Session 14

SECURITY LOSS CONTROL

Security

a) Freedom from risk or danger, safety;
b) Freedom from doubt, anxiety or fear; confidence;
c) Something that gives or assures safety as:
- a group or department of private guards;
- measures adopted by a government to prevent espionage, sabotage or attack;
- measures adopted by a business or homeowner to prevent a crime such as burglar or assault.

Security

……. is defined as traditional methods (security officers, fences, and alarms) used to increase the likelihood of a crime-controlled, tranquil, and uninterrupted environment for an individual or organization in pursuit of objectives.

Loss prevention

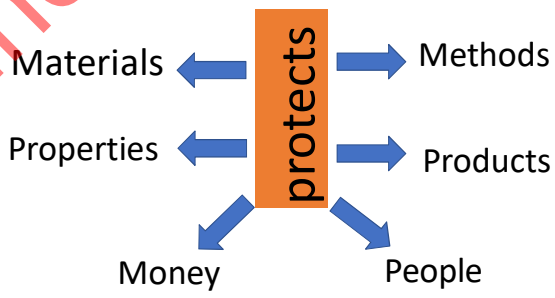
…defined as almost any method (e.g., security officers, safety, auditing) used by an individual or organization to increase the likelihood of preventing and controlling loss (e.g., people, money, productivity, materials) resulting from a host of adverse occurrences (e.g., crime, fire, accident, natural disaster, error, poor supervision or management, bad investment).

SECURITY

protection of property from all kinds of loss, through theft, fraud, fire, and other forms of damage and waste

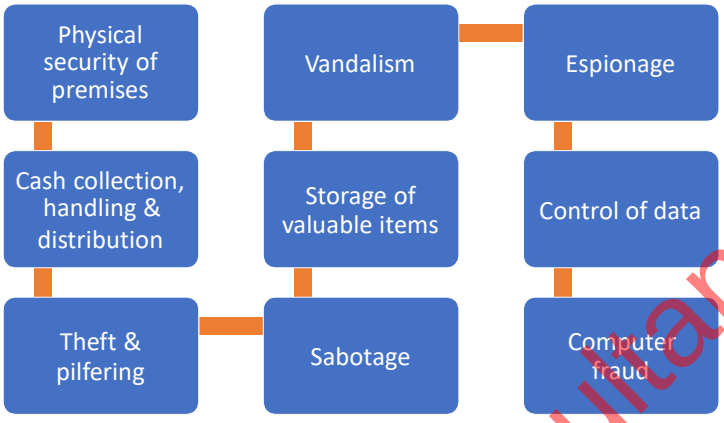
hidden process, financial data, sales projects and other information vital to a company's interest against losses, through what is described as industrial espionage

Security



Based on economic considerations because they are not considered accidental in nature

LC Program should examine



Chief Security Officer (CSO).

The Chief Security Officer Guideline (ASIS International, 2004) is designed "… as a model for organizations to utilize in the development of a leadership function to provide a comprehensive, integrated security risk strategy to contribute to the viability and success of the organization."

ASIS is American Society for Industrial Security

Chief Security Officer (CSO).

This guideline is a response to an increasingly serious threat environment, and it recommends that the CSO report to the most senior level executive of the organization. The guideline lists specific risks, job duties and services, and skills required.

Chief Security Officer (CSO).

The CSO designation and the guideline supporting it provide an excellent reference from which the security profession and senior management can draw on to improve the protection of people and assets and help organizations survive in a world filled with risks.

