Nick Lawrence-Taylor
Qatar’s Aviation Cyber Security Guidelines
Overview

• Background
• National Policy and Task Force
• Aviation Cyber Security (ACS) Guidelines Initiative
• Penetration Testing
• Main Challenges
• Future Development
• Summary
Background

- 2015: QCAA introduced aviation cyber threats to NCASP as a possible method of attack

- ICAO Ann 17 – Amendments 13 and 14 incorporated new SARPs related to cyber threats:
  - 4.9 Measures Relating to Cyber Threats
    - 4.9.1 (Standard)
    - 4.9.2 (Recommendation)

- 4.9.1 (formerly a recommendation) became a standard in the latest amendment to Ann 17

- Gradual addition of more SARPs related to cyber threats are likely in the future
The transportation sector is critical for Qatar’s security and prosperity.

Recognition that every aspect of today’s aviation sector is affected by ICT.

Acknowledgment of the distinction between AVSEC expertise and technical cyber security expertise.

Qatar needed to develop an aviation cyber security policy and associated strategy:

- to satisfy the new Annex 17 SARP
- improve aviation cyber security resilience and awareness
- develop and implement suitable protective measures to mitigate against potential cyber vulnerabilities.
National Policy and Task Force

- In 2016, the QCAA in partnership with the Ministry of Transport and Communications (MoTC) established an aviation cyber security task-force.
- Task Force purpose:
  - gather strategic information regarding aviation cyber security
  - develop a best practice approach
  - conduct a comprehensive assessment of interconnected critical areas within Qatar’s aviation ecosystem
ACS Guidelines

• Approach
  – Joint consultations between MoTC and QCAA
  – Industry consultations to understand the business
  – Reference to published international standards and guidelines (Aviation Sector)
  – Closed review of the draft guidelines with stakeholders
  – Review of the draft guidelines by an international consulting organization
ACS Guidelines cont’d

- Encompasses the general CIA Approach
  - Confidentiality, Integrity, Availability
- Proposes the 360 Degree approach
  - Predict, Prevent, Detect, Respond
- Assists the aviation sector to identify and adopt secure best practice and effective cyber hygiene
- Integrates with MOTC’s National Information Assurance Policy (NIAP)
  - The NIAP is based on the principles of Information Classification and Baseline controls
- Aligns with International standards and best practices.
- Developed with direct support from:
  - Qatar Ministry of Transport and Communications (MOTC)
    - Cyber Security Sector (Q-CERT)
  - Qatar Aviation Stakeholders:
    - Qatar Airways
    - Hamad International Airport (HIA)
    - QCAA Air Navigation Department (ATC)
ACS Guidelines cont’d

• Some of the main areas which were assessed:
  • QCAA Air Navigation Department
    – Air Traffic Control (ATC)
    – Communication and Navigation Surveillance (CNS) & Air Traffic Management (ATM) systems
  • Airport Systems
    – Flight Information Display Systems (FIDS)
    – Baggage Handling Systems
  • Airline/Aircraft/Airport Systems
    – In-Flight Entertainment systems (IFE)
    – Reservation System
ACS Guidelines Cont’d

• Specific to Aviation Security
• Now an appendix to the Qatar NCASP
• Publicly available via the QCAA website
• Dynamic “live” document
Penetration Testing

- Penetration Testing forms an essential element of Qatar’s aviation cyber security strategy
- To help identify potential vulnerabilities and progress development of the ACS guidelines, Q-CERT performed Pen Tests on the QCAA’s secure and public websites
- Pen Tests are very effective – but have some limitations
  - Expensive for industry
  - Scope of Pen Tests (on aviation systems) not fully defined
  - Lack of resources and expertise (pertaining to aviation)
  - Complex in nature – requires high level coordination and approvals
- QCAA plan to expand Pen Testing across various aviation specific systems
Main Challenges

• Dynamic, fast moving, evolving nature of cyber security makes effective mitigation challenging
• Scope definition – difference between broad ICT (which is generally well protected) and critical aviation systems
• Stakeholder acceptance
• Some industry resistance
• Raising awareness
Future Development

• Extending stakeholder support and capacity building
• Technical assistance with the support of existing MoU/MoC
  – Currently UK, US, Australian Governments
• Develop internal QCAA cyber security capacity
  – Training, participation in global events, recruitment, stakeholder engagement
• Introduction of general regulations related to ACS
  – Expansion of the ACS Guidelines, NCASP and national policy
• Expand Penetration Testing
  – Aviation systems, software, websites and potentially aircraft systems
• Regulatory oversight functions
  – Audits, tests, inspections, exercises, desktop activities
Summary

• Qatar needed to develop an aviation cyber security capability
• ACS guidelines were developed, disseminated to industry and are now publicly available
• Qatar’s cyber security strategy is dynamic and subject to continuous review
• Qatar will continue to seek industry, intergovernmental and international input and assistance
Availability

• ACS Guidelines are available on the QCAA public website:

www.caa.gov.qa
Located at: Media Center → All Publications → Guidelines

Nick Lawrence-Taylor
nick.lawrence@caa.gov.qa
+974 3339 3061
Thank You