DLE 2083: INTRODUCTION TO SECURITY MANAGEMENT

CHAPTER 9

CONTROLS AND STRATEGIES

VISION COLLEGE

Chapter 9: Learning Outcomes

- At the end of the topic, students should be able to:
  - Defined controls and strategies.
  - Explained on establishing tolerable risks.
  - Explained the six "T" strategies to controls risk.
  - Understand the importance to protect critical infrastructure of the country.

Defining Control

- A control is anything that was intended to or effectively does reduce a risk.
- If a control reduces a risk, the **pre-control** state of the risk is usually known as the **inherent risk**, while the **post-control** state is usually known as the **residual risk**.

Defining Control

- The control is not necessarily an absolute solution to the risk.
- It may reduce a risk to a still intolerable level or to an only temporarily tolerable level.
- Consequently, good risk management processes prescribe monitoring the risk, even after control.

Establishing Tolerable Risks

- Tolerable risk is the risk remaining after suitable and sufficient controls have been applied to significant hazards that have been identified, assessed, communicated to the appropriate stakeholders and sanctioned after proper evaluation.

Establishing Tolerable Risks

- The concept of reducing the residual risk to tolerable levels is nothing new, the fact that, for all practical purposes, the products, processes or services we utilize are not risk-free is tolerated by all of us.

Defining Strategy

- A risk management strategy is any purposeful response to insecurity or risk.
- The strategy might be emergent or subconscious, but must aim to affect security or risk.

Defining Strategy

- The strategy is usefully distinguished from the controls.
- The particular actions used to change a particular risk, such as a guard acquired as part of a protective strategy.

The Six “T” Strategies

- The six “T” strategies to controls risk consist of:
  1. Tolerate the risk
  2. Treat (Terminate) the risk
  3. Turn the risk
  4. Take the risk
  5. Transfer the risk
  6. Thin the risk

1. Tolerate the risk

- The strategy of toleration might be also known as acceptance.
- A bank is fully aware of its risks and puts in the necessary controls. But if risks occur after the event, the bank will accept it.
  - For example risk due to natural disaster such as flood or earthquake is beyond the control of bank organization and they need to accept the remaining impact or also known as residual risks.

2. Treat (Terminate) the risk

- If we were to decide that we could not tolerate a risk, we should treat the risk.
- Treating the risk means the application of some control to a risk in order to reduce the risk, ideally to a tolerable level, possibly until we terminate the risk.
- A strategy of termination includes prevention of things like the threat's intent or capabilities or our exposure to threats.

3. Turn the risk

- We could effectively terminate the risk by turning the source or cause in our favour.
- For example, rather than kill the leader of the criminal gang, we could ally with it against another threat or offer a cooperative return to lawful activities.
- The strategy of turning the risk offers more than either terminating or taking the opportunity because it turns a negative into a positive risk.

4. Take the risk

- Taking a risk is a deliberate choice to pursue a positive risk, even if negative risks are taken too.
- The strategy of taking risk is known elsewhere as a strategy of pursuing, enhancing, or exploiting positive risks.
- Taking risk could include accepting some potential negative returns, as long as we are simultaneously pursuing positive risk.

5. Transfer the risk

- Transferring the risk means that we transfer some of the risk to another party.
- A bank can take insurance to transfer portion of the risk (e.g. robbery case) to the insurance company.
- A bank also can outsource certain operations which they don’t have much expertise to handle it.

5. Transfer the risk

- This can give the bank opportunity to be more focusing on their core business activities.
- For example, a bank can hire security services to taking care the bank safety and security or appoint contractor for maintenance services purposes of the bank.
- Contractors who agree to provide the bank with some service effectively share the risk of their non-performance.

6. Thin the Risk

- Thinning the risk is a strategy known usually as diversification.
- It is a unique strategy that does not terminate, turn, take, transfer, or treat any particular risk but nevertheless reduces our total risk by spreading or thinning our loss exposure across more diverse types of risks, sites, partners, providers, etc.

6. Thin the Risk

- You could take on more types of risk while reducing your total negative risk, although at the same time you may reduce your potential positive returns.

Security for Critical Infrastructure

Introduction

- Critical infrastructure is vital for essential functioning of a country.
- Incidental or deliberate damage will have serious impact on the economy as well as providing essential services to the communities it serves.

Introduction

- Infrastructure security is the security provided to protect infrastructure especially critical infrastructure such as:
  - Airports
  - Highways
  - Rail transport
  - Hospitals
  - Bridges

VISION COLLEGE

Introduction

- – Transport hubs
- – Network communications
- – Media
- – Electricity grid
- – Dams
- – Power plants
- – Seaports
- – Oil refineries
- – Water systems

VISION COLLEGE

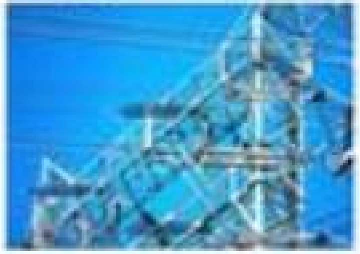
Roads

Airports

Harbors

Railway systems

Energy networks



Utility systems

Education

Healthcare

Social Infrastructure

Introduction

- Critical infrastructures basically utilize and relying on information technology.
- As a result, they have become highly interconnected and interdependent.
- Intrusions and disruptions in one infrastructure might provoke unexpected failures to others.

Potential Causes of Infrastructure Failure

- There are few reasons why infrastructure needs to be heavily secured and protected.

1. Terrorism

- Person or groups deliberately targeting critical infrastructure for political gain. E.g. In November 2008 Mumbai attacks, the Mumbai central station and hospital were deliberately targeted).

Potential Causes of Infrastructure Failure

2. Sabotage

- Person or groups such as ex-employee, political groups against governments, environmental groups in defense of environment. (E.g. Bangkok's International Airport Seized by Protestors).

Potential Causes of Infrastructure Failure

3. Information warfare

- Private person hacking for private gain or countries initiating attacks to glean information and also damage a country's infrastructure.

VISION
COLLEGE

Potential Causes of Infrastructure Failure

4. Natural disaster

- Tsunami, earthquake, and other natural events which damage critical infrastructure such as oil pipelines, water, and power grids. E.g. Tsunami in Acheh, 2004.

VISION COLLEGE

Security Challenges For The Electricity Infrastructure

- One of the fundamental foundations of modern society is the electrical power systems.
- An intentional disruption of electricity supplies would affect national security, the economy, and every person's life.
- Because power grids and their sources are widely dispersed, this is a challenge for the effectiveness of defensive organizations and structure.

Security Challenges For The Electricity Infrastructure

- Sabotage can damage electrical sources for the power grid, including civilian nuclear power stations.
- Sabotage in the form of cyber attacks can create havoc with computer, communication, and information systems, which could severely interrupt the electrical supply.
- This in turn can cause major disruptions to other infrastructure components of society.

Security Challenges For The Electricity Infrastructure

- One method is to isolate load systems.
- Sophisticated defense systems should be wide-area, real-time protection, with control systems that are alerted and guided by sensing technologies.
- Communication and information must be capably routed.

National Security Measures

- A number of government organizations has focus on infrastructure security and protection.
- In Malaysia, the Ministry of Home Affairs (KDN) and National Security Council (MKN) are the government agencies had been directly involves in managing the security critical infrastructure of the country.
- There were dedicated security agencies also to protect the facilities such as Auxiliary Police.