ICAO Asia/Pacific Regional Cybersecurity Webinar
"Management Framework for CNS/ATM Systems"
14 June 2021

A Proactive and Systematic Approach in Protecting Digitized Air Traffic Services against Cyber Threats in Hong Kong from ANSP and Regulatory Perspective

Presented by Hong Kong, China

Regulatory Perspective

Regulatory Perspectives

- Aviation Cybersecurity under Regulatory Regime in Hong Kong

  - HKASP Section 6.10 – Measures relating to Cyber Threats (Reference Annex 17 SARPs 4.9.1, 4.9.2)

  - Submission of Cybersecurity Programme by Air traffic control service provider.

Security Plan for Air Traffic Services

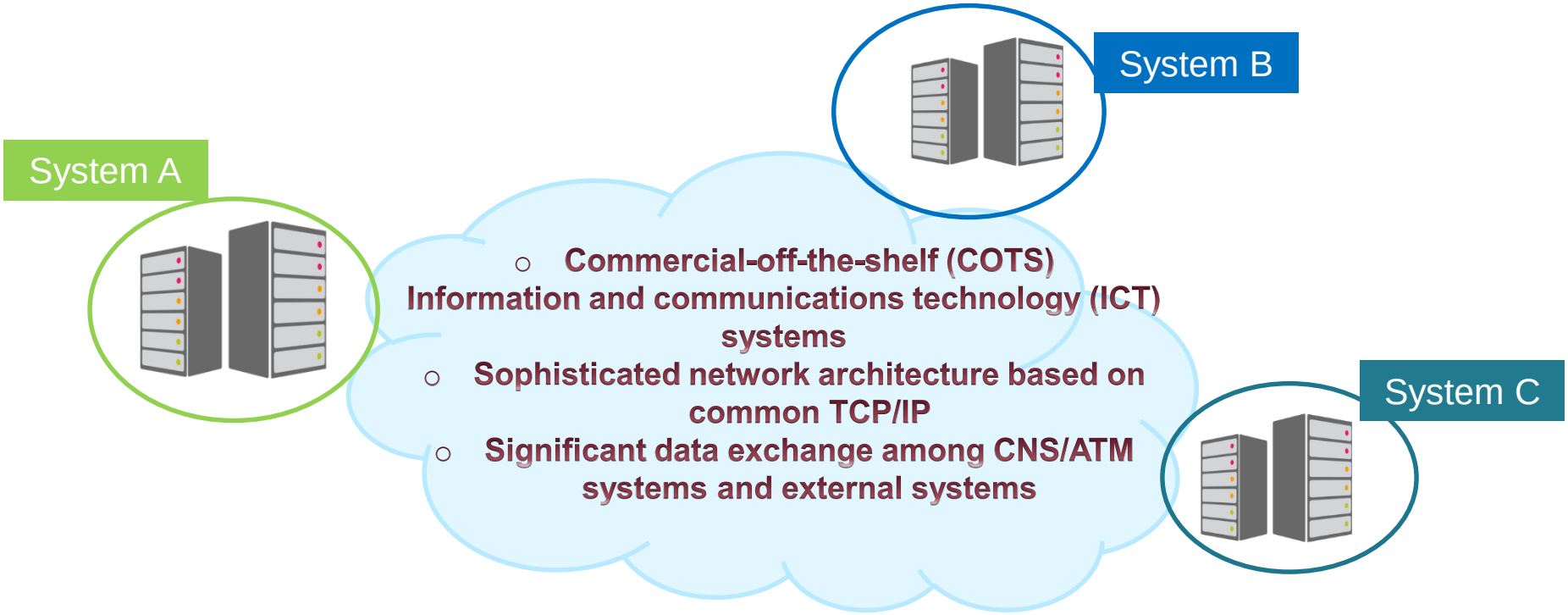
- Uphold a common baseline to work towards Cybersecurity Standards and Recommended Practices

  (Reference: Chapter 18 , Doc 8973)

Service Provider Perspective

Introduction

- New Generation of Air Traffic Services (ATS)
  - High level of digitization
  - Increasing interconnectivity



Introduction

- The Challenge for ANSPs:
  - Cyber threats might impact the safety and security of Air Traffic Services.
- Objectives
  - Protecting information data and physical assets against cyber threats
  - A proactive and systematic approach in implementation of cyber security measures to protect ATS from cyber threats.

Cyber Security Management in HKCAD

- HKCAD achieving the objectives by:
  - Setting up a cyber security management;
  - Managing cyber security processes in a proactive and systematic manner; and
  - Ensuring that all significant cyber threats risks to ATS are adequately addressed and mitigated.

