# Cyber Threat Landscape in Civil Aviation

ICAO APAC Regional Seminar on Aviation Cybersecurity

12-14 March 2025

Civil Aviation Department
Hong Kong, China

# Your Presenter

- **Management Trainee in HAECO** (2005-2011)
  - Quality Assurance
  - Production Planning & Control
  - Line Maintenance & Ramp Services

- **Operations Officer** (2011-Present)
  - **Flight Standards**
    MOR Scheme, SMS implementation, SSP
  - **Air Traffic Management**
    Safety and Quality Management
  - **Aviation Security**
    Avsec standards, air cargo security, screening equipment
    CMCs, background checks
  - **Avsec Professional Manager** (since 2017)

**Taka Chow**
Senior Operations Officer
(Avsec Support)
tctchow@cad.gov.hk

# Threat Landscape

- The evolving environment of
  - cyber threats
  - attack methods; and
  - attack vectors
  - targeting organisations, governments and individuals

- Essential for
  - identifying potential threats
  - monitoring attack vectors
  - Implementing defences

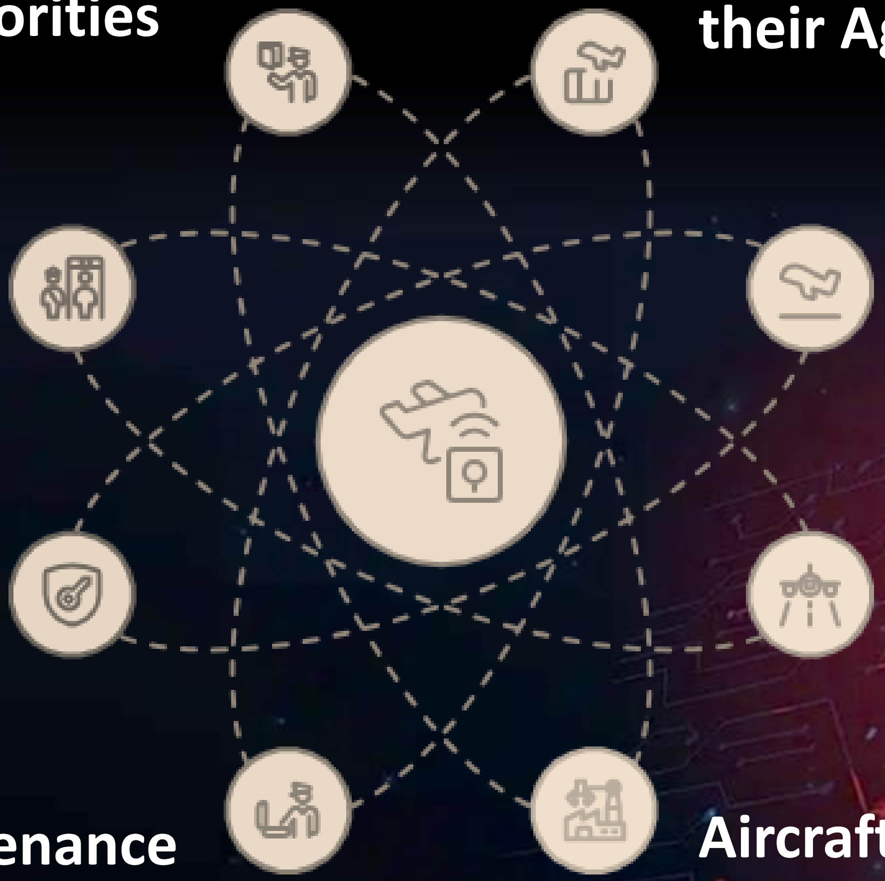
**Reduce breaches**
**Ensure resilience**

# Threat Landscape in Civil Aviation

- Usually a part of the critical infrastructure
  - Critical logistics for essential supplies
  - Critical transportation system
  - National security and public safety
  - Massive and prolonged interruption of traffic due snowball effect