Components of Company Security

MANAGEMENT

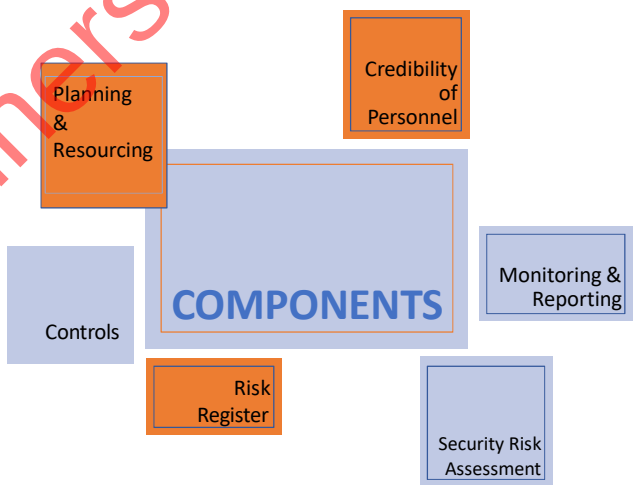
WORKER'S COOPERATION

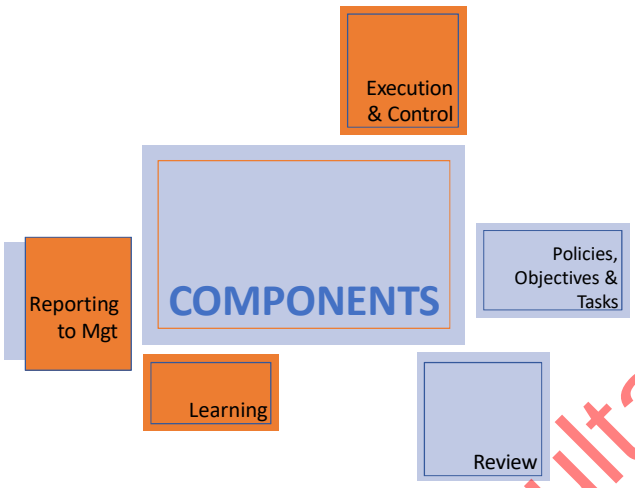
COMMON FUNCTIONS OF SECURITY

- ü Investigation of risks
- ü Evaluation of risks
- ü Developing plans to avoid or reduce loss in a company
- ü Implement and monitor the success of the plans and programs developed
- ü Revision or maintenance of the plans and programs for effective implementation and improved productivity

COMMON AREAS OF CONCENTRATION

- ü Fire inspection
- ü Emergency preparedness
- ü Accident investigation
- ü Workers' screening





Component 1: Credibility and Integration of the Personnel

- **Professionalism** - living the corporate values;
- **Expertise** - demonstrating a thorough knowledge of the subject;
- **Vision** - demonstrating an understanding of the wider business objectives;
- **Teamwork** - working closely with other disciplines to understand their contributions and aspirations;
- **Collaboration** - conducting security risk assessments in support of specific operations, not in isolation;
- **Communication** - security considerations to top management in a clear, concise manner, demonstrating due consideration to all factors.

Component 2: Policies, Objectives and Tasks

There should exist a single security policy which outlines the security architecture, strategy and protocols. The following sections are addressed:

- Security management objectives;
- Statement of the attitude of the organization to security;
- Description of the security environment;
- Statement of the security risk appetite;
- Security organization, roles and responsibilities;
- Procedures for security risk assessment;
- List of security Standard Operating Procedures (SOPs).

Component 3: Threat, Vulnerability and Security Risk Assessment

Security risk assessments should take into consideration a wide range of elements beyond physical security threats. Such elements should include:

- operating environment and groups/events by which it is characterized;
- profile of the organization, the footprint and the social impact;
- strategic, long term objectives of the organization;
- voluntary Principles of Security and Human Rights.

Component 3: Threat, Vulnerability and Security Risk Assessment

- legislation and local expectations;
- capability and intent of local criminal/terrorist elements;
- vulnerability and attractiveness of assets to criminal/terrorist elements;
- availability of resources.