Cyber Security Management in HKCAD

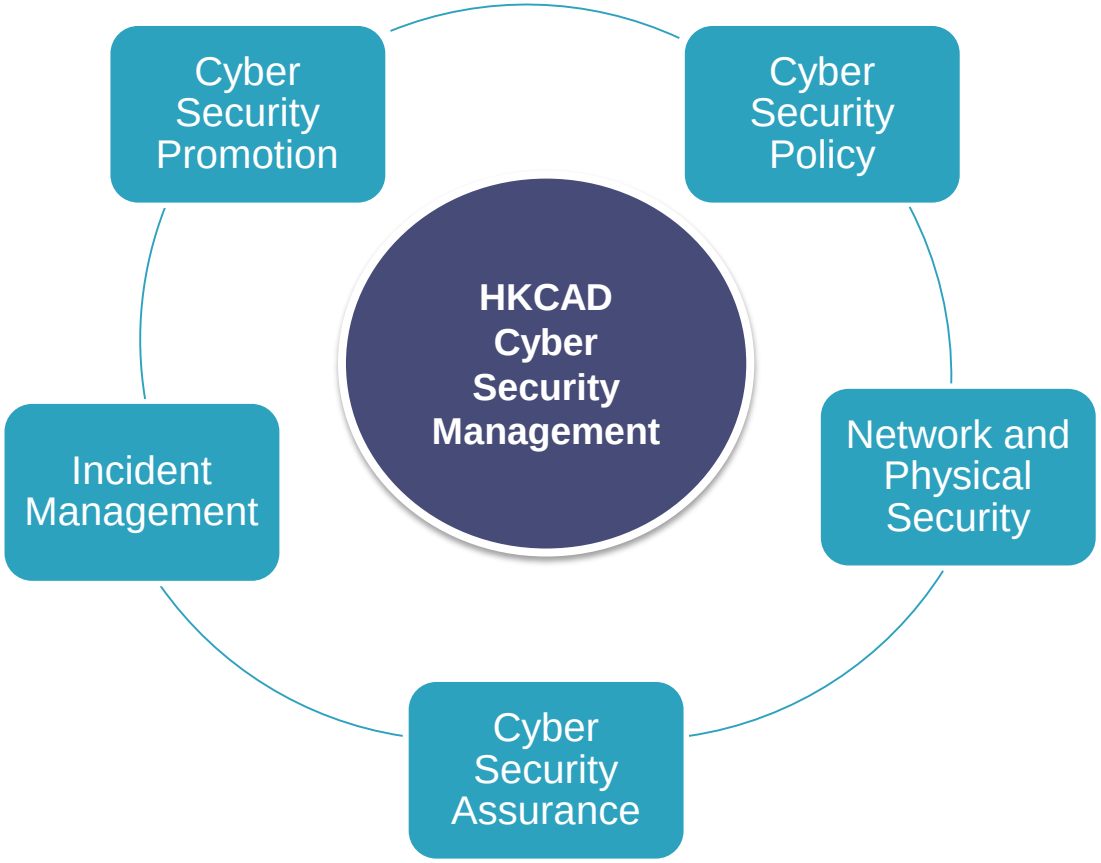
Establishment of CAD ANS Cyber Security Committee (CACSC)

- Regular meetings to set out policies and steer the implementation of cyber security control measures throughout the whole life cycle of the ATS systems.

- Committee members are from various perspectives (regulatory, operational and technical staff)

Cyber Security Management in HKCAD

- The key cyber security processes under HKCAD cyber security management are as follows:



Cyber Security Policy

- Documented Policy and Procedure
  - Developed documentation in accordance with ICAO Annex 17, Doc 9985 and Doc 8973
  - Provide protection of safety-critical ATS systems against cyber threats

1. Cyber Security Manual
2. Cyber Security Handbook
3. User Account Management Policy for ATS
4. Security Plan

Cyber Security Policy

- The “**Identify”** element of the framework is included in defining the security policy.
- A list of core ATS systems was identified with reference to risk management assessment process and business need, then documented the applicable scope in the policy.
- Based on the cyber threat risk management, business needs to prioritize the organisational efforts to implement physical and cyber security measures.

Risk Management

- Established cyber security assessment processes to identify hazards, and analyse, evaluate and mitigate risk to an acceptable level.

Cyber threats Identification

identify

Analyse & Evaluate

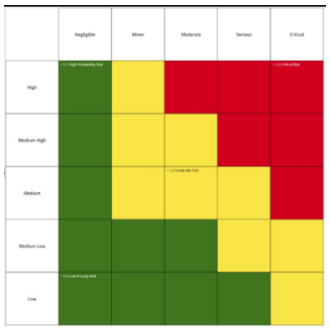
Severity of occurrences due to cyber threats

X

Probability (Likelihood)

