CYBERSECURITY AND RESILIENCE SYMPOSIUM
PROTECTING AVIATION FROM CYBER ATTACKS
DOHA, QATAR | 6 – 8 NOVEMBER 2023
ICAO MID
الهيئة العامة للطيران المدني
CIVIL AVIATION AUTHORITY
QATAR قطر

Cybersecurity and Resilience Symposium

(Doha, Qatar, 6 – 8 November 2023)

Summary Outcome

Symposium Objectives

The main objectives of the Cybersecurity and Resilience Symposium were to:

- **address cybersecurity from two different perspectives (AVSEC and ANS);**
- **raise awareness about cyber threats, risks, challenges and solutions;**
- **foster a cybersecurity culture that promotes a resilient and secure cyberspace; and**
- **provide a forum for sharing experience and best practices.**

- **96 Participants**
- **13 States**
- **3 International Organizations**

Agenda

Session 1: Setting the scene

Session 2: Cyber-attack Governance and effective legislation and regulations: a path to Cyber maturity

Session 3: Aviation Cybersecurity Framework: to enhance the resilience of aviation infrastructure against cyber threats

Session 4: Effective Cybersecurity intelligence and Monitoring techniques: to mitigate Cyber-attack impact

Session 5: Emergency Response and Contingency Planning

Session 6: Cybersecurity Case study

Session 7: Human Factors in Cybersecurity

Session 8: Aviation Cybersecurity: Emerging Challenges and Solutions

CYBERSECURITY AND RESILIENCE SYMPOSIUM

PROTECTING AVIATION FROM CYBER ATTACKS

DOHA, QATAR | 6 – 8 NOVEMBER 2023

ICAO MID

الهيئة العامة للطيران المدني
CIVIL AVIATION AUTHORITY
QATAR قطر

Session 2: Cyber-attack Governance and effective legislation and regulations: a path to Cyber maturity

Outcomes, Challenges and Recommendations

Session 2: Outcomes

- Recognized the need for national governance and coordination in cybersecurity.

- Highlighted the importance of formulating effective legislation and regulations at the state level.

Session 2: Challenges

- Lack of coordinated national governance structures for cybersecurity.

- Insufficient legislation and regulations in place to address cyber threats effectively.

Session 2: Recommendations

- Establish competent national authorities responsible for cybersecurity.
- Develop and enforce comprehensive legislation and regulations to enhance cybersecurity.
- Foster international cooperation and information sharing to address cyber threats collectively.

CYBERSECURITY AND RESILIENCE SYMPOSIUM

PROTECTING AVIATION FROM CYBER ATTACKS

DOHA, QATAR | 6 – 8 NOVEMBER 2023

ICAO MID

الهيئة العامة للطيران المدني
CIVIL AVIATION AUTHORITY
QATAR قطر

Session 3: Aviation Cybersecurity Framework: to enhance the resilience of aviation infrastructure against cyber threats

Outcomes, Challenges and Recommendations

Session 3: Outcomes

- Explored real instances of cyber-attacks on aviation infrastructure and their impact on safety and service disruption.

- Discussed cybersecurity frameworks focusing on risk management and identification of threats and vulnerabilities.

- Showcased best practices for protecting critical aviation infrastructure from cyber threats.

Session 3: Challenges

- Increasing sophistication and frequency of cyber-attacks targeting aviation systems.

- Ensuring the implementation and compliance of cybersecurity frameworks across the aviation industry.

Session 3: Recommendations

- Enhance cybersecurity awareness and training programs for aviation personnel.

- Implement robust risk management frameworks to identify and mitigate cyber threats.

- Foster collaboration between aviation stakeholders to share information and best practices.

CYBERSECURITY AND RESILIENCE SYMPOSIUM

PROTECTING AVIATION FROM CYBER ATTACKS

DOHA, QATAR | 6 – 8 NOVEMBER 2023

ICAO MID

الهيئة العامة للطيران المدني
CIVIL AVIATION AUTHORITY
QATAR قطر

Session 4: Effective Cybersecurity intelligence and Monitoring techniques: to mitigate Cyber-attack impact

Outcomes, Challenges and Recommendations

Session 4: Outcomes

- Emphasized the importance of information sharing on cybersecurity vulnerabilities, threats, and best practices.

- Highlighted the need for incident management mechanisms and cybersecurity integration in national contingency planning.

- Explored effective monitoring tools, including the establishment of Security Operation Centers (SOC).

Session 4: Challenges

- Limited information sharing and collaboration among organizations in the cybersecurity domain.

