Aviation Cybersecurity National Governance

Bashar Ahmed Alohali

Background

- The global aviation IoT market, which encompasses aspects of both OT and IT, was valued at 6.88$ billion in 2022 and is projected to grow at a compound annual growth rate (CAGR) of 23.3% from 2023 to 2030.
- Additionally, the global market for Airport Information Systems is expected to grow from 3.21$ billion in 2021 to 4.20$ billion in 2028, reflecting a CAGR of 3.89% over the period 2021-2028.
- The global Advanced Airport Technologies Market is forecasted to grow from 27.92$ Billion in 2023 to 45.3 Billion by 2032, reflecting a continued investment in advanced technologies at airports.

Civil Aviation Sector Overview

- Airport

1. **Baggage Handling Systems**: ensures the transportation of baggage from check-in to aircraft.
2. **Security Systems:** monitor and ensure airport security.
3. **Information Display Systems:** Provide flight information, announcements, and advertisements.

Civil Aviation Sector Overview

Airport:

4. **Check-in Systems**: Automate the check-in process for passengers.
5. **Maintenance Systems:** Manage and schedule maintenance activities.
6. **Airport Operation Systems:** Centralize operations management including scheduling, resource allocation, etc.

Civil Aviation Sector Overview

- Air Navigation:

1. **Air Traffic Management (ATM)**: Ensures safe and efficient navigation through the control of air traffic.
2. **Communication Systems:** Ensure clear communication between aircraft and ground stations.
3. **Surveillance Systems:** Monitor and provide information on aircraft position and movement.

Cybersecurity in Civil Aviation Sector

- Cybersecurity Issues in Aviation Sector:

1. **Vulnerability of Key Systems**: Systems such as Aircraft IP Networks, Digital Air Traffic Controls (ATCs), and Flight-By-Wire Systems are susceptible to cyber threats due to their digital nature.
2. **Operational Technologies (OT)**: These technologies are prevalent areas of cyber risk in the aviation industry requiring effective cybersecurity measures for protection.

Cybersecurity in Civil Aviation Sector

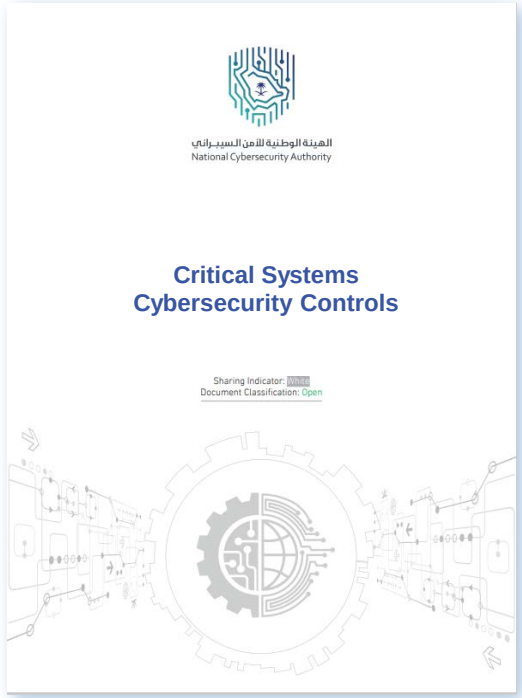
- Cybersecurity Issues in Aviation Sector:

3. **Supply Chain Vulnerabilities:** Insecure supply chains, vulnerability of third-party and supplier operations, and digitization of operations expose the aviation sector to additional cybersecurity risks.
4. **Interconnected Systems:** The interoperation of multiple systems needs protection from a cybersecurity perspective due to their interconnectedness.

Cybersecurity Attacks in Civil Aviation Sector

- The rate of unique malware attacks increased by 50% between October 2022 and January 2023.
- There was a 530% increase in cyber-attacks reported to Eurocontrol between 2019 and 2020. In 2020, there were 775 cyber-attacks on airlines and 150 at airports.
- In the first half of 2023, cyberattacks in the aviation industry surged by 24% worldwide.
- The rate of unique malware attacks increased by 50% between October 2022 and January 2023, as per a 2023 **Blackberry Global Threat Intelligence Report.**

National Cybersecurity Authority (NCA) in Saudi Arabia



Aviation International Instruments and Documents

Aviation Industry International Instruments and Documents	
International Air Law Instruments	• Convention for the Suppression of Unlawful Seizure of Aircraft (1970) • Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971) • Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971) • Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (2010) • Beijing Supplementary Protocol to the 1970 Hague Convention for the Suppression of Unlawful Seizure of Aircraft (2010)
International Civil Aviation Organization (ICAO)	• Annex 17 – Security. Safeguarding International Civil Aviation Against Acts of Unlawful Interference • ICAO Aviation Cybersecurity Strategy • Doc 8973 Aviation Security Manual (Restricted) • Doc 9985 Air Traffic Management Security Manual (Restricted) • Doc 10108 Global Risk Context Statement (Restricted) • Assembly Resolution A40-10: Addressing Cybersecurity in Civil Aviation
European Commission	• Commission Implementing Regulation (EU) 2015/1998 of 5 November 2015 laying down detailed measures for the implementation of the common basic standards on aviation security • Commission Implementing Regulation (EU) 2019/1583 of 25 September 2019 amending Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures • Commission Implementing Regulation (EU) 2017/373 of 1 March 2017 laying down common requirements for providers of air traffic management/air navigation services and other air traffic management network functions and their oversight, repealing Regulation (EC) No 482/2008, Implementing Regulations (EU) No 1034/2011, (EU) No 1035/2011 and (EU) 2016/1377 and amending Regulation (EU) No 677/2011 • Transport Cybersecurity Toolkit
European Strategic Coordination Platform (ESCP)	• Strategy for Cyber Security in Aviation
Qatar (Civil Aviation Authority)	• Aviation Cyber Security Guidelines

