

Protection of Essential Infrastructure and Services

NOR'AZUWA MUHAMAD PAHRI
CONSULTANT, MIMOS CONSULTING GROUP,
MIMOS BERHAD
azuwa@mimos.my

MIMOS Consulting Group
"Valuing Trust, Lasting Partners"

Table of Content

- Introduction
- Reality of Cyber Attack
- CyberSecurity Issues & Challenges
- CyberSecurity Components
- Way Forward

MIMOS Consulting Group
"Valuing Trust, Lasting Partners"

Introduction

Protection of **Essential Infrastructure** and **Services**

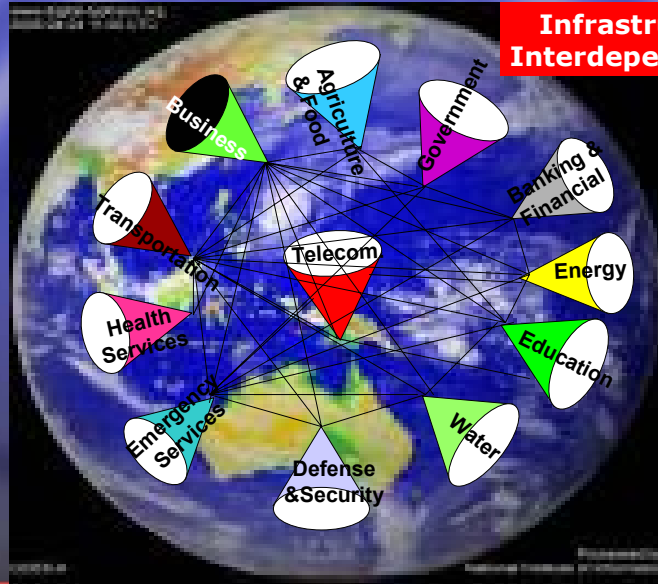
- Protection = **CYBERSECURITY = THE DEFENSE AGAINST CYBER ATTACKS**
- Essential Infrastructure = **CRITICAL INFRASTRUCTURE = ASSETS (REAL AND VIRTUAL), SYSTEMS AND FUNCTIONS.**
- Services = **BUSINESS**

Introduction

- **Cybersecurity Is Vital For The Continuity Of Critical Infrastructure Services In Ensuring The Business Continuity.**
- **Eventually, The Failure Of These Critical Infrastructure Will Affect The Economy, Image, Defense.**

Introduction

Infrastructure Interdependencies



MIMOS Consulting Group
"Valuing Trust, Lasting Partners"

Introduction

Reality of Cyber Attack

- Known/Unknown Vulnerabilities
- It can be spreaded / infected
- Significant Injuries
- Major/minor Failure
- Unhealthy Business & People
- Unhealthy Image

MIMOS Consulting Group
"Valuing Trust, Lasting Partners"

Introduction

Reality of Cyber Attack

Cyber Attack = **DISEASE**

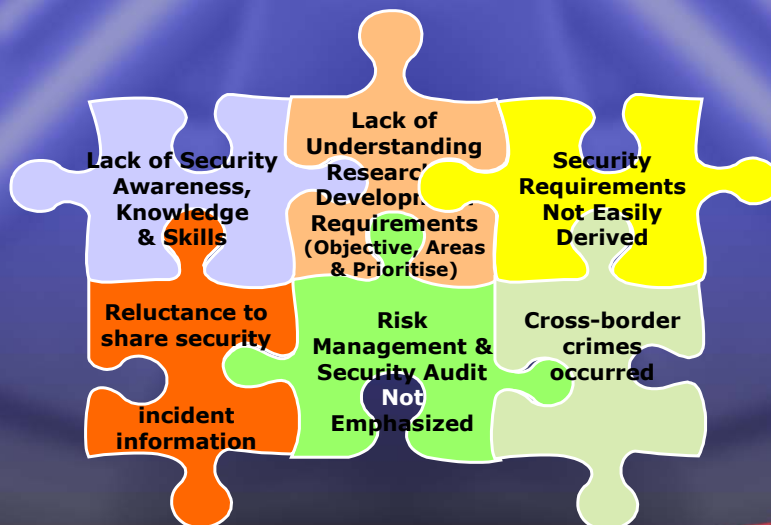
Protection = **Medicine/Vitamin**

“Prevention is Better than Cure”

“A healthy mind lives in a healthy body”

MIMOS Consulting Group
“Valuing Trust, Lasting Partners”


CyberSecurity Issues & Challenges



MIMOS Consulting Group
“Valuing Trust, Lasting Partners”



CyberSecurity Components



Awareness & Education

- Awareness : Using the security best practices and efficient technologies
- Education : Provide competent knowledge and skills to handle and response on cyber attack

- Cybersecurity technologies, eg. Authentication, Crypto, Access Control, System Integrity, Audit and Monitoring Security Audit Tools, etc.
- Minimum security requirements and security controls to deployed and the process to validate the security level of product/services before the procurement.



Technology

MIMOS Consulting Group
"Valuing Trust, Lasting Partners"

CyberSecurity Components

- Cooperation with R&D institutions to address existing cybersecurity threats



Security Standard

- Reference to Security Standards i.e. ISO 17799 ISMS, ISO 15408 CC, etc.

- Effective reporting structure, efficient response process plan and information sharing

Incident Response & Handling

MIMOS Consulting Group
"Valuing Trust, Lasting Partners"

CyberSecurity Components

Business Continuity Management

- To identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.

- Regular Security Audit to be conducted within and across the sectors
- Monitor the incoming and outgoing activities.

Security Audit & Monitoring

Physical Security

- Prevention of unauthorised access to the premises and data center
- Securing business operation equipments, eg. Server, Firewall, routers, PCs, Backup Media, Cabling, etc.

MIMOS Consulting Group
"Valuing Trust, Lasting Partners"

CyberSecurity Components

Public & Private Cooperation

- Coordination of cooperation & partnership arrangements between Public and Private sectors

- Regulatory and legislative governing operations and implementations of security systems (Compliance)

Regulatory & Legislative

International Cooperation

- Benchmark against international model and standards

MIMOS Consulting Group
"Valuing Trust, Lasting Partners"

Some References of National Critical Information Infrastructure Protection

Country	Central Coordinating Body on Information Security
South Korea	Korea Information Security Agency (KISA)
Singapore	Infocomm Development Authority (IDA)
United Kingdom	National Infrastructure Security Coordination Center (NISCC)
United States	Department of Homeland Security (DHS) - "National Strategy to Secure Cyberspace"

MIMOS Consulting Group
"Valuing Trust, Lasting Partners"

Way Forward

- Cybersecurity of critical infrastructure of APECTEL business **MUST** include **TECHNOLOGY, PEOPLE, PROCESS and POLICY** components
- APECTEL CyberSecurity Strategy should focus on, but not limited to :
 - Development of CyberSecurity Policy & Guidelines
 - Promoting Awareness and Increase The Efficiency of Security Training
 - Coordinate Information Sharing and Security Incident Response Process
 - Engagement and Interaction with public and private sectors.
 - Cooperation with International CERT