- Lack of standardized incident management mechanisms and protocols.

Session 4: Recommendations

- Establish robust information sharing networks and platforms for cybersecurity intelligence.

- Develop national contingency plans that incorporate cybersecurity considerations.

- Invest in advanced monitoring tools and capabilities, including the establishment of SOC.

CYBERSECURITY AND RESILIENCE SYMPOSIUM

PROTECTING AVIATION FROM CYBER ATTACKS

DOHA, QATAR | 6 – 8 NOVEMBER 2023

ICAO MID

الهيئة العامة للطيران المدني
CIVIL AVIATION AUTHORITY
QATAR قطر

Session 5: Emergency Response and Contingency Planning

Outcomes, Challenges and Recommendations

Session 5: Outcomes

- Shared best practices and experiences related to contingency plans and emergency response in the aviation sector.
- Highlighted the importance of formal emergency response plans for a seamless transition from normal to emergency operations.

Session 5: Challenges

- Developing comprehensive and effective emergency response plans tailored to the aviation industry.

- Ensuring coordination and cooperation among multiple stakeholders during emergency situations.

Session 5: Recommendations

- Develop emergency response plans specific to the aviation sector.
- Conduct regular drills and simulations to test and improve emergency response preparedness.
- Enhance collaboration and communication channels among stakeholders in emergency situations.

CYBERSECURITY AND RESILIENCE SYMPOSIUM

PROTECTING AVIATION FROM CYBER ATTACKS

DOHA, QATAR | 6 – 8 NOVEMBER 2023

ICAO MID

الهيئة العامة للطيران المدني
CIVIL AVIATION AUTHORITY
QATAR قطر

Session 6: Cybersecurity Case study

Outcomes, Challenges and Recommendations

Session 6: Outcomes

- Engaged participants in a simulated cybersecurity incident scenario to enhance preparedness.

- Provided insights into the outcomes and challenges of dealing with cybersecurity incidents.

Session 6: Challenges

- Rapidly evolving nature of cyber threats and attack techniques.
- Limited resources and expertise for handling cybersecurity incidents effectively.

Session 6: Recommendations

- Conduct regular cybersecurity training and exercises to improve incident response capabilities.

- Establish collaboration and coordination mechanisms for incident response among relevant organizations.

- Stay updated on emerging cybersecurity trends and share knowledge within the aviation community.

CYBERSECURITY AND RESILIENCE SYMPOSIUM

PROTECTING AVIATION FROM CYBER ATTACKS

DOHA, QATAR | 6 – 8 NOVEMBER 2023

ICAO MID

الهيئة العامة للطيران المدني
CIVIL AVIATION AUTHORITY
QATAR قطر

Session 7: Human Factors in Cybersecurity

Outcomes, Challenges and Recommendations

Session 7: Outcomes

- Explored the role of human factors in cybersecurity and vulnerabilities related to security knowledge and skills.

- Emphasized the need to build a cybersecurity culture and strengthen cybersecurity skills and capacity.

Session 7: Challenges

- Lack of cybersecurity awareness and training among aviation personnel.
- Human errors and social engineering attacks as significant cybersecurity risks.

Session 7: Recommendations

- Implement comprehensive cybersecurity training programs for aviation personnel at all levels.

- Foster a culture of cybersecurity awareness and accountability within organizations.

- Invest in continuous skill development and capacity building to mitigate human-related cybersecurity risks.

CYBERSECURITY AND RESILIENCE SYMPOSIUM

PROTECTING AVIATION FROM CYBER ATTACKS

DOHA, QATAR | 6 – 8 NOVEMBER 2023

ICAO MID

الهيئة العامة للطيران المدني
CIVIL AVIATION AUTHORITY
QATAR قطر

Session 8: Aviation Cybersecurity: Emerging Challenges and Solutions

Outcomes, Challenges and Recommendations

Session 8: Outcomes

- Discussed the challenges posed by emerging technologies and increasing connectivity in aviation cybersecurity.
- Explored means to manage complexity and improve safety and efficiency in flight operations.
- Highlighted the potential of emerging technologies for enhancing cybersecurity in aviation

Session 8: Challenges

- Rapid advancements in technology outpacing cybersecurity measures and practices.
- Balancing connectivity and automation with the need for robust cybersecurity measures.

Session 8: Recommendations

- Promote research and development in aviation cybersecurity to address emerging challenges.

- Implement risk-based approaches to cybersecurity, considering the evolving threat landscape.

- Foster collaboration between aviation stakeholders, technology providers, and cybersecurity experts to develop innovative solutions.

THANK YOU