



Physical Security



Presented for: PISA

By: Penny FUNG of IPSA(HK)

Date: May 25, 2006

AGENDA

- Basics
 - What is Physical Security?
 - What does it involve?
 - What are the objectives?
 - How to achieve the objectives?
- Common Mistakes
- Good Practice
- Other Considerations
- Q & A



BASICS

What is Physical Security?

“Physical Security means the physical measures designed to safeguard personnel, property, and information.”

(ASIS International)



IPSA(HK) Ltd.

3

BASICS

What does it involve?

Architectural Features

- Location / Layout
- Barriers / Doors
- Locks & Bolts
- Lighting

Electronic Systems

- Access Control System
- Alarm System
- CCTV System
- Communications

Staff and Procedures

- Deployment
- Policies & Procedures
- Communications
- Training



IPSA(HK) Ltd.

4

BASICS

What are the objectives?

- Deterrence
- Detection
- Delay
- Response



BASICS

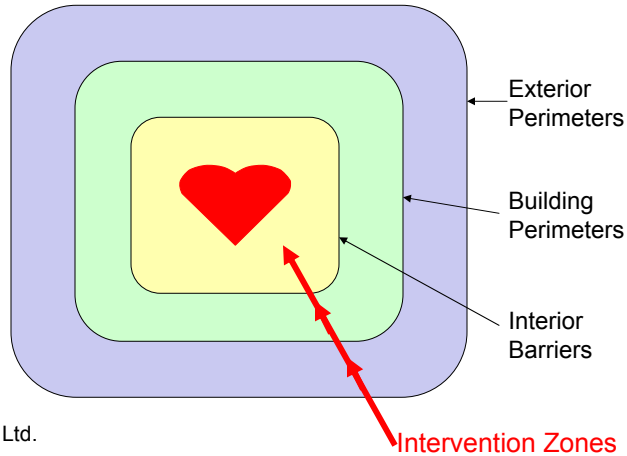
How to achieve the objectives?

- Protection in Depth
- CPTED
- Risk-based approach



BASICS

Protection in Depth



IPSA(HK) Ltd.

Intervention Zones 7

BASICS

CPTED – Crime Prevention Through Environmental Design

“The proper design and effective use of the built environment can lead to a reduction in the fear of crime and the incidence of crime, and to an improvement in the quality of life.”

(Dr. Jeffery, Crime Prevention Through Environment Design)



IPSA(HK) Ltd.

8

BASICS

The 3D's of CPTED

- Designation
- Definition
- Design



BASICS

Risk-based Approach

- Preparation
- Resource Appreciation
- Audit of existing security strategies
- Threat assessment
- Identification of vulnerabilities
- Formulation of strategies and recommendations



BASICS

Strategies

- Reduction
- Transfer
- Avoidance
- Redistribution
- Acceptance



BASICS

Recommendations

- Practicality
- Cost-effectiveness

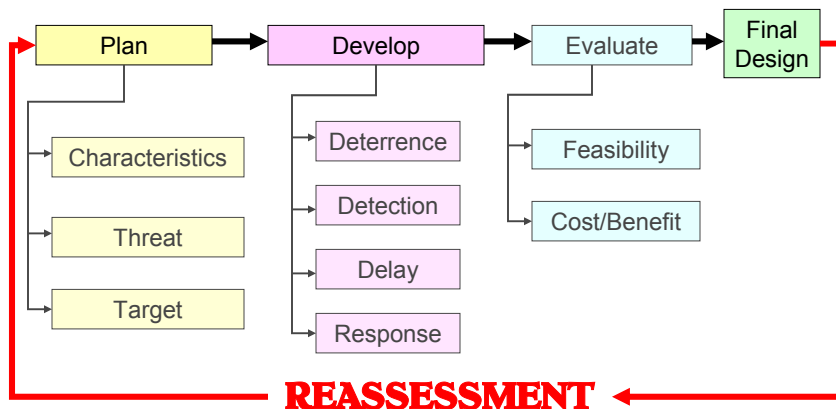


COMMON MISTAKES

- Putting security before lives
- Not knowing what is at risk
- Not achieving the objectives
- No policies and procedures
- Not integrated with business operations
- Low staff awareness of policies and procedures
- No information classification
- Not compliant with local rules and regulations relevant to physical security
- No business continuity planning



GOOD PRACTICE



OTHER CONSIDERATIONS

- Safety first
- Support business mission
- Adopt risk-based approach
- Integrate with business operations
- Aim at achieving the objectives of deterrence, detection, delay and response
- Plan for business continuity
- Comply with rules and regulations
- Establish policies and procedures
- Raise staff awareness
- Periodic review and continuous improvement



DISCUSSION

