Cyber Security
Fact Sheet

Cyber security may be defined as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment as well as organizations’ and users’ assets. It encompasses the protection of electronic systems from malicious attacks and the means by which the consequences of such attacks should be handled.

The airline industry relies on computer systems extensively in their ground and flight operations. Some systems are directly relevant to the safety of aircraft in flight, others are operationally important, and many directly impact the service, reputation and financial health of the industry. There is no question that automation significantly enhances safety and aircraft capabilities while simplifying many routine tasks. However, as a result, the number of entry points into systems is increasing steadily.

Many airlines and airports have robust systems in place to address common hacking threats, but they haven’t always taken a holistic approach to the IT environment or considered the broader threat to the aviation system.

Three-Pillar Strategy
IATA has developed a three-pillar strategy to understand, define and assess the threats and risk of cyber-attacks. This represents the basis for appropriate regulation and the mechanisms for increased cooperation throughout the industry with the support of governments.

<table>
<thead>
<tr>
<th>Risk Management</th>
<th>Advocacy</th>
<th>Reporting and Communication</th>
</tr>
</thead>
</table>
| • Develop framework for and provide input to Threat Guide for cyber security in aviation  
• Develop Cyber Security Management System to assist airlines in performing risk assessment and implementing mitigation strategies  
• Advocate with key regulators for risk based regulation and coordinated requirements  
• Support airline leadership and technicians in advocating "security by design" measures with systems providers and manufacturers  
• Raise awareness of Cyber security issues through outreach and communication program  
• Identify reporting and intelligence sharing mechanisms |

Aviation Stakeholder Cooperation on Cyber Security
In December 2014, IATA, the International Civil Aviation Organization (ICAO), Airports Council International (ACI), the Civil Air Navigation Services Organisation (CANSO), and the International Coordinating Council of Aerospace Industry Associations (ICCAIA), agreed on a common roadmap to align their respective actions on cyber threats.

An appropriate high-level coordination mechanism has been established through the Industry High Level Working Group (IHLG) which meets on a regular basis. This group concentrates on the delivery and the promotion of the industry position on cyber security.
In cooperation with other IHLG participants, a proposed declaration on cyber security has been developed and adopted by the 39th ICAO Assembly\(^1\). The declaration calls upon States to define and align cyber security responsibilities within respective governments and adopt a flexible, outcome-focused approach.

**Aircraft Cyber Security Task Force (ACSTF)**

Safety and security are IATA's top priorities. Airlines and aircraft manufacturers demand the highest safety/security standards and precautions surrounding aircraft systems. IATA has established an aircraft cyber security task force to address industry concerns and priorities in this area.

Connectivity of aircraft systems—through traditional information technologies, aviation-specific protocols, and RF communications—has extended the attack surface to the aircraft itself, whether on ground or in flight.

In addition, the digital footprint of aircraft has increased and continues to do so; therefore, the question of digital communication between systems, data validity and information/data security (the protection against intentional interference) has become increasingly relevant.

---

\(^1\) [http://www.icao.int/Meetings/a39/Documents/WP/wp_017_en.pdf#search=Cybersecurity%20resolution](http://www.icao.int/Meetings/a39/Documents/WP/wp_017_en.pdf#search=Cybersecurity%20resolution)