Mitigate

Risk Categories and Acceptance Levels



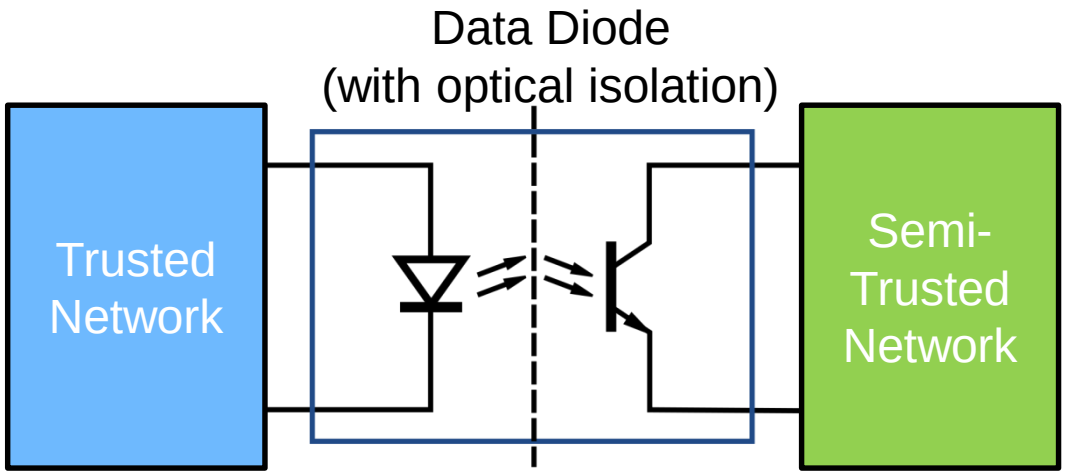
Risk Matrix

Network Security

- The “**Protect**” element of the framework is included in this process.
- ATS Systems interconnected for information exchange.
- Connection via a common Internet Protocol (IP) data network, Air Traffic Control Data Network (ATCDN)
  - Multi-tier defence-in-depth scheme
  - Network equipment with firewalls, Network Intrusion Detection System (NIDS) or Network Intrusion Prevention System (NIPS) to guard against external connections
  - Data Diode to allow uni-directional communication

Network Security

- Data Diode Network
  - Restrict uni-directional communication from trusted zone to semi-trusted zone
  - Optical isolation at transmitting and receiving ends
  - Uses for dissemination of surveillance multicast data



Network Security

- Removable Media Control
  - Common route for importing malicious content to information system.
  - Restrict the use of removable media
  - Media are scanned for malicious content by the machine prior to uploading data to ATS systems.

Physical Security

- Physical Security Measures
  - Multi-layer approach
  - From perimeter security down to console/rack level
  - Control measures include:
    - Facility management
    - Security guards
    - CCTV surveillance
    - Room access control
    - Physical lock, etc.

Cyber Security Assurance

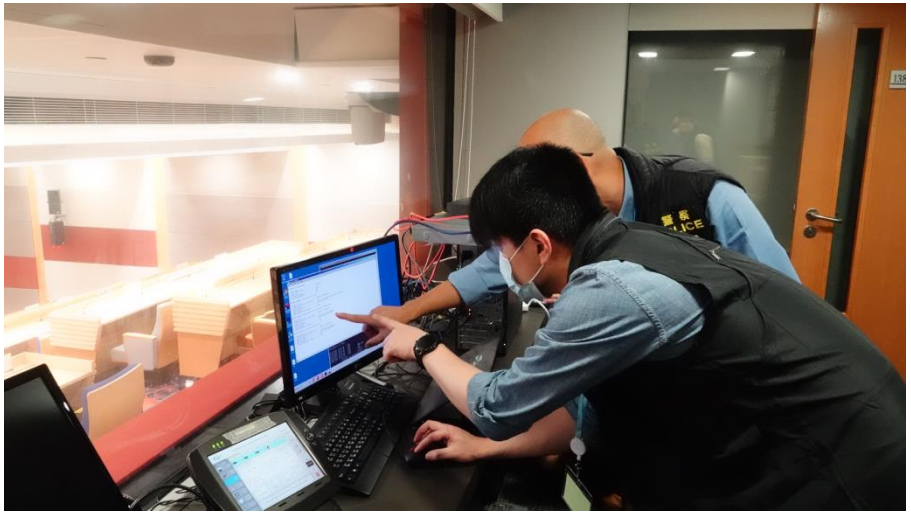
- The “**Detect”** element of the framework is included in this process.
- Performance Monitoring and Measurement
  - External and Internal Audit
- Continuous Improvement
  - Software Security Patch Management
    - Assess the requirements of security vs system performance.
    - Work closely with system manufacturers to evaluate system patch when considered appropriate.

Incident Management

- The "**Response" & "Recover"** element of the framework are included in this process.
- Established the escalation procedure of cyber security incidents
  - Work closely with Cyber Security and Technology Crime Bureau (CSTCB) of the Hong Kong Police Force (HKPF).
  - Direct reporting mechanism has established for HKCAD to seek swift assistance from CSTCB.
  - CSTCB provides advice and independent assessment on cyber security measures implemented.
  - Conduct drill exercises to keep up staff awareness and ensure the robustness of the response planning and recovery planning.

Incident Management

- The Joint Cyber and Physical Security Drill with HKPF was conducted at CAD Headquarters in April 2021 to enhance our response capability.
  - A storyline included both cyber and physical security incident to practice an all-rounded response.
  - Discovery, incident response and investigation activities were drilled to strengthen our readiness.



Cyber Security Promotion

- Staff awareness is essential to implement cyber security.
  - HKCAD provides cyber security training to our staff regularly to strengthen their awareness of cyber security.
  - HKCAD staff also raise their security awareness by participating in security drills, conference and seminars.


Q
&
A
QUESTION
ANSWER

Thank you


• Safe • Orderly • Efficient
• Airworthy • Teamwork
Committed to a Safe, Efficient and Sustainable Air Transport System