Aviation Cybersecurity – Online Short Course

- ✓ **From October 18 – November 10, 2022 (4 Weeks, 8 Classes, 16 Total Hours)**
- ✓ **Every Tuesday and Thursday at 1900-2100 Eastern Time *(all sessions will be recorded and available for replay; course materials will be available for download)***
- ✓ **All students will receive an AIAA Certificate of Completion at the end of the course**

Overview

This course covers Aviation Cybersecurity Management, a discipline that is fast becoming one of the most important aspects of the aviation industry. Aircraft systems integrity, airport security, security of the passengers, cargo and the myriad systems that support aviation are a few areas where the reliance on computer networks is significant and the consequences of cyber breaches are great. Students will learn the needs and developments of cybersecurity, and techniques to minimize or eliminate threats. The course treats aviation cybersecurity management within the context of rapid technological changes.

Learning Objectives

- Recall the history, scope, gaps and vulnerabilities of cybersecurity in the aviation industry and in the National Airspace System
- Understand and explain cybersecurity applicability and problems within the aviation industry
- Synthesize the relevant cybersecurity information pertaining to aviation and propose solutions for desired outcomes
- Demonstrate an understanding of the legal, social, economic, environmental, and global ramifications of cybersecurity actions in the aviation industry
- Identify, formulate, and solve cybersecurity problems in the aviation industry by selecting and applying appropriate tools and techniques
- Demonstrate advanced knowledge of cybersecurity and the impact of technology within the aviation industry
- Understand common cybersecurity vulnerabilities and modern threat actors and evaluate their relevance to the aviation industry
- Understand trends in cyber breaches and threats and analyze their importance to aviation management

- Apply principles and best practices of information security, intelligence and risk assessment to mitigate gaps and vulnerabilities in aviation cybersecurity
- Create a cybersecurity strategy for an aviation management company

Who Should Attend: Any and all aviation professionals and students, as cybersecurity is fast becoming an essential skill that all engineers, researchers, and managers will need in their jobs and for their careers.

Course Fees (*Sign-In to Register*)

- AIAA Member Price: $995 USD

- Non-Member Price: $1195 USD

- AIAA Student Member Price: $495 USD

Course Outline

WEEK 1

Learning Objectives

- Understand the need for an aviation industry-wide strategy for cybersecurity (PWC report)
- Evaluate the 2021, and 2022 Verizon Data Breach Incident Reports' conclusions and relevance to aviation cybersecurity
- Recall and explain marketplace drivers for the U.S. UAS marketplace
- Analyze concerns for cybersecurity in the UAS marketplace
- Recall the history of regulation of various modes of travel for the last 150 years
- Explain the roles of legislation, regulations, judicial processes and their impacts on the aviation industry
- Explain the roles of federal, state, and local governments in regulating air traffic
- Discuss efforts by the FAA to improve aviation cybersecurity

Recommended Reading

- *Aviation Perspectives - Introduction, Part 1 of 4*, PricewaterhouseCoopers (2016)
- *Unmanned Aircraft Systems in the Cyber Domain*, chapters 1 & 2 -- Textbook by Nichols, R., Mumm, H., Lonstein, W., Ryan, J., Carter, C., and Hood, J. (2019). Manhattan, KS: New Prairie Press.
- 2021, and 2022 Verizon Data Breach Incident Reports
- *Aviation Cybersecurity Initiative* (2021), US Federal Aviation Administration (FAA)
- *Aviation Cybersecurity, Scoping the Challenge,* Pete Cooper (et al.), Atlantic Council

WEEK 2

Learning Objectives

- Discuss the role of prevention in aviation cybersecurity (PwC report)
- Discuss the basics of risk management theory and how it applies to aviation cybersecurity
- Describe the unique challenges that UAS present to cybersecurity
- Explain why public trust in the aviation system is the most valuable asset we must protect as aviation cybersecurity experts
- Describe the problem of countering hostile use of UAS against us national interests.
- Identify critical components of an Unmanned Aircraft System (UAS), identify potential cyber vulnerabilities and understand the taxonomy of UAS operations that may be compromised.