- Legacy IT infrastructure and protection
- Systems highly interconnected

# Highly Interconnected Business



Government & Authorities

Airlines & their Agents

Security Contractor

Airports

Commercial & Supporting Services

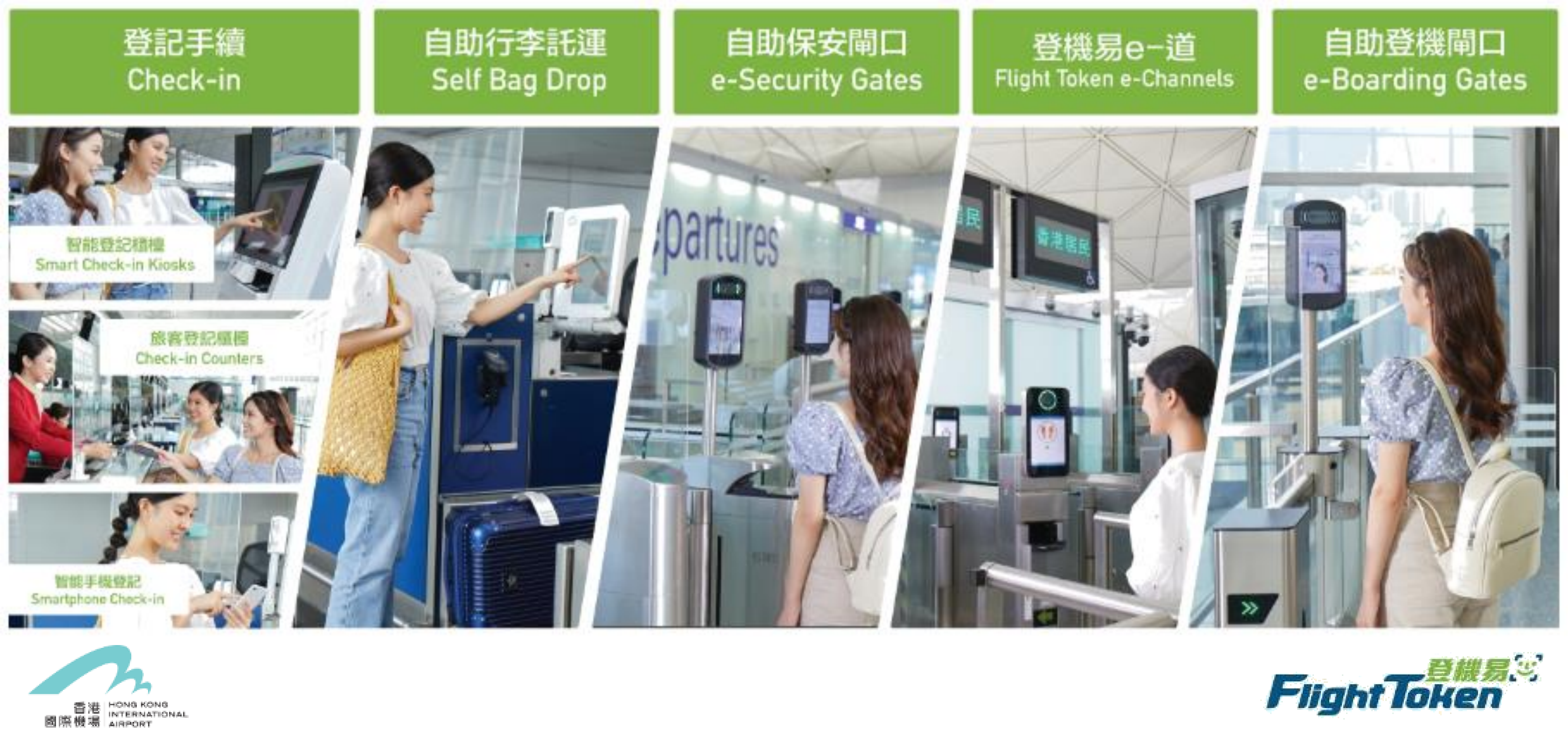
Air Traffic Control

Aircraft Maintenance & Services

Aircraft Manufacturer

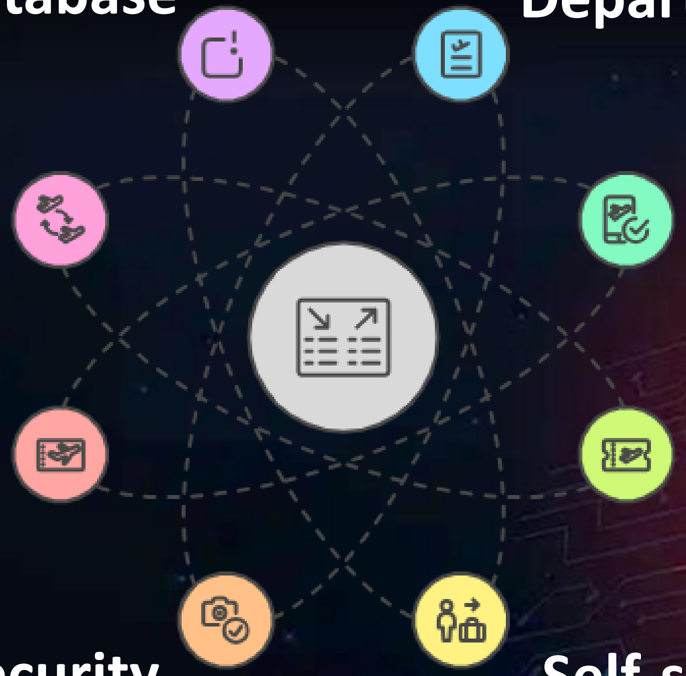
# Highly Interconnected Systems

## Example – HKIA’s Flight Token Journey



# Highly