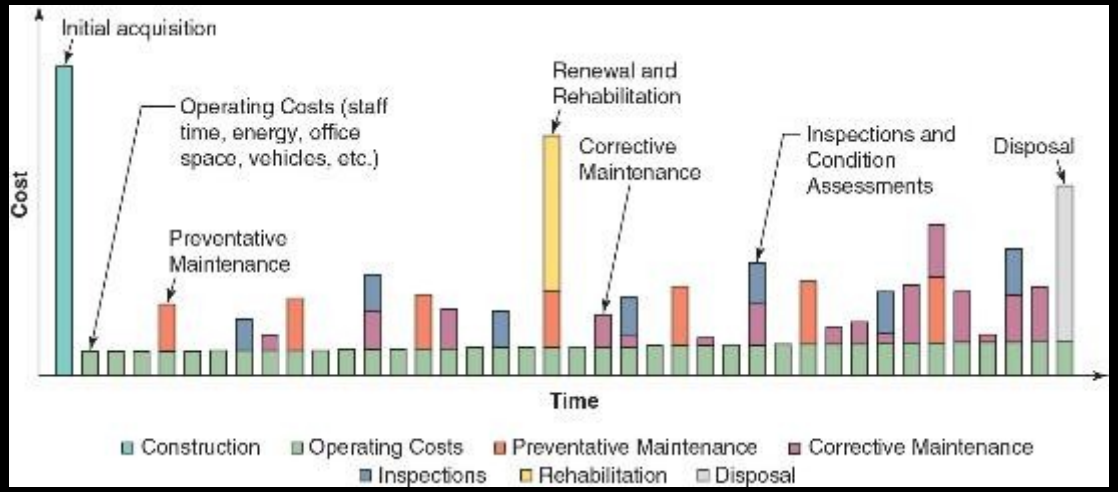
- **Cybersecurity asset management (CAM)** is a process that combines asset management with information security
  - CAM can identify assets on a continuous and real-time basis
  - It can also identify the potential security risks or gaps that affect each asset through **vulnerability scanners**
- CAM provides an up-to-date listing of assets that can immediately be reference in the event of an attack

Asset Management

- An asset’s lifecycle begins when a need is first identified
- From there, the asset is planned, created, or acquired
- It is then operated and maintained, monitored, and replaced or upgrade when it reaches the end of its life
- Costs associated with an asset are accumulated throughout its lifecycle and can vary depending on the current phase of the lifecycle of the asset

Asset Lifecycle & Cost





Selected Asset Management Tasks

- **Asset acquisition** (also called **asset procurement**) is the process of identifying and then securing an asset to support a business goal
- Once the asset has been identified, approved, and funded, most business use a bidding process to ask vendors to submit a qualified bid
- There are two types of bidding processes:
  - Standard bidding process
  - E-bidding process

Selected Asset Management Tasks

- **Asset assignment/accounting** is the process of determining and recording **ownership** (who owns the asset) and **classification** (into which category the asset belongs)
- Assets are generally classified based on one of three factors:
  - How easy it is to turn the asset into cash
  - How the asset is used
  - If the asset physically exists – a **tangible asset** is one that can be touched, and an **intangible asset** is one that has monetary value but no physical form

Selected Asset Management Tasks

- **Asset tracking** is tracing the location of tangible assets
- It is important to have a detailed tracking process as part of an asset management system for all assets
- **Inventory** is the raw materials, works in progress, and finished goods that are available for sale that a business owns
- **Asset enumeration** is a listing of the assets by a seller of those assets

Selected Asset Management Tasks

- Disposal of assts typically involves a two-step process:
  - The asset should be withdrawn from service (**asset decommissioning**)
  - The asset should be physically removed (**asset disposal**)
- Assets that contain valuable data should have that data transferred to a different device (**data retention**) before it is “scrubbed” clean of data (**sanitization**)
- Paper media is usually destroyed by shredding

Micro-Cut Shredding

Change Management

- Day-to-day business processes are called **standard operating procedures**, which can impact information security
- **Change management** is a systematic approach to dealing with transformations (adjustments, replacements, etc.) within an organization
- **Change management policies** are formal statements that outline specific rules that must be met
- **Change management procedures** are detailed mandatory steps needed to comply with a policy

Change Management

- Documentation is critical, both to maintain an audit trail and to ensure compliance with internal and external controls
- Change management watches for any adjustments or variations to assets that could impact security
- Change management tools can be as simple as spreadsheets and flowcharts
  - In larger organizations, specialized change management software suites are used to maintain change logs digitally

Risk Management

- Assets are continually under threat, which is a type of action that has the potential to cause harm
- Organizations must determine the chance that a given threat will compromise an asset (called the **likelihood of occurrence**)
- **Risk** is defined as a situation that involves exposure to some type of danger
- Risk can also be described as a function of threats, consequences of those threats, and the resulting vulnerabilities

