Graduate Certificate in Aviation Cybersecurity

(Asia-focus)

The Graduate Certificate in Aviation Cybersecurity is specifically created to focus on the aviation cybersecurity landscape in the Asia-Pacific region. It consists of 4 courses offered in a face-to-face classroom in Asian countries, or in an online synchronous environment.

The certificate will provide airport and airline management and staff, air navigation service providers, industry planners, manufacturers, policy and law advisors, third party vendors and other aerospace professionals the knowledge and tools necessary to develop and implement sound policies and procedures to address the aviation cybersecurity challenges facing the Asia-Pacific Region – today and in the future.

Core Courses Learning Objectives

All Core courses are required for the Graduate Certificate

- **The Practice of Cybersecurity** - students will be able to:
  - describe access control mechanisms that work together to protect information and computing assets;
  - define network structures, transmission methods, and security measures used to provide confidentiality, integrity, and availability of information;
  - propose governance and risk management policies, standards, procedures, and guidelines;
  - discuss the integration of information security methods and policies to organizational and legal structures;
  - apply controls to include security within systems and software applications development;
  - describe different cryptographic methods for the protection of information and communications;
  - articulate the concepts, principles, structures, and standards used to design, implement, monitor, and secure operating systems, equipment, networks, and applications;
  - explain the various controls that can be employed to protect hardware and media;
  - devise incident response, disaster recovery, and business continuity plans;
  - and identify relevant laws and regulations that impact the use of information, as well as investigative and evidence gathering methods that can be used to determine if a crime has been committed.

- **Security Engineering and Management** - Students will be able to:
  - describe the roles and responsibilities of cybersecurity technologies and processes;
  - apply the basic tools and principles of security (e.g., protocols, passwords, access controls, and cryptography) to build dependable, distributed information systems. Differentiate between different information security technologies and their relevance in information systems (e.g., applications, market segments, etc.);

  - evaluate and analyze how information security methods and policies impact organizational and legal structures; create information security policies and procedures that meet organizational requirements;
  - apply industry best information security practices to real-life environments;
  - and apply the precepts of Integrated Reflective Practice to the management of information security practices.

- **Aviation Cyber Policy and Law** – students will be able to:
  - compare and contrast physical space and cyberspace in terms of policy, law, society, rights, and security, with particular emphasis on the aviation industry;
  - articulate the role of national and international laws in cyberspace, as well as cyber laws affecting aviation;
  - examine the rights of users in cyberspace, including freedom of expression, privacy, and anonymity;
  - analyze the cybersecurity policies of the Asia-Pacific region and international bodies, the protection of critical infrastructures, and the cyber safety of aviation;
  - and produce a set of recommendations to better secure aviation industrial sector from threats -- and opportunities -- in cyberspace.

- **Topics in Aviation Cybersecurity** – students will be able to:
  - characterize the latest issues and trends in the field of cybersecurity, particularly as they impact aviation;
  - compare and contrast the evolving aviation cybersecurity threat landscape that will dominate the field in the next three to five years;
  - identify the system of systems that comprise the aviation and aeronautics sector and cyber-attack vectors unique to the aviation industry;
  - communicate to colleagues and superiors about the current state of research in a particular aviation cybersecurity subject area;
  - evaluate the legal, policy, and societal implications of emerging cybersecurity technologies and research, and the potential impact on the future of the aviation industry;
  - and describe the methods by which an attacker would plan an attack on a system, and find and exploit vulnerabilities, and the methods by which a defender would build a proper cyber defense.

Who Should Attend

- Students about to enter, or recently entered the aerospace workforce
- Aerospace professionals in an operations or management role (airport, airline, air navigation, MRO, legal, etc.)
- Government officials in the aerospace industry
- Other professionals interested in the Aviation Cybersecurity landscape in Asia-Pacific

EMBRY-RIDDLE Aeronautical University ASIA

Training Method

- Face-to-Face instructions in classroom or using Virtual Reality, or online synchronous
- Supported by practical case studies

General Information

Duration: Each course is 3 days or 24 hours, the entire program can be completed in 2-4 months

Venue: Local or Virtual Classroom

Prerequisites:

- Familiarity with IT word-processing and presentation software
- Basic knowledge of aviation industry