Interconnected Systems

## Example – HKIA’s Flight Token Journey



Border Control’s Database

Airline’s Departure Control

Immigration Clearance

Airline’s Mobile App

e-Boarding Gate

Airport’s Database

e-Security Gates

Self-service Kiosks
Self-Bag Drop

# Threat Landscape in Civil Aviation

Ransomware & Malware

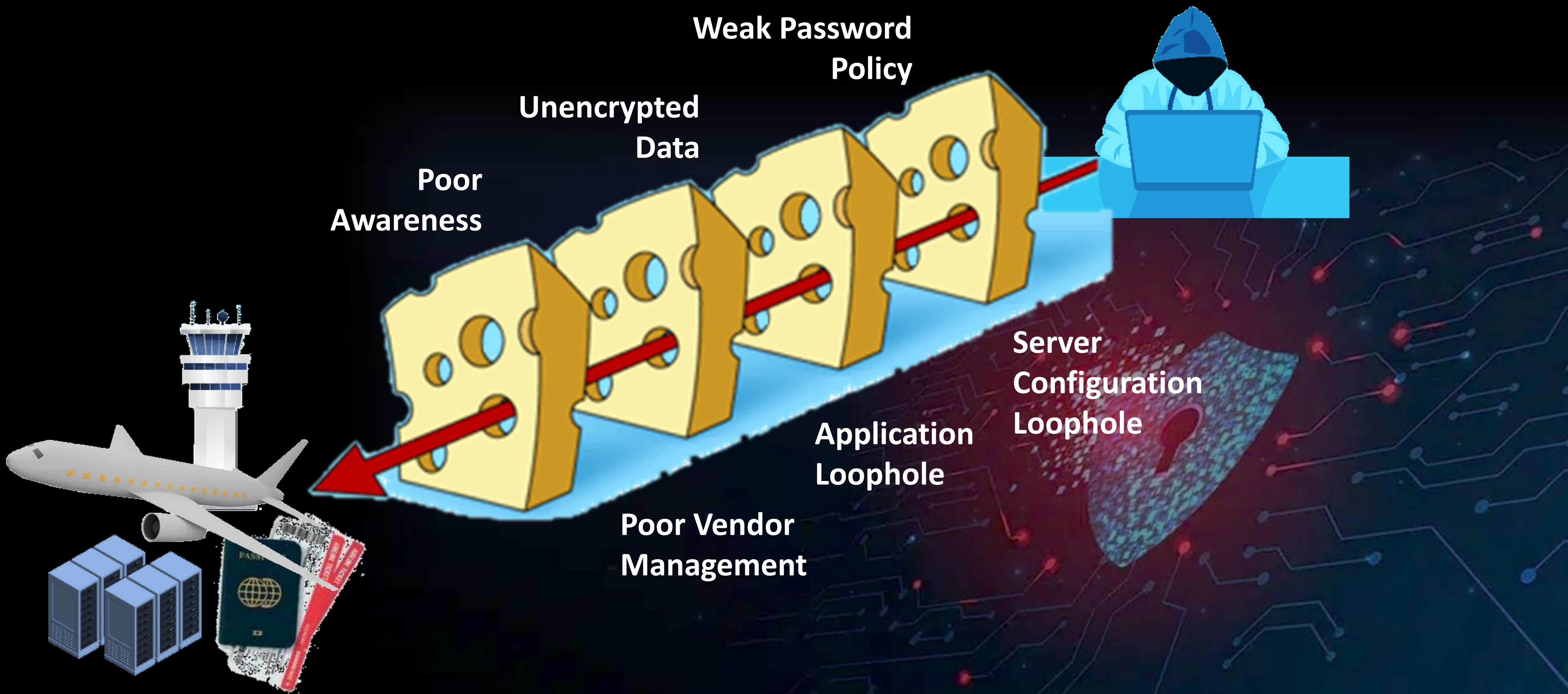
Social Engineering Attacks

Data Breaches & Leaks

Denial of Service DoS/DDoS

Zero-Day Exploits