Risk Management

- The following are different sources that can generate risk:
  - **Internal and external**
  - **Legacy systems**
  - **Multiparty**
  - **Software compliance and licensing**

Analyzing Risk

- Risk analysis is a process to identify and assess the factors that may jeopardize the success of a project or reaching a stated goal (often called **risk identification**)
- Following a methodology for performing a risk analysis is crucial
  - These include a risk control self-assessment and a risk assessment
- **Risk Control Self-Assessment** (**RCSA**) is an “empowering” methodology by which management and staff collectively work to identify and evaluate risks
  - A reason identifying risk is difficult is **unconscious human biases**

Analyzing Risk

Bias	Explanation
Aggregate bias	Inferring something about an individual by using data that actually describes trends for the broader population
Anchoring bias	Holding on to a specific feature or set of features of information early in the decision-making process
Availability bias	Perceiving how likely an event is to occur given how frequently the event is heard of
Confirmation bias	Making a decision before investigating and then only looking for data that support the theory
Present bias	Trending to discount future risks and gains in favor of immediate gratification
Framing effect	Deciding on an option based on how the choices are worded
Fundamental attribution error	Viewing the failures or mistakes of others as part of their identity rather than attributing them to contextual or environmental influences

Analyzing Risk

- Risk assessment can be performed by the following schedule:
  - A scheduled assessment (**one-time assessment**)
  - Whenever necessary (**ad hoc assessment**)
  - On a calendar basis (**recurring assessment**)
  - Year-round (**continuous assessment**)

Analyzing Risk

- The frequency of conducting a risk assessment can be determined through the following two risk assessment approaches:
  - **Qualitative risk assessment** uses an “educated guess” based on observation
    - Typically assigns a numeric value (1-10) or label (High, Medium, or Low) that represents the risk
  - **Quantitative risk assessment** attempts to create “hard” numbers associated with the risk of an element in a system by using historical data

Analyzing Risk

- The following quantitative tools can be used to predict the likelihood of the risk:
  - **Mean Time Between Failure (MTBF)**
  - **Mean Time To Recovery (MTTR)**
  - **Mean Time To Failure (MTTF)**
  - **Failure In Time (FIT)**
- Historical data can be used to determine the likelihood of a risk occurring within a year, known as **Annualized Rate of Occurrence (ARO)**

Analyzing Risk

Source	Explanation
Law enforcement agencies	Crime statistics on the area of facilities to determine the probability of vandalism, break-ins, or dangers potentially encountered by personnel
Insurance companies	Risks faced by other companies and the amounts paid out when these risks became reality
Computer incident monitoring organizations	Data regarding a variety of technology-related risks, failures, and attacks

Analyzing Risk

- **Risk impact** involves comparing the monetary loss associated with an asset in order to determine the amount of money that would be lost if the risk occurred
- The following formulas are used to calculate expected losses:
  - **Single Loss Expectancy (SLE)** is the expected monetary loss every time a risk occurs
  - **Annualized Loss Expectancy (ALE)** is the expected monetary loss that can be expected for an asset due to risk over a one-year period
  - **Risk exposure factor** is the probability of a risk occurring multiplied by the total loss on the occurrence of the risk

