ICAO EUROPE, MIDDLE EAST AND AFRICA (EMEA) CYBERSECURITY IN CIVIL AVIATION SUMMIT

BUCHAREST, ROMANIA

7 TO 9 MAY 2018

OUTCOMES AND CONCLUSION

Similar to other industries, aviation needs to maintain the trust of its stakeholders by accurately perceiving the opportunities of information technology as well as understanding vulnerabilities and threats. As technology radically transforms, cyber risk management should include: concept; design; development; delivery; operations; and maintenance, and existing models of safety and security must adapt.

Previously, cybersecurity received little attention as an international issue in the aviation industry and was addressed individually, in silos, by aircraft manufacturers, air navigation service providers and operators. More recently, aviation experts have warned that a malicious cyber attack on civil aviation operations would be disruptive, and could potentially be catastrophic.

The challenges facing a connected and digitalized civil aviation are the following:

1. As the aviation industry increasingly connects systems and services, the potential attack surface of systems is growing larger and more complex, resulting in a bigger target.
2. The aviation industry has extensive experience in addressing safety and security issues, but the cybersecurity challenge is comparatively new. It may take longer to develop and replace aviation systems than it does for perpetrators to develop capabilities, creating a challenge in accurate and up to date risk assessment.
3. Perception of the cyber threat is going to be critical in understanding and managing the risk. It is necessary that everyone in the industry attains the same level of awareness and understanding.
4. Because the aviation industry relies heavily on technology, understanding and overcoming the cultural differences with the cyber domain will require a paradigm shift. Developing a shared culture, and viewing the challenges and potential solutions together will require cross-disciplinary cooperation.
5. Appropriate protection of air traffic management (ATM) systems and physical security systems from cyber threats at airports is critical. The air transport system is a federation of several distinct organizations with potentially different approaches and the cyber vulnerability of one can affect all others.

6. National and international policies and regulations are agreed and understood for safety and physical security, but it is yet unclear how aviation cyber security can achieve the same maturity and clarity. That is why the International Civil Aviation Organization (ICAO), European Union (EU), European Aviation Safety Agency (EASA), European Organisation for the Safety of Air Navigation (EUROCONTROL), European Civil Aviation Conference (ECAC), as well as other multilateral entities, must work together to develop policy, regulation and standards.
7. ICAO is in a critical position to draw together the numerous global aviation cybersecurity initiatives and bring consistency, leadership, set appropriate standards, develop guidance and share best practices.
8. Developing cybersecurity capabilities – people, technology and processes – using an information network-based operation approach and being able to detect, protect, defend, analyse, decide and react, as well as restore, will ensure the resilience of civil aviation in the foreseeable future.
9. Comprehensive and timely information sharing will help mitigate risks, and the added value of such collaborative work is a better management of cybersecurity for stakeholders.
10. EASA produced the "Bucharest Declaration on high-level efforts in civil aviation cybersecurity" with a focus on several objectives, such as coordination at a European level, international cooperation, risk assessments, increasing awareness, information sharing and research and development. There was also a desire for the regulations to be internationally harmonized because the challenges need a wider holistic approach.
11. To develop a cybersecurity strategy, cyber risk management goes from concept, design, development, delivery, operations and maintenance; there is therefore a need for a global and comprehensive approach. In order to bridge the gap between the present situation and the desired outcome there is a need to mitigate the risks and threats in the new cyber environment.

— END —