Department for Transport

Cyber Security in Aviation

NOT PROTECTIVELY MARKED

Introduction

- This presentation provides an overview of the UK's approach to cyber security in the aviation sector. It will cover:

  - the cyber threat
  - the relevant regulatory requirements
  - which aviation entities are affected
  - how the CAA oversees the industry's compliance.

The Cyber Threat

- The aviation industry is an attractive target for malicious cyber actors. The amount of data the industry holds and processes, including passenger data and intellectual property is highly desirable to attackers. The economic importance of the sector also makes it appealing. The threat comes from different sources, including hostile states and serious and organised crime groups.

- Ransomware almost certainly remains the largest and most persistent threat to the aviation sector. Denial of Service (DDoS) attacks against aviation-linked websites are also likely. Supply chain attacks are increasing.

- It is almost certain that the aviation industry, especially airlines, will continue to be a target for malicious cyber actors. Their methods are likely to evolve as innovation and new technologies are deployed. Attackers may also look to exploit a world-wide shift to remote working.

Background

States have responsibilities under **ICAO** in this area:

***Annex 17* - 4.9 Measures relating to cyber threats**

4.9.1 Each Contracting State shall ensure that operators or entities as defined in the national civil aviation security programme or other relevant national documentation identify their critical information and communications technology systems and data used for civil aviation purposes and, in accordance with a risk assessment, develop and implement, as appropriate, measures to protect them from unlawful interference.

UK Approach

- To meet our international obligations, we brought new cybersecurity provisions for aviation into UK law by amending aviation security (Avsec) regulation.
- These cyber security provisions apply to UK airports and air carriers registered in the UK. They came into force on 1 January 2022.
- The provisions are similar to those set out in EU regulation.
- We will consider the case for extending to other sectors of the aviation industry (e.g. regulated cargo agents) in slower time.

As well Avsec regulations, some entities have to comply with cyber provisions in other regulations, air traffic management regulations and the Network and Information Systems Regulation 2018 (for operators of essential air services).

Avsec Regulation

The UK cyber security provisions in Avsec regulation require the relevant aviation entities to:

- identify their critical information systems and data
- identify and implement appropriate security controls to protect systems and data from unauthorised interference through a risk assessment process
- reference these security controls within their aviation security programmes
- ensure that staff having access to critical systems and data, and those responsible for implementing security controls, receive the right level of vetting and training
- comply with the UK's CAA cyber security oversight procedures (CAP1753).

Cyber Security Oversight in Aviation

- In the UK, oversight of the aviation industry's compliance with regulations is the responsibility of the CAA (acting on DfT's behalf).
- Over 90 aviation entities come into scope of the regulations.
- The CAA's approach to cyber security oversight, the Cyber Security Oversight Process for Aviation, is laid out in CAP 1753 and it consists of six key steps.
- Aviation entities must nominate a Cyber Security Responsible Manager to monitor and oversee the organisation's compliance.
- The CAA issue a 'Certificate of Compliance' once satisfactory progress has been made to meet the requirements of CAP1753.
- The CAA used a 'stepped approach' to enforcement.

Cyber Security Oversight in Aviation

CAP1753 – 6 Stage Process

1. Engagement
2. Critical Systems Scoping
3. Cyber Self Assessment
4. ASSURE cyber audit
5. Provisional Statement of Assurance
6. Final Statement of Assurance and Certificate of Compliance

- The applicability of each step is discussed and agreed with an aviation organisation during the initial engagement step and determined based on several factors including; the assessment of cyber security risk, aviation organisation complexity, and regulatory requirements.

Critical Systems Scoping

- It is important that systems (including networks, information technology - IT and operational technology - OT) which are critical to an aviation organisation are within scope of cyber security oversight. Guidance on identifying critical systems has been produced and is available in CAP 1849.
- The guidance given in CAP 1849 provides a recommended method to identify critical systems through performing a functional decomposition from the aviation organisations' key aviation functions. CAA also publish a scoping template to help aviation organisations to document their identified critical systems and critical suppliers.

Cyber assessment framework (CAF) for aviation

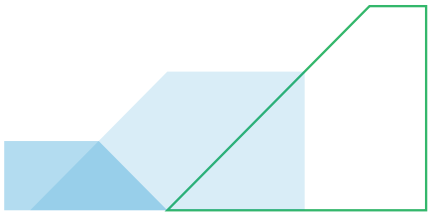
- Once an aviation organisation has identified it's critical systems it can assess them against the Cyber Assessment Framework (CAF) for Aviation.
- The Cyber Assessment Framework (CAF) is an outcome-focused assessment against fourteen principles and four objectives, it was developed by the UK's national technical authority National Cyber Security Centre (NCSC).
- The self-assessment helps the organisation to produce a corrective action plan to mitigate risk.
- The CAA use the information obtained from this self-assessment to gain an understanding of the cyber security posture of the organisation.

ASSURE

- On completing the Cyber Assessment Framework (CAF) for Aviation, an organisation is required to procure an ASSURE Cyber Audit from an accredited ASSURE Cyber Professional.
- An ASSURE audit report is issued after the audit and may require amendments to be made to the organisation's corrective action plan.
- Following this, an organisation can submit to the CAA a provisional Statement of Assurance to confirm it has complied with the CAP1753 process.

CERTIFICATE OF COMPLIANCE

- The CAA's Cyber Security Oversight Team conducts an analysis of the information provided by an organisation. This includes reviewing the provisional Statement of Assurance and any amendments to corrective action plans arising from the ASSURE audit.
- A Certificate of Compliance is issued by the CAA as confirmation that an aviation organisation has met the agreed requirements of the Cyber Security Oversight Process for Aviation.



Department for Transport

Questions?