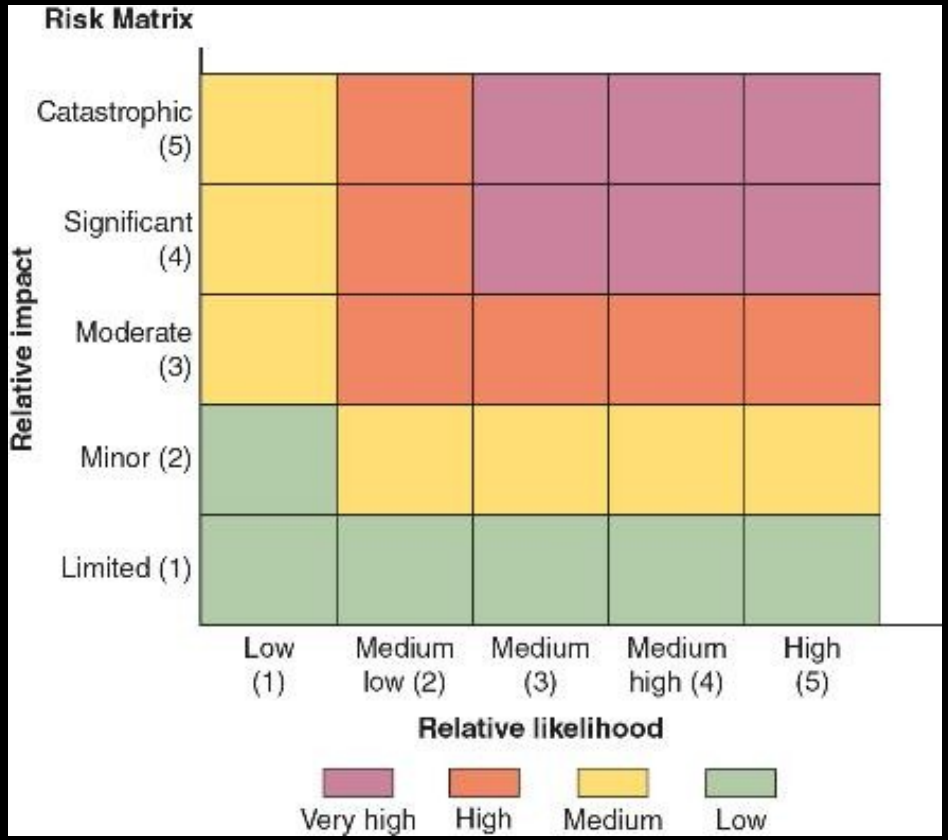
Analyzing Risk

- **Risk register** is a list of potential threats and associated risks
  - It can help provide a clear snapshot of vulnerabilities and risks
  - Risk registers may include **key risk indicators** (the primary risk factors), **risk owners** (those responsible for the asset), and the **risk threshold** (the maximum amount of risk that can be tolerated)
- **Risk matrix/heatmap** is a visual color-coded tool that lists the impact and likelihood of risks

Risk Register

Risk Register											
Risk Id	Risks	Current risk			Status	Owner	Raised	Mitigation Strategies	Residual risk		
		Likelihood	Impact	Severity					Likelihood	Impact	Severity
Category 1: Project selection and project finance											
RP-01	Financial attraction of project to investors	4	4	15	Open		01-march	• Data collection • Information of financial capability of investor • Giving them assurance of tremendous future return	4	3	12
RP-02	Availability of finance	3	4	12	Open		03-march	• Own resources • Commitment with financial institution • Exclusive management of investor	3	3	9
RP-03	Level of demand for project	3	3	9	Open		08-march	• Making possibility and identification of low cost and best quality material • Eradication of extra expenses from petty balance	2	3	6
RP-04	Land acquisition (site availability)	3	3	9	Open		13-march	• Making feasibilities • Analysis and interpretation of feasibilities • Possession and legal obligation of land	2	2	4
RP-05	High finance costs	2	2	4	Open		15-march	• Lowering operational expenses and transportation expenses • Proper management of current expenses	1	2	2

Risk Matrix/Heatmap



Managing Risk

- **Risk tolerance** is the level of risk that an organization can accept per individual risk
- **Risk appetite** is the total risk that the organization can bear in a given risk profile
  - The risk appetite of an organization can be **conservative** (little tolerance for risk), **expansionary** (high tolerance for risk), or **neutral** (neither low nor high tolerance for risk)
- Managing risk involves using specific strategies, addressing third-party risk, and applying awareness management

Managing Risk

- There are four strategies for dealing with risks:
  - **Accept –** risk is acknowledged but no steps are taken to address it
  - **Transfer –** risk is transferred to a third-party
  - **Avoid –** risk is identified but making the decision not to engage in the activity
  - **Mitigate –** attempt to address risk by making the risk less serious

Managing Risk

- A risk associated with using third parties is that it can be difficult to coordinate their diverse activities with the organization
- Risks of third-party integration include the following:
  - **On-boarding and off-boarding**
  - **Application and social media network sharing**
  - **Privacy and risk awareness**
  - **Data considerations**

Managing Risk

- Reducing risk with third-party vendors can be accomplished through requiring a close oversight of a vendor (**vendor monitoring**) and may include the following:
  - Requiring completion of **questionnaires** about their supply-chain security protections
  - Demand they perform regular **penetration testing**
  - Requiring **evidence of internal audits**
  - Create **rules of engagement**
  - Demand third parties follow **due diligence**

Managing Risk

- Vender agreement examples include the following:
  - **Service-level agreement (SLA)**
  - **Business partnership agreement (BPA)**
  - **Memorandum of understanding (MOU)**
  - **Nondisclosure agreement (NDA)**
  - **Measurement system analysis (MSA)**
  - **Memorandum of agreement (MDA)**
  - **Work order (WO)/statement of work (SOW)**

Managing Risk

- **Security awareness management** (**risk awareness**) is the raising of understanding to all employees of what risks exist, their potential impacts, and how they are managed
- The goal of this training is to help users achieve **anomalous behavior recognition**
- Training should help users be able to determine that which is unexpected, unintentional, and as such it becomes risky
  - This is known as **situation awareness**

Managing Risk

- Different techniques employed for user training include the following:
  - **Computer-based training (CBT)**
  - **Role-based awareness training**
  - **Gamification**
  - **Phishing simulations**

Phishing Simulation Dashboard