Foundations of Aviation Cybersecurity Leadership and Technical Management

Schedule (5 full days)

Day 1 Part 1— Introduction to Cybersecurity

Module 1

- Welcome and Introductions
- Course objectives and week at a glance (overview)
- The history of cybersecurity, fundamental concepts, and terminology

Module 2

- How technology underpins all aviation systems and how they are connected
  - Safety, Security
  - Airports, Air Traffic Management, Aircraft, the Enterprise
- Understand the interdependencies between aviation safety / security / cybersecurity

Module 3

- **Why** adversaries attack such systems (using examples and working through attack phases*)
  - Examples
    - Financial (Extortion, ransomware, etc.)
    - Disruption (nation-state, terrorist, activist)
    - Geopolitics
- Discussion: Adversary motivations

Module 4

- **How** adversaries attack such systems (using examples and working through attack phases*)
  - Examples
    - Vulnerabilities, Including the concept of known and unknown (Zero-day vulnerabilities)
    - Email phishing
    - Insider threat
    - Wireless (Wi-Fi, Bluetooth, RF)
    - Capability – 'Living off the land' to zero-day capability
- Pulling it all together - Technology as an attack surface
- Discussion: Cybersecurity as an evolving challenge, how adversaries evolve their tactics, techniques, and procedures
- Recap, Q&A

Day 1 Part 2 — Critical Systems, Regulations and Risk Management

Module 5

- Review Day's Outcomes
- Defining cybersecurity objectives in aviation; security / safety / privacy / trust / financial / operational continuity
- Critical aviation elements
    - Airport
    - Air Traffic Management
    - Aircraft
    - Services / Suppliers

Module 6

- How to identify and scope cybersecurity critical systems within aviation
- Critical thinking exercise: Identifying assets in your organization/domain that could be defined as a critical system and why
- Discussion: The interdependent nature of aviation systems, being critically dependent on each other

Day 2 Part 1 — Critical Systems, Regulations and Risk Management (continued)

Module 7

- The concept of cybersecurity risk
- Introduction to cybersecurity risk management and assessment
  - Threat
  - Vulnerability
  - Risk
  - Metrics
- The importance of a single perspective of risk across the leadership and into the technical team

Module 8

- Understand the regulatory and legal considerations of aviation cybersecurity
  - ICAO documentation, regional, national
- Recap, Q&A

Leadership Track

Day 2 Part 2 — Cybersecurity Leadership and Management

Module 9

- Review Day's Outcomes
- Cybersecurity Governance and oversight
  - The role of leadership
  - The role of the board
- Developing a cybersecurity program
- Discussion: Challenges of developing and deploying a cybersecurity program

Module 10

- Developing a cybersecurity budget
  - Objectives, challenges, and best practices
- Cybersecurity culture; importance and value
- Learning Activity: Establishing a cybersecurity culture within your organization

Modules 11 & 12

- Workshop: Developing an aviation cybersecurity program
- Recap, Q&A

Leadership Track

Day 3 — Key Cybersecurity Elements

Module 13

- Review Day's Outcomes
- Managing supply chain risk
  - Hardware
  - Software
  - Services
- The role of contracts
- The increasing role of third-party audit

Module 14

- Information sharing
  - The need for information to get ahead of risks and threats
  - What information?
  - Potential blockers to sharing
  - Sources of information
    - Own Systems
    - Third parties (Vendors, industry bodies, Govts, researchers)
  - Discussion: Comparing approaches to information sharing; safety, security cybersecurity

Module 15

- Personnel
  - Cybersecurity roles across aviation organizations
    - The need for skills diversity
    - Promoting collaboration
  - Staff training
    - Dedicated cybersecurity personnel
    - Wider staff training and awareness
  - Recruiting and retaining cybersecurity workforce

Module 16

- Organizational resilience and incident response
  - Roles in cybersecurity incidents
  - Lifecycle of a cybersecurity incident
  - Preparing for cybersecurity incidents
- Recap, Q&A

Technical Management Track

Day 4 Part 1 — Securing assets and systems

Module 17

- Review Day's Outcomes
- Aviation perspectives to be included throughout the day
  - Airport / Air Traffic Management / Aircraft Operators
- Operating Systems / communications protocols that may be found in aviation
- Digitized, connected hardware that may be found in aviation
- High level architecture and connectivity

Module 18

- Identity and Access Management
  - Verification, authentication, authorization
  - Device management
  - Privileged User Management

Module 19

- Data Security
  - Encryption
  - Key management within aviation systems
  - Stored Data
  - Data in transit

Module 20

- System Security
  - Secure by Design
  - Secure Configuration
  - Secure management
- Recap, Q&A

Day 4 Part 2 — Resilient Systems

Module 21

- Review Day's Outcomes
- Resilient Networks and Systems
  - Finding and understanding the attack surface
  - Resilience Preparation
  - Design for Resilience
  - Secure Configuration management and monitoring

Module 22

- Resilient Networks and Systems continued
  - Storage and backups
  - Dealing with Operational Technology / IoT
- Mitigating and managing ransomware attacks
  - Before / During / After
- Discussion: On Premises vs Cloud Storage – advantages, disadvantages, and challenges

Day 5 Part 1 — Resilient Systems (continued)

Module 23

- Vulnerability Management Programmes
  - The benefit
  - The approach
  - Vulnerability notification
    - Internal team
    - External contractors
    - External researchers
- Testing / auditing
  - Regulators
  - Questionnaires – best practice to respond and use
  - Red Teaming / Purple Teaming / Blue Teaming

Module 24

- Incident Management
  - Developing a response plan and team
  - Testing and exercising the team
  - Collaborating with third parties
    - Airport / Other operators / Govt
  - Communications and media
- Recap, Q&A

Day 5 Part 2 — Cyber Risk Management and Incident Response

Module 25

- Review Day's Outcomes
- Building an Aviation cybersecurity strategy
  - Connect major topics from both tracks
  - Discuss: policy, governance, best practices, etc
  - Exercise

Module 26

- Table-top exercise introduction
  - Roles
  - Scenario Brief. Must include both leadership and technical aspects that draw together all the elements of the course, put into practice all learning objectives and serve as an exemplar of how such exercises can be held
- Tabletop exercise execution

Module 27

- Tabletop exercise debrief
  - The setting and objectives
  - Teaching staff perspectives
  - Participant perspectives
- Discussion: Setting up and running a tabletop exercise

Module 28

- Where to find more assistance and support (other than the cybersecurity industry)
  - ICAO
  - National Bodies
  - Industry Bodies (ACI, IATA, etc.)
  - Other international cybersecurity bodies (examples)
    - Global Cyber Alliance
    - Centre for Internet Security
    - Cloud Security Alliance
    - European Centre for Cybersecurity in Aviation
- Looking to the Future
  - IoT, 5G, Machine Learning and Artificial Intelligence
- Recap, Q&A
- Course evaluations, Wrap