AVIATION CYBERSECURITY

Finding Lift, Minimizing Drag

EXECUTIVE SUMMARY

AVIATION IN THE DIGITAL AGE: Increasing complexity, multiple stakeholders and the new nature of risk

As an "always on" generation of travelers demand to be "always connected," an increasingly interconnected aviation industry is employing evermore digital technologies to deliver efficiencies: across aircraft (including Unmanned Aircraft Systems [UAS]), Air Traffic Management (ATM), airports, and their supply chains.

This study indicates that the aviation industry will likely experience cybersecurity challenges similar to other industries that have embraced the "digital revolution." As the industry moves forward, will it be able to maintain stakeholder trust by accurately perceiving the risks and opportunities as well as understanding adversary threats?

Connectivity of aircraft systems, through traditional information technologies and aviation-specific protocols, has now extended the attack surface to the aircraft itself. Aircraft are now complex data networks, yet the ability to monitor them arguably lags comparable ground-based networks—as does the ability to avoid and respond to potential cybersecurity incidents.

As the domains of aviation and cybersecurity increasingly overlap, the common goals of safety, resilience, and trust can be achieved sooner by working together. Preserving aviation's strengths relies on clear definition of governance and accountability and recognition of shared responsibility across the supply chain.

The challenges of cybersecurity are testing these existing industry policies and frameworks as nations, organizations, and businesses attempt to develop best practices. There will be a key role for the International Civil Aviation Organization (ICAO) in bringing both leadership and vision to the challenge. With multiple perspectives and stakeholders, it is essential for the increasingly interconnected aviation industry to have a clear, coherent vision.

A CYBERSECURITY VISION FOR A CONNECTED AVIATION INDUSTRY AND ITS FOUNDATION

A vision or aspirational state for the aviation industry as it faces cybersecurity challenges may be characterized as: A safe and prosperous aviation industry with resilient trust and systems. To achieve this vision, the industry must focus on strengthening the foundations of aviation cybersecurity:

1. SYSTEMS THINKING, GOVERNANCE, AND ACCOUNTABILITY

In a complex, interdependent, system of systems, finding and securing the weak links is not only an essential requirement but also a critical test of governance and accountability. The ICAO plays an important role in working with national regulators to decide how the aviation industry should manage cyber risks and to clarify and simplify the legislative burden for stakeholders.

2. RESILIENT SYSTEMS

Advanced adversaries will still breach the IT infrastructure. This assumption of future breach, failure, or attacks on data integrity has resulted in a greater focus to deliver resiliency as well as security. It will require both resilient systems engineering practices and a resilient personnel culture to safely work through such adversary activity.

3. RESILIENT TRUST

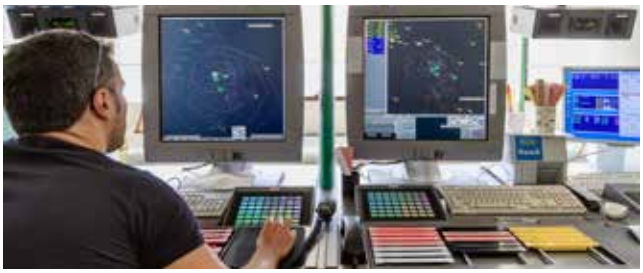
The importance of stakeholder trust is at the forefront of the aviation cybersecurity challenge. If adversaries can erode trust, they are able to control passenger and stakeholder experience, perspective, and confidence. The longer it takes for an operator to counter perceptions and regain trust, the less credibility the operator will have in the eyes of the stakeholder.

4. SECURED HUMAN DECISION-MAKING

Human error or technical failure is inevitable, but all aviation systems are designed to help a human operator recognize and deal with an accident or incident before it impacts safety. Therefore, there must be a focus on protecting the integrity of the data that operators are presented with so they are able to make safe and timely decisions.

5. SHARED PERSPECTIVE AND CULTURE

The importance of collaboration cannot be underestimated. Even beyond sharing knowledge and different perspectives, there is great potential for cultural exchange between the aviation and cybersecurity industries. Developing a shared culture in which both groups synergize and view the challenges and potential solutions will increase awareness of risk and robust resilience.



SUGGESTED NEXT ACTIONS

To build and fortify the foundations of aviation cybersecurity, it is recommended that all stakeholders take the following actions:

- Reinforce Leadership and Standardization (Globally, Nationally, Regionally, etc.)
- Reevaluate, Develop, and Use Robust Threat Models
- Find Ways to Develop Trust with Non-Technical Audiences
- Train for Safety Across Multiple Disciplines
- Develop a Common Understanding of Aviation Cyber Safety and Security
- Develop and Communicate Coherent Messaging on Cybersecurity Risks
- Improve Agility in Security Updates › Design Systems and Processes to Capture Cybersecurity-Relevant Data
- Incorporate Cyber Perspectives into Accident and Incident Investigations

As organizations seek to exploit the opportunities of a connected aviation industry, they must retain the ability to be objective about both the benefits and risks. It will take consideration and incorporation of multiple stakeholder perceptions to reduce the risk posed by adversaries. In a rapidly evolving environment, the industry must exercise leadership and utilize teamwork to boldly look to the horizon with clear purpose and maintain stakeholder unity. The conditions are ripe to find alignment, direction, and progress under strong international leadership to ensure a safe and thriving aviation industry in the years to come.

To view and download the full report, visit:
http://aviationcyber.atlanticcouncil.org

Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

THALES