# Interconnectivity x Vulnerability



Weak Password Policy

Unencrypted Data

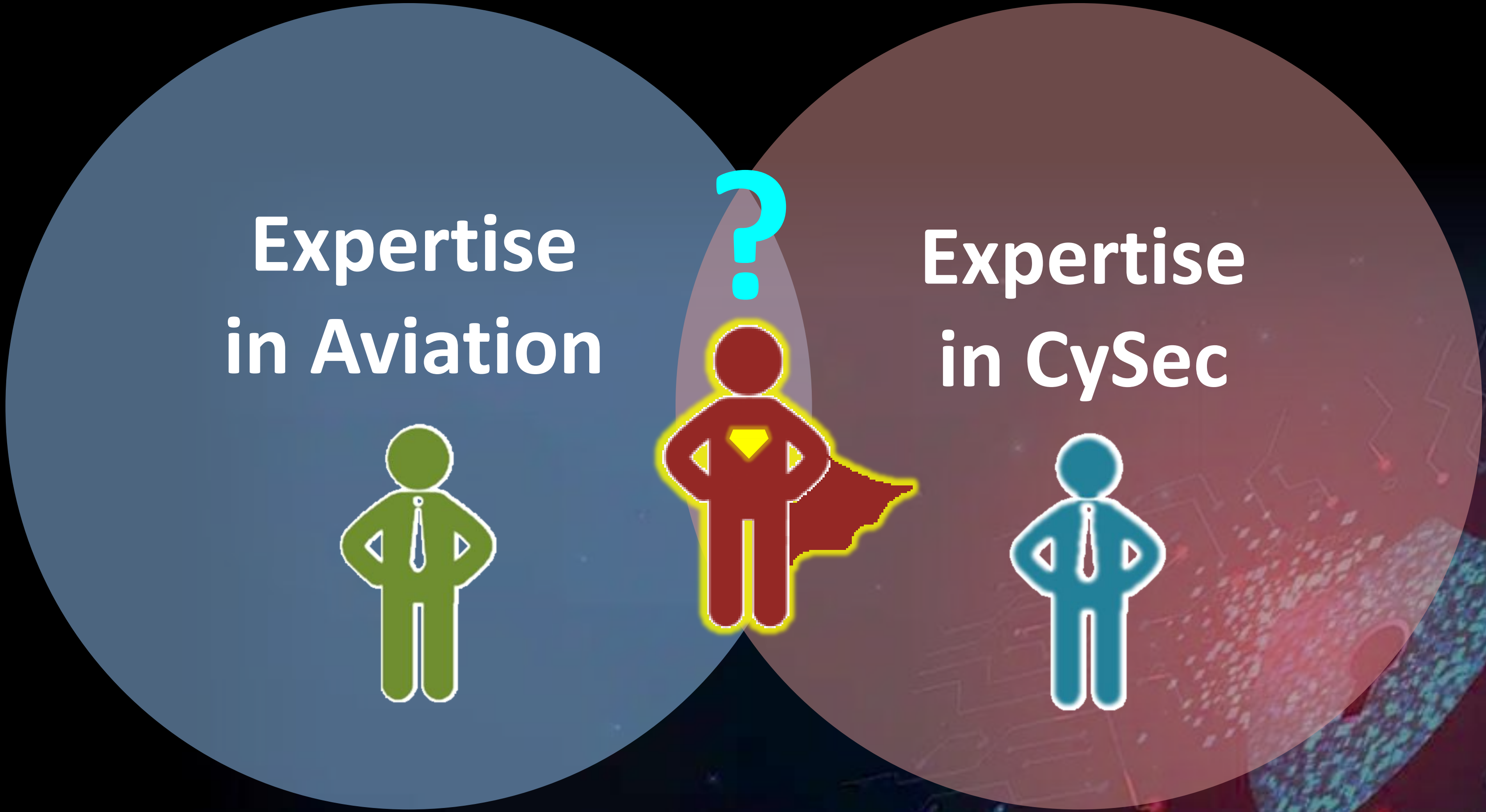
Poor Awareness

Server Configuration Loophole

Application Loophole

Poor Vendor Management

# Our Common Desire



Expertise in Aviation

Expertise in CySec

# Similarity between AvSec and CySec

Perimeter Protection

Physical Protection

Access Control

Access Rights/ MFA

Permit System

User Credential

Surveillance

Network Surveillance

Background Check

Blacklist/ Whitelist System

