KENYA INSTITUTE OF SECURITY AND CRIMINAL JUSTICE

DIPLOMA IN SECURITY MANAGEMENT

INTRODUCTION TO SECURITY MANAGEMENT

RISK MANAGEMENT

Introduction

In organizations security of assets has been viewed from different perspectives Patterson (2004) assets that to protect a company and its assets, the very first step is to perform a threat and vulnerability analysis. Based on that analysis the security team should implement physical protection systems (PPS) to provide safeguards that mitigate the threats.

The common thread of these approaches is that they characterize protection from the position of controls; "How good are our existing controls against perceived threats" this we can call the security approach. This is a specific narrow focus on threat and vulnerabilities and exclusive approach which activities usually are confined to security professionals.

Fisher, Halibozek and Green (2008) argues that there has been a paradigm shift in how we view security and risk, and take a more contemporary approach, which we can call the risk approach: The risk approach takes in account organizational contest, organizational objectives, assets and how they are used. It identifies threats to assets and the success of the mission. It quantifies the potential impact of those threats.

It identifies and addresses vulnerabilities and establishes a framework to manage risk to **as low as reasonably practical** (ALARP). This is an inclusive approach, designed to involve the business in risk management decision making. Specialist advice is provided by the security professionals, who lead and own the process.

The first step in security planning is a detailed analysis of potential areas of loss, their probability and their criticality in terms of business impact should a loss occur that affects corporate goals and assets. Only then can the specific objectives of security function be defined. This is referred to as the security risk analysis process.

These approaches characterize protection from the starting point of risk: "What are the risks that have the potential to impact on our mission and what are we going to do about it." The risk approach includes all of the elements of the security approach but it is presented as part of an enterprise-wide analysis using the language of business.

Importantly, it begins by establishing the context in which the organizations, its assets and its mission exist, and concludes with the assumption that while every security risk should be mitigated, there may be risk management alternatives to pure security solutions.

Definition of Key Concepts

1.1.1 a) ***Risk*** is defined as the measurement of the frequency, probability and severity of losses from exposure to threats and hazards.

b) Risk actually refers to two things:

1 The likelihood of a threat materializing
2 The degree of damage that can be expected if the threat occurs,

For security professionals- these two aspects of risk are referred to as a threats probability and criticality. Probability refers to the likelihood a threat will actually occur. Criticality is used to indicate the extent of damage if that threat occurs.

1.1.2 ***Threat*** refers to a serious, impending or recurring event that can result in loss and it must be dealt with immediately.

A threat is an item that is identified and placed on a list of specific events that may emerge in a target environment and that is likely to cause some form of loss to the target environment.

A threat is inherently a negative impact event, a possibility of some future time. Every threat has a risk component. The risk factor associated with a particular threat is almost always determined by environmental conditions.

List of Potential Threats

- Arson
- Burglary
- Explosion
- Fire
- Embezzlement
- Terrorism
- Sabotage
- Shoplifting
- Severe weather
- Battery
- Extortion
- Sexual harassment
- Personal injury
- Theft
- Internal Strife
- Parking lot crime
- Vendor theft

1.1.3 A ***hazard*** is a source of danger that has the potential to cause unwanted outcomes such as injury, death, property damage, economic loss and environmental damage that adversely impact on society.

1.1.4 ***Vulnerability*** refers to any weakness or flaw in the physical layout, organization, procedures, management, administration, hardware or software that may be exploited to cause harm to the institution, business or activity.

A ***Vulnerability gap*** is the difference between the level of security in place and the level of security needed for appropriate protection in a target environment. The larger the vulnerability gap, the higher the risk factors in terms of probability and/ or criticality associated with the threat.

1.1.1 **Risk Analysis**: This refers to a complete and thorough assessment of the perils and hazards that a business may face.

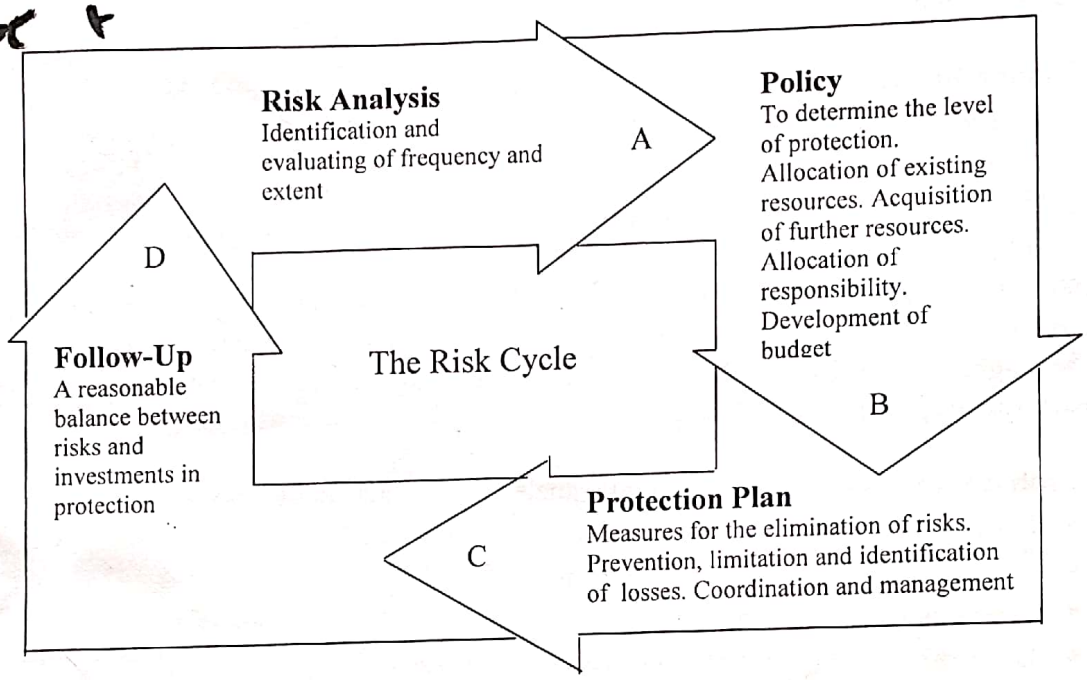
1.1.2 **Risk Management** involves anticipating, recognizing and analyzing risks taking steps to reduce or prevent such risks and evaluating the results

