Key Terms

- Asset and Asset Valuation
- Asset Protection and Layered Security
- Risk
- Vulnerability
- Mitigation
- Cost-Benefit Analysis
- Risk Management
- Physical Security Planning

What are Assets?

Any real or personal property , tangible or intangible, that a company or individual owns that can be given or assigned a monetary value. *Intangible* assets include goodwill, proprietary information and reputation (ASIS International Guideline: *General Security Risk Assessment, 2003*.)

Four Classifications of Assets

> People
> Property
> Information
> Image/Reputation

People **are most often placed first as their protection is of the highest priority.**

Asset Valuation

An asset must have some type of value. The value of the asset could be its real value (ex. A gold bar being worth a set amount of money) or the value could be based on what it would cost to replace (ex. Stolen proprietary information.)

The value of the asset must be known prior to the implantation of a protection program.

Vulnerability

Vulnerabilities are weaknesses that can exploited by an adversary.

Risk

Incidents likely to occur at a site, either due to a history of such events or circumstances in the local environment (ASIS International, 2003.)

How are risks determined?

- Criticality: Impact of the loss.
- Frequency: How often the events occur.
- Probability: Trending of future events.
- Impact: Tangible and intangible costs.

Cost-Benefit Analysis

Conducted to assist in evaluating the mitigation measures against the costs incurred. If it is determined that the cost of mitigating the risk is greater than the value of the asset, other measures must be employed.

Mitigation measures must be designed so as not to substantially interfere with the operation of profitability of the enterprise (ASIS International, 2003.)

Cost-Benefit Analysis Process

The process involves three (3) steps:

1. Identification of all direct and indirect consequences of the expenditure.
2. Assignment of a monetary value to all costs and benefits resulting from the expenditure.
3. Discounting expected future costs and revenues accruing from the expenditures in current monetary values.

A mitigation process that employs the concept of layered protection, also known as “defense in depth”.

The principles behind this concept are:

1. **Deterrence:** The practice of discouraging an adversary from attacking, or even attempting to attack, the asset. This is accomplished through a number of means such as fences, lighting, cameras, security personnel and signage.
2. **Detection:** Identification of a threat at the earliest possible opportunity.
3. **Delaying:** Delaying the adversary gives the other layers of defense a chance to work together. Sufficient layers of delay must be incorporated so that the detection and defense/response pieces of the security system can perform their roles.
4. **Defense/Response:** Allows for a defense to be mounted at the site of the attack to repel the adversary or for a sufficient response to be put together to proceed to the site.

Risk Management

A term that is closely associated with the insurance industry. It is conceptually similar to the physical security planning process but deals with risks other than “security” threats caused by humans.

Three types of risk management strategies are:

1. **Risk Acceptance:** Accepting to risk because it has a low probability of occurring, the cost of mitigation is prohibitive or the value of the asset is so low that loss would be inconsequential.
2. **Risk Reduction:** Employment of mitigation measures.
3. **Risk Transfer:** Example would be an insurance policy. Risk is transferred to the insurance company.

Physical Security Planning

The process used to plan physical security measures is as follows:

1. Asset identification.
2. Identify loss events which can occur.
3. Calculate the probability of the loss event occurring.
4. Determine the impact the loss event will have in terms of direct, indirect and extra-expense costs.
5. Identify countermeasures that can be employed.
6. Implement selected countermeasures.
7. Evaluate effectiveness of countermeasures.

Cycle of History

"Security" implies protection from intentional harm.

The security industry has evolved to offer services to those who seek to avoid, mitigate and respond to perceived and manifested threats.

Trends:

1. There is a strong relationship between commerce and protective services.
2. Private security initiatives often precede public ones. Private corporations are more flexible than governments.
3. Demographics plays a key role in crime control and safety.
4. Security efforts are generally a step behind the latest methods of criminal attacks.
5. Protective efforts usually initiated after a serious incident (ex. 9/11 attacks.)

The Path to Professionalism

Private security has evolved into a modern professional occupation employing highly skilled employees. Significant developments along the path towards professionalism in the security industry include:

1952: *The Industrial Security Manual* was published. It became the "bible" for US Department of Defense contractor procedures.

1955: The American Society for Industrial Security (ASIS) formed in Washington, DC.

1971: *Rand Report on Private Police in America* is published. Led to regulation and higher training standards for private security organizations.

1977: Certified Protection Professional (CPP) program established by ASIS.

1988: International Foundation for Protection Officers (IFPO) formed.

1988: The Association of Certified Fraud Examiners (ACFE) formed.

Contemporary Careers in Asset Protection

There are numerous career fields open to people seeking a career in asset protection. A sampling of these positions are:

- Fixed posts
- Patrol Officer
- Retail Loss Prevention
- Central Alarm Station Operator/Dispatcher
- Security Auditor/Investigator
- IT Security
- Specialized Security Functions: K-9, crowd management, drone pilot, etc.