Screening

Virus/Malware Scanning

Segregation

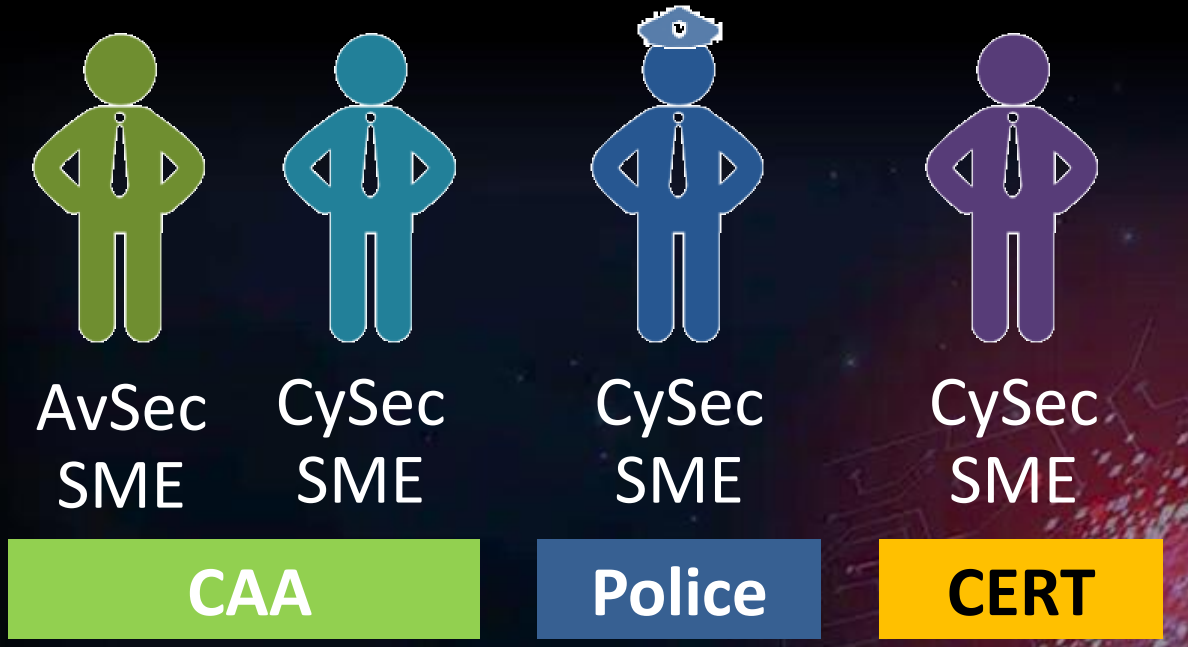
Network Segregation/ Firewalls

Behaviour Detection

Intrusion Detection

# Collaborative Approach

ICAO SARPs
& Guidance



AvSec
SME

CySec
SME

CySec
SME

CySec
SME

CAA

Police

CERT

Cyber Security
& Technology
Crime Bureau

Computer
Emergency
Response Team

Local CySec
Regulations

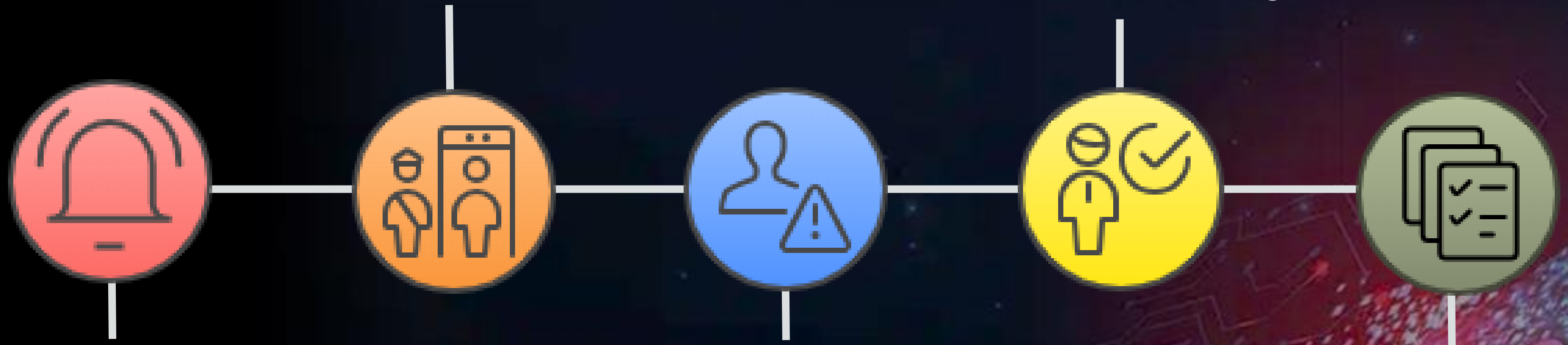
# Collaborative Approach
# Industry Best Practice

