UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Chapter 14

Always A Pioneer, Always Ahead

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

UTeM

Assessment of Resources in Physical Security System

Dr Zaheera Zainal Abidin

zaheera@utem.edu.my

MyUTeM

By the end of the lesson the student will be able to:

a) understand the assessment of resources available in the physical security system

b) understand the mitigation plan to protect the resources in the physical security system

OVERVIEW

- Introduction to physical security assessment
- Acceptable Level of Risk in the Organization
- The mitigation Plan to protect the resources
- Action Plan or Assessment Checklist

INTRODUCTION

INTRODUCTION – 1

- Physical security is responsible for developing and enforcing controls to secure the software security management, hardware security management, resource talents, applications policy and procedures.
- Organization must consider about the computer installation, backup facility, office organization and personnel background checks.
- Organization measures the level of security using baseline or security parameter to ensure the safety at the acceptable level.
- To make sure that the security is at the maximum protection, assessment need to be done.

INTRODUCTION – 2

- After the security has been implemented in the organization, then how to know that the security is effective enough? Need to do the balance check.
- Why does the assessment is vital?
  - To know the current cost involved, resources and talent in the office.
  - To check the integration of various programs or hardware or software applications align / meet between the business requirements and security performance.
- A comprehensive vulnerability assessment and risk measures are important to understand the security performance in an organization.

ACCEPTABLE LEVEL OF RISK IN THE ORGANIZATION

ACCEPTABLE LEVEL OF RISK

- Based on the nature of the business, organization must define the acceptable level of risk and sets a certain threshold values for security parameter measurements.
- The method for study the acceptable level of risk is by using either quantitative approach or qualitative approach or both.
- Organization must has an acceptable level of risk table.

EXAMPLE

- The location of automated teller machine (ATM) at the shopping mall.

ATM Location	Requirement	Acceptable Risk Level
Banking Area	Guard + CCTV	Low
ATM Area	CCTV	Medium
ATM Area	No CCTV	High

Table 1: Acceptable Level of Risk

- The level of acceptable risk is depending on the location, security policy, procedure and at the specific time of implementation.

MITIGATION PLAN

MITIGATION PLAN

- Develop a table consists of list of resources (assets, hardware, software, talent, cash), vulnerability, threat and attack.
- Identify policy and guideline to follow method and model.
- From the table created, identify area under study, measurement criteria and resources.
- Decide on scoring using quantitative or qualitative.
- Mapping the resources with weight or metric or scorecard, compliance assessment, incidents and vulnerability assessments.
- Define all output plan (progress meetings, documents, report, action plans, presentation and video).

ASSESSMENT CHECKLIST

ASSESSMENT CHECKLIST

- What preventive measures currently you have in place? (✓ or X or **NULL**)

No.	Description	Status (✓ or **X** or **NULL**)
1.	Access to area of protection limited to personnel?	
2.	Monitor the physical keys and access codes?	
3.	When employee left the company, all access codes are terminated?	
4.	Use CCTV to monitor areas that difficult to view?	
5.	Employee did the medical check-up?	
6.	Complaint to Public Safety when incident occurred?	

ASSESSMENT CHECKLIST

- What protection measures currently you have in place? (✓ or X or **NULL**) – [The place is computer lab / IT Facility]

No.	Description	Status (✓ or **X** or **NULL**)
1.	Is the system located at stable surface and grounded ?	
2.	Is the system safe from dust, humidity and extreme temperatures?	
3.	Is the room is secured by lock and alarm system?	
4.	Are these locks and alarms activated during off hours?	
5.	Is the power and reset switches disabled?	
6.	Is your physical network secured or encrypted?	

Checklist

Electric Field Sensors

Exterior Perimeter IDS

Interview Items

Installation location: _____

Operational test frequency: _____

Operational test method: _____

Sensitivity test frequency: _____

Sensitivity test method: _____

Acceptance criteria for sensitivity test: _____

Procedures for vegetation removal: _____

Procedures for snow removal: _____

False alarm history/records: _____

Make/model: _____

Physical Security Systems Assessment Guide – December 2016

Data Collection Sheet
Exterior Perimeter CCTV System

Test Method

	Zone Tested	Functional Test	Field of View Test	Obstruction Test	Speed of Response Test
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
Comments:					

CONCLUSION

CONCLUSION

- The assessment assists the organization to discover unknown things about your environment.
- To determine that actions taken and policy implementation have follow the security standard and procedure.
- To understand if you are compliant to legal and regulatory requirements.
- The assessment of resources help the management to make decision on financial dan budget.

Thank You

MyUTeM

www.utem.edu.my