3.2 **Risk Assessments**

Risk ~~management~~ assessment is a complex challenge to security managers. They must define and analyze all risks companies may encounter to make it possible to restrict the number of and scope of such disturbances. Risk ~~management~~ assessment is a comprehensive system of measures aimed at achieving that end.

3.2.1 **Understanding the Risk Cycle**

An efficient, effective, non-crisis oriented security system should be put in place to prevent losses in business. It should also consider all the stakeholders.



The Risk Cycle

The risk cycle is a systematic approach to preventing loss through risk management. It includes risk analysis, policy formulation, specification of a protection plan and follow-up.

3.2.2 **Risk Analysis:** Its purpose is to create awareness within a company of any risks and to determine their potential influence on the business.

3.2.3 **Policy Formulation:** The necessary security measures are arranged in order of importance, the cost of such measures is computed and management determines the level of protection the company should choose.

3.2.4 **Protection Plan** is specified that includes which risks are to be eliminated and how, the degree of need for loss prevention and loss limitation, risks to be insured and allocation of responsibility, management and coordination.

3.2.5 **Follow-up** should insure a reasonable balance between the risks with which a company has to live and the protection against these risks.

3.3 **Risk Analysis**
There are three factors to consider in risk analysis:

1. Vulnerability
2. Probability
3. Criticality

3.3.1 **Vulnerability:** Establish vulnerability involving threat areas.

- Where could losses occur?
- How?
- What types of thefts might occur?
- What safety hazard exists.

Security managers should consider their vulnerability to such risks as accidents, arson, assault, auto-theft, bombs, burglary, fraud, kidnapping, larceny/ theft, robbery, sabotage, sex crimes, shoplifting and vandalism. Vulnerability to natural disasters like earthquakes, floods, tornadoes, fires e.t.c. should be considered.

3.3.2 **Probability:** Establish probability by analyzing the factors that favor loss

- Is the establishment located in high or low crime area?
- How tight is the existing physical security?
- Where is shrinkage occurring?
- Is it primarily due to internal or external causes?
- Where is it more likely to occur?

3.3.3 **Criticality:** This involves deciding whether a loss, if it occurs, would be of minimum or maximum consequences

- How serious would it be?

2.0 Management of Risks

Once the risks have been identified, measures are taken to reduce vulnerability to the risks. Risk management is a logical systematic approach to deal with the recognized hazards.

The alternatives for handling risk include the following:

- Risk elimination
- Risk reduction
- Risk spreading
- Risk transfer
- Risk acceptance

2.1 Risk Elimination

Where possible and practical, eliminate the risk entirely. Losses from cheques can be eliminated by refusing to accept cheques/ credit card.

2.2 Risk Reduction

Where risks cannot be eliminated, they can be reduced by establishing certain procedures and use physical hardware to reduce or minimize risk. For example- installing locks, security lighting and alarm systems can reduce the risk of loss from burglary by helping to delay and/ or detect intruders.

2.3 Risk Spreading

The risk can also be spread. This approach uses methods that ensure that the potential loss in any single incident is reduced. For example: placing expensive jewelry in separate display cases.

2.4 Risk Transfer

Risk may be transferred by taking out an insurance cover e.g. insurance against fire and other natural disasters.

2.5 Risk Acceptance

If the value of the assets is low, the cost of recovering from the incident is low and the threat is low, risk can be accepted. Risks can never really be eliminated.

3.0 Conclusion

Corporate/ Retail/ Private Security managers must recognize, and deal with both pure- risks which have the potential for injury, damage or loss with no possible benefits. They should also deal with dynamic risks that have the potential for both benefits and losses. A systematic approach to preventing loss through risk management includes risk analysis, risk policy formulation, specification of a protection plan and follow-up. An effective tool for analysis is the security survey.

[redacted]