Component 4: Controls

Example of security controls may include:

- Physical protection measures (lights, fences, CCTV, barriers, etc.);
- Introduction of security procedures (ID checking, access control, mail screening, etc.);
- Intelligence networking (local social/political leaders/intelligence providers, etc.);
- Electronic security (encryption, password protection, etc.);
- Resourcing (security personnel, equipment, etc.);
- Local integration (CSR program, local content, etc.;)

Component 5: Security Risk Register

A security risk register should:

- facilitate ownership and management of security risks;
- provide overview of significant security risks faced by an organization;
- record the results of threat/vulnerability security risk assessment;
- maintain record of security risks identified;
- record additional proposed actions to improve the security profile;
- facilitate prioritization of security risks.

Component 6: Planning and Resourcing

Effective planning will answer:

- What are we going to do?
- How are we going to do it?
- When are we going to do it?
- How long do we need to do it for?
- How are we going to coordinate and communicate?
- What do we do if something goes wrong?

Component 6: Planning and Resourcing

Effective resourcing will answer:

- What do we need to do it?
- How do we get it?
- How much does it cost?
- What is our back up if something doesn't work or isn't available?

Component 7: Execution and Control Activities

The execution of a plan is predicated on all of the previous components in the management system:

- The plan has identified all the security risks to the operation;
- All control mechanisms are established;
- The plan has been accordingly and appropriately resourced;
- Any bespoke procedures are documented, approved and validated;

Component 7: Execution and Control Activities

- The plan has been effectively communicated to those with responsibility for its execution;
- Assurance that those with responsibility for carrying out the plan have the correct competencies;
- All correct back up and reinforcement strategies are established and tested.

Component 8: Monitoring and Security Reporting

Monitoring is based, upon effective two-way communication. Where appropriate, traditional methods are often effective and should be considered:

- Inspections;
- Review meetings;
- Auditing;
- Interviews;
- Workshops.

Component 9: Review

The purpose of the review may be any combination of the following:

- critically debrief the plan in order to determine strengths weaknesses and areas that could be improved;
- obtain feedback from those involved in the execution of the plan/ project regarding the manageability of the plan;
- highlight any competency issues arising from exposure to new challenges;

Component 9: Review

- examine how much contribution the operation brings to the achievement of the organization's objectives;
- assurance to top management that security is being managed effectively;
- enables security management to assess whether established protocols are being effective, and to take action accordingly;
- highlight examples of good practice.

Component 10: Learning

Effective processes for learning lessons will enable an organization to:

- introduce improvements to procedures;
- introduce improvements in organizational structure;
- update documentation;
- implement of new training courses;
- increase awareness of new threats/update on existing threats;

Component 10: Learning

- introduce new equipment/technology;
- better integrate to the wider organization; better
- understand the organization's objectives; heightened
- awareness of the contribution of security;
- improved relationship with/understanding of other business functions;
- improvements to the management system.

Component 11: Reporting to Top Management

Providing feedback to top management:

- offers reassurance that security is being effectively managed;
- offers reassurance that security understands its role in the achievement of the business objectives;
- gives confidence in decision-making that all security issues have been given appropriate consideration;

Component 11: Reporting to Top Management

- reinforces the importance of security considerations in making decisions;
- reinforces the role of security in protecting the organization's people, assets and information;
- emphasizes that security operates in support of business operations, and not as a barrier to them.

KEY POINTS

- Security concerns are economic but oftentimes lead to safety hazards
- A **system** of security can improve the overall safety of the organization
- Security concerns the overall protection against losses.

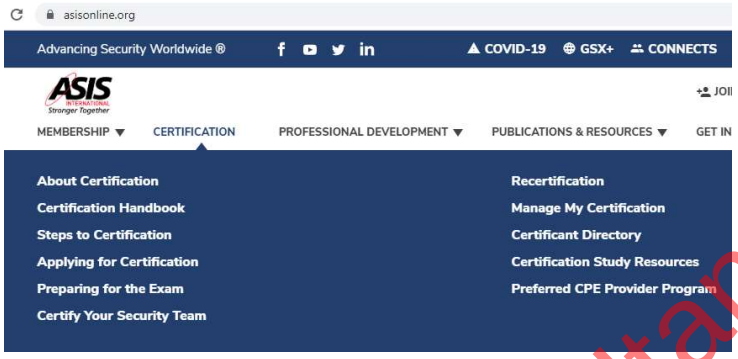
American Society for Industrial Security

Founded in 1955, ASIS International is a global community of security practitioners, each of whom has a role in the protection of assets - people, property, and/or information.