## ICAO SARPs & Guidance

## Local Avsec/CySec Regulations

## Industry Best Practice

# Case Sharing: Ransomware Attack



### Security Breach Identified

- Car park reservation system failed

### Access Impact

- CCTV system encrypted & failed
- Visitor pass system encrypted & failed
- Limited to security network

### Follow-up Actions

- Enhanced perimeter patrol
- Visitor pass to be issued by manual processing
- Report to Police / CySec Branch & Airport Division

### Medium-term Remedial Actions

- Third party forensic investigation
- Security hardening measures:
  - Limited remote access
  - Enhanced firewall
  - Reviewed network segmentation

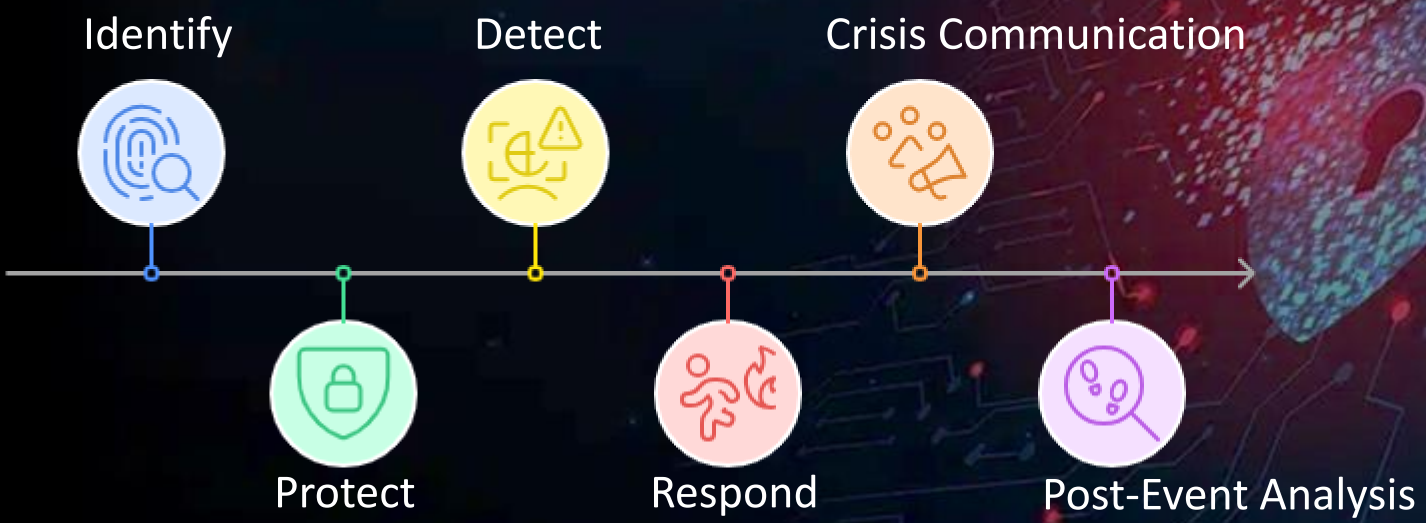
### Wrap-up

- CAD inspection to ensure effective implementation of remedial actions

# Conclusion

- Civil Aviation: A highly interconnected business
  - Critical infrastructure: a likely target of CySec attack
  - Single point of failure → interlocking malfunction

- Collaborative approach under ICAO’s guidance and local regulation:
  - AvSec SME (operational AvSec expertise) x CySec SME (technical)



Identify

Protect

Detect

Respond

Crisis Communication

Post-Event Analysis

# Thank you

Civil Aviation Department
Hong Kong, China