- Propose ways the FAA can help move UAS technology forward in keeping with its mission to ensure a safe and efficient transportation system that meets national interests.
- Discuss efforts by the ICAO to improve aviation cybersecurity

Recommended Reading

- *Aviation Perspectives – Prevention, Part 2 of 4*, PricewaterhouseCoopers (2016)
- Chapters 3 & 4 of textbook (Nichols, et al.)
- Wurzler (2013). *Information Risks and Risk Management*.
- *Cybersecurity Strategy* (2019), International Civil Aviation Organization (ICAO)
- *Annual Report* (2020) pp.71-83, Lufthansa Group

WEEK 3

Learning Objectives

- Discuss the challenges of detecting cyber incidents in the aviation environment (PwC report)
- Explain the Intelligence Cycle and its relevance to this industry
- Articulate the role of intelligence in aviation cybersecurity
- Articulate a strategy to obtain the intelligence needed for an aviation company
- Explain red teams and blue teams and how they can be used to enhance cybersecurity of aviation companies or aircraft
- Describe how attack/defend scenarios can take cyber defense strategies to the next level
- Explain the communications vulnerabilities of aircraft for cyber attack
- Explain how you can prevent the data being collected by UAS from being intercepted
- Discuss security controls that should be considered for the case where your aviation UAS asset goes missing
- Design a security policy to protect against equipment probing
- Propose a method for knowing when unauthorized UAS are operating near your aviation company or operations
- Explain the potential dangers of unauthorized UAS operating near sensitive areas

Recommended Reading

- *Aviation Perspectives – Detection, Part 3 of 4*, PricewaterhouseCoopers (2016)
- Chapters 5, 6 & 14 of textbook (Nichols, et al.)
- *National Strategy for Aviation Security* (2018). White House.
- *How a Fish Tank Helped Hack a Casino,* Alex Schiffer for the Washington Post
- *Global Threat Report (2017),* Darktrace

WEEK 4

Learning Objectives

- Discuss some ways aviation enterprises can react more effectively to cyber incidents (PwC report)
- Explain how the IoT is increasing risks to aviation safety
- Explain how data integrity can be attacked and cause hazards to flight
- Propose strategies for driving down the risks to infrastructure, networks, and vehicles in the aviation industry
- Propose a strategy for enhancing the cybersecurity of avionics systems on modern transportation aircraft.
- Describe the weaknesses of the current FAA cybersecurity oversight program

- Explain how you, as a flying company manager, could help your company reduce the risks that the FAA is leaving un-addressed in avionics cybersecurity
- Propose ways to make progress on an industry-wide framework for cybersecurity (AIAA paper)

Recommended Reading:

- *The Connectivity Challenge*, AIAA Decision Paper (2013)
- *Aviation Perspectives – Reaction, Part 4 of 4*, PricewaterhouseCoopers (2016)
- *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (2017). White House.
- *FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks*. Government Accountability Office.
- *Connected Aircraft: Cyber-Safety Risks, Insider Threat, and Management Approaches* (2019). Proceedings of the 52nd Hawaii International Conference on System Sciences.
- *Global Threat Report (2022),* Darktrace

Instructor

CAPITOL
Technology University

Todd Raines is a senior Air Force civilian at US Space Force, Pentagon. He recently completed over 12 years at US Cyber Command, planning and executing cyber operations. His first career was in conventional air warfare; he retired after 21 years of flying F-4, F-15, and F-16 fighter aircraft for the Air Force. He was also a Flight Officer for United Airlines for seven years.

“Rhino” has a Bachelor of Science in Astronautical Engineering from the US Air Force Academy, and a Master of Science in Cyber Security from National University. In addition to multiple overseas deployments as an Air Force fighter pilot, he has twice deployed to Afghanistan civilian in cyber warfare and leadership roles. He served an Adjunct Professor at the National Cryptologic School at Fort Meade, where he taught Adversary Cyber Methodologies. He also teaches Aviation Cyber Security as an Adjunct in the Masters program at Capitol Technology University, near Fort Meade. He enjoys teaching cyber security because adult learners are fun to teach.

Classroom hours / CEUs: 16 classroom hours / 1.6 CEU/PDH

Course Delivery and Materials
The course lectures will be delivered via Zoom. You can test your connection here: https://zoom.us/test

Access to the classroom will be provided to registrants near to the course start date.

All sessions will be available on-demand within 2 days of the lecture. Once available, you can stream the replay video anytime, 24/7.

All slides will be available for download after each lecture. No part of these materials may be reproduced, distributed, or transmitted, unless for course participants. All rights reserved.

Between lectures during the course, the instructor(s) will be available via email for technical questions and comments.

Cancellation Policy: A refund less a $50.00 cancellation fee will be assessed for all cancellations made in writing prior to 5 days before the start of the event. After that time, no refunds will be provided.

Contact: Please contact Lisa Le or Customer Service if you have questions about the course or group discounts (for 5+ participants).