Our members represent virtually every industry in the public and private sectors, and organizations of all sizes. From entry-level managers to CSOs to CEOs, from security veterans to consultants and those transitioning from law enforcement or the military, the ASIS community is global and diverse.

https://www.asisonline.org/

American Society for Industrial Security



https://www.asisonline.org/

American Society for Industrial Security

Certified Protection Professional (CPP®)
The Certified Protection Professional (CPP) is considered the "gold standard" for security management professionals. This certification validates your knowledge in all areas of security management. Eligibility requirements include 7-9 years of security experience and 3 years in responsible charge of a security function.

Professional Certified Investigator (PCI®)
The Professional Certified Investigator (PCI) certification provides demonstrable proof of an individual's knowledge and experience in case management, evidence collection, and preparation of reports and testimony to substantiate findings. Requirements include a high school diploma or GED equivalent and five years of investigations experience, with at least two years in case management.

https://www.asisonline.org/

American Society for Industrial Security

Associate Protection Professional (APP)
The Associate Protection Professional (APP) designation provides the first "rung" on the security manager's career ladder. It is for those with 1-4 years of security management experience and measures the professional's knowledge of security management fundamentals, business operations, risk management, and response management.

Physical Security Professional (PSP®)
The Physical Security Professional (PSP) demonstrates your knowledge in physical security assessments, application, design, and integration of physical security systems, and implementation of security measures. Eligibility requirements include a high school diploma, GED equivalent, or associate degree AND six years of progressive experience in the physical security field OR a Bachelor's degree or higher AND four years of progressive experience in the physical security field.

https://www.asisonline.org/

International Facility Management Association

What is Facility Management?

Who manages one of your organization's largest assets with one of the largest operating budgets? Your facility manager.

Facility management (FM) is a profession that encompasses multiple disciplines to ensure functionality, comfort, safety and efficiency of the built environment by integrating people, place, process and technology.

https://www.ifma.org/

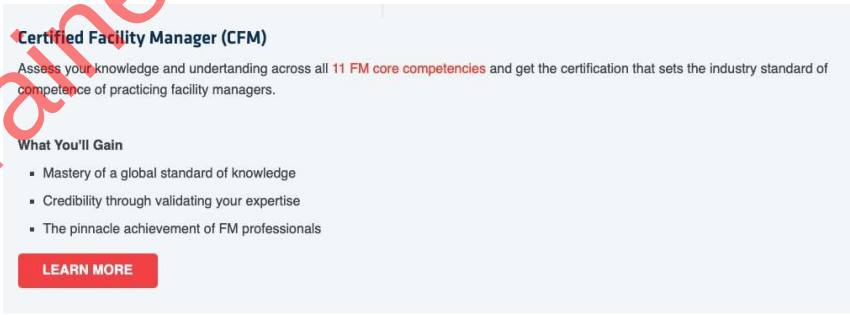
International Facility Management Association

Founded in 1980, IFMA is the world's largest and most widely recognized international association for facility management professionals, supporting over 23,000 members in more than 100 countries.

This diverse membership participates in focused component groups equipped to address their unique situations by region (142 chapters), industry (16 councils) and areas of interest (six communities). Together they manage more than 78 billion square feet of property and annually purchase more than US$526 billion in products and services.

https://www.ifma.org/

International Facility Management Association



https://www.ifma.org/

International Facility Management Association

Facility Management Professional (FMP)

Gain the skills you need. This is a great course for business professionals and others new to the facility management industry.

What You'll Learn

- Best practices for managing your facilities
- Effective strategies and critical thinking skills
- The four pillar areas of study for a strong foundation

LEARN MORE

https://www.ifma.org/

Any Questions?