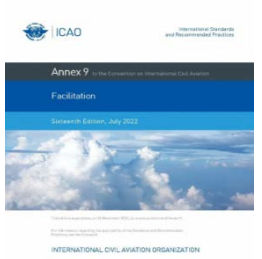
Relevant Cyber Industry Framework

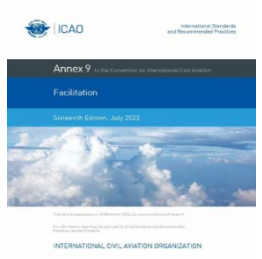
Framework	*Description*
International Organization for Standardization (ISO)	ISO/IEC/IEEE 15288:2015 Systems and software engineering—Systems life cycle processes ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management ISO/IEC 27036-1:2014 Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts ISO/IEC 27036-2:2014 Information technology — Security techniques — Information security for supplier relationships — Part 2: Requirements • ISO/IEC 27036-3:2013 Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security
National Institute of Standards and Technology (NIST)	NIST Framework for Improving Critical Infrastructure Cyber Security • NIST SP 800-37 Rev. 2 Risk Management Framework for Information Systems and Organizations—A System Life Cycle Approach for Security and Privacy • NIST SP 800-39 Managing Information Security Risk: Organization, Mission, and Information System View • NIST SP 800-53 Rev. 5 Security and Privacy Controls forInformation Systems and Organizations • NIST SP 800-82 Rev. 2 Guide to Industrial Control Systems (ICS) Security • NIST SP 800-160 Vol. 1 Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems • NIST SP 800-160 Vol. 2 Rev. 1 Developing Cyber Resilient Systems: A Systems Security Engineering Approach • NIST SP 1900-202 Cyber-Physical Systems and Internet of Thing • NIST IR 8259 Recommendations for IoT Device Manufacturers • NIST IR 8259 Recommendations for IoT Device Manufacturers • NIST IR 8276 Key Practices in Cyber Supply Chain Risk Management: Observations from Industry
International Society of Automation	ISA/IEC 62443-2-1:2009 Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program ISA/IEC 62443-3-3:2013 Security for industrial automation and control systems Part 3-3: System security requirements and security levels ISA/IEC-62443-4-2-2018 Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components
National Cybersecurity Authority (NCA) - KSA	Essential Cybersecurity Controls (ECC-1:2018) Operational Technology Cybersecurity Controls (OTCC-1:2022) Critical Systems Cybersecurity Controls (CSCC-1:2019)

Aviation Cybersecuritv National Governance

Aviation International References

International Civil Aviation Organization





Local References

الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

NCA - CCC

NCA - ECC

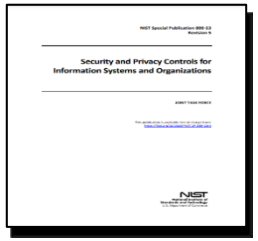
NCA - CSCC

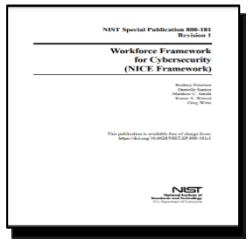
Cybersecuirty International References

COBIT 5

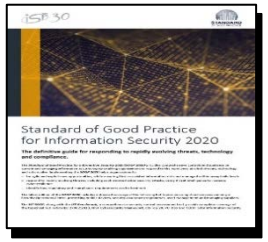
ISO27K

NIST – 800 53 and NICE





ISF Standard of Good Practice



The need for Cybersecurity National Governance for Aviation Sector

- **Support the stakeholders:** Cybersecurity in the aviation sector is pivotal in supporting stakeholders such as airlines, airport authorities, aviation service providers, government agencies, and passengers.
- **standardize coexisting entities:** Promote understanding as well as regulating how different entities can co- exist within the same ecosystem and operate in a secure manner.
- **Unique aviation systems** : Aviation systems are considered to be unique as special controls, requirements and procedures are needed in airplanes, airports and communications centers.

References

- "Aviation IoT Market Size, Share And Growth Report, 2030“ from www.grandviewresearch.com
- "Airport Information Systems Market Size, Trends | Growth, 2021-2028" www.fortunebusinessinsights.com
- "Advanced Airport Technologies Market to Reach USD 45.3“ www.globenewswire.com
- BlackBerry. (2023). Global Threat Intelligence Report. Retrieved from BlackBerry Website
- LinkedIn Article. (2021). Cyber Security in Civil Aviation: A Critical Concern. Retrieved from LinkedIn.
- Simple Flying. (2023). Cyberattacks Are On The Up: What Are The Risks & Remedies For Aviation? Retrieved from simpleflying.com.

THANK YOU