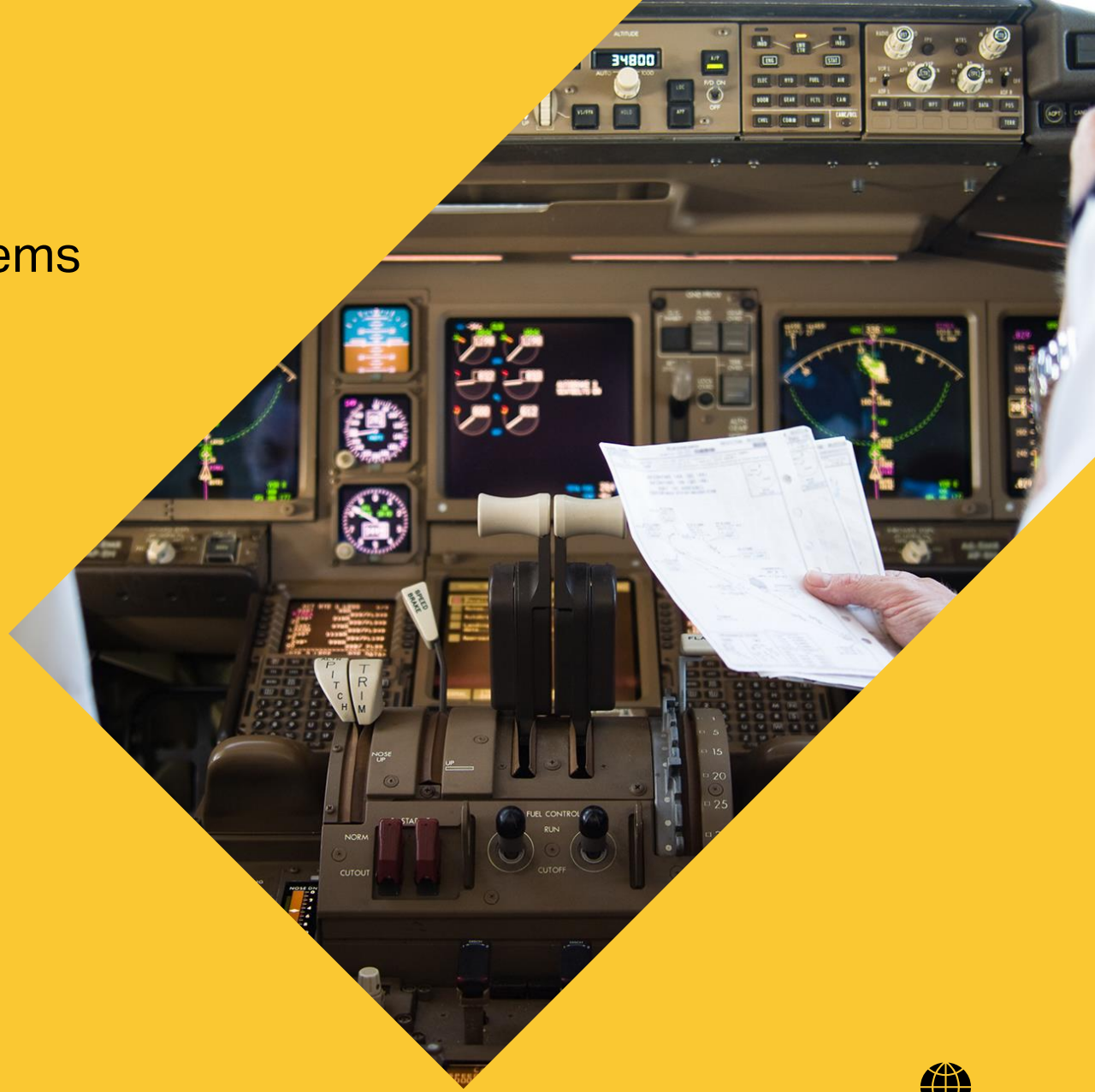
ICAO Asia & Pacific Regional
Cybersecurity webinar

Management Framework for CNS/ATM Systems

Protecting All Systems



John Moore

Assistant Director,
Safety & Flight Operations
Asia-Pacific

14 June 2021

IATA

The Challenge

- Airlines have many business, financial and administrative systems
- Also, many Communications, Navigation, Surveillance, and Air Traffic Management (CNS/ATM) systems
- Solutions must protect all systems from cyber-attacks

Background

- Increasing threat of cyber attacks in aviation
- New generation aircraft are connecting to the ground in real-time
- More networks, more digitization
- Not just business systems – CNS/ATM as well
- New entrants – UAS?
- What needs to be done to ensure critical information & systems remain protected?

Today's protection?

Aviation security historically strong
Mature Governance
Critical systems and safety-critical information 'isolated'
Firewalls protect against penetration
Data and information via secure pathways, eg: CRV
Encryption

Current environment

- Many connections now and more foreseen
- Datalinks between aircraft and ATM systems
- Point-to-point sharing and tight coupling through defined interfaces
- Defined procedures and governance
- High physical security
- Already connected in several ways in the cabin

Emerging Environment

Airlines seek continual safety and efficiency benefits

Increased connectivity for entertainment and communication – passenger experience

System Wide Information Management (SWIM) is becoming a game-changer

Cockpit connected via IP?

Electronic Flight Bags (EFBs)

Greater sharing of information between ground stations

Potential for less ‘isolation’, increased scope for attacks

What sort of attacks?

1. Denial of Service – prevents access to a service or system

- Cockpit systems
- Airline flight planning systems
- Airline ticketing systems
- Satellite interruption
- ATM systems (surveillance and FDP)
- Ground station or pathway interruptions

What sort of attacks?

2. Compromising or corrupting the integrity of data and / or information

- Value of information?
- Partial – deleting or blocking delivery of required data
- Delayed – data or information is delayed causing systems to miss critical decision-points
- Inaccurate – information is intentionally incorrect creating false analyses outcomes

What are potential consequences?

- Avionics fail or become inaccurate and unreliable
- Aircraft operation compromised
- Airline systems corrupted (Flight Planning / Ticketing)
- ATM systems – safety compromised
- One incident can escalate

Electronic Flight Bags (EFBs)

- EFBs now widely used
- Connectivity creating significant efficiencies
- No incidents in 170 million flights using EFBs
- Various levels of current protection:
  - Vendor included strategies
  - OEM & airline cooperation
  - Company policies for connecting

Unmanned Aerial Systems (UAS)

- Growing number of UAS
- New capabilities more system interconnections
- Protecting against intentional damage
- New risks and vulnerabilities
- Perpetrators difficult to identify
- Mitigating cyber risks is key to enabling UAS

Prevention:

- Safety by design – firewalls, encryption, standards
- Layered resilience – in SMS planning
- AI detection systems in CNS/ATM, aircraft, airline and airport systems
- Rapid response and recovery capabilities
- Strong Governance
- Training and education
- Physical security
- ICAO Global Resilient Aviation Network ConOps

Summary

- Operational systems as well as business systems
- Current protection is strong
- Growing reliance on connectivity and system-of-systems integration
- More data sharing (SWIM, EFBs)
- New entrants (UAS)
- Must continue to evolve to ensure all systems will be protects

QUESTIONS?

John Moore

Assistant Director,

Safety & Flight Operations

Asia-Pacific

moorej@iata.org