ADMM Cybersecurity and Information Centre of Excellence

UPDATE ON

THE CYBER DOMAIN

Issue 5/24 (May)

Cyber Threats in Aviation

INTRODUCTION

1. Aviation provides the only rapid worldwide transportation network which facilitates international commerce and business, trade and tourism. With the growing demand for air transport as well as advances in technology, the civil aviation sector has gone through digital transformation, like many other industries, to enhance its efficiency and capacity. The global aviation Internet of Things (IoT) market, valued at USD 7.4 billion in 2022 is projected to reach USD 50.9 billion in 2031, driven by the growing air travel trend emphasising passenger experience.

CYBER THREATS – CLEAR AND PRESENT DANGER

2. However, the aviation industry's digital advances also exposed the sector to cyber-attacks. The impact of a cyber-attack can be amplified given the global nature of the aviation sector, its reliance on interconnected digitised infrastructures to manage global supply chains as well as the handling of humongous volume of sensitive data – all of which made it an attractive target for malicious actors. According to Resilinc, in the first half of 2023, cyber-attacks in the aviation industry increased by 24% worldwide and ransomware attacks on supply chain players in 2023 went up as much as 600% compared to 2022.

3. Some of the impact of cyber-attacks include:

a. **Operational Disruptions**. As airport systems such as flight planning, information display systems, boarding processes, maintenance operations and air navigation systems such as digital air traffic controls, aircraft IP networks and flight-by-wire systems are heavily dependent on digital systems, a successful cyber-attack can cause significant disruptions to these operations.

b. **Financial Losses**. Direct costs include ransoms paid in ransomware attacks, regulatory fines and the resources need for incident response and system recovery. Indirect costs include lost revenue due to operational disruption, reputational damage, reduced sales due to drop in customer confidence.

c. **Data Privacy Violations**. The aviation industry handles massive amount of sensitive personal and financial information. A data breach can expose this information, violating privacy rules and regulations.

d. **Safety Risks**. If a cyber-attack were to interfere with flight control systems, a plane's systems can be hacked to affect its course, controls and passenger safety. If air traffic control systems were hacked, there may be confusion in the air and planes may not be able to fly, take off or land safely. The impact of a successful cyber-attack will be catastrophic if the aircraft is airborne.

RISING TIDE OF AVIATION CYBER THREATS

4. Threat actors are drawn to the aviation sector due to the high-value targets such as passenger information, financial records and proprietary technology, with motivations ranging from data and monetary theft to causing disruptions and harm. Among the most prevalent threats to the aviation industry are ransomware attacks, DDoS attacks and supply chain attacks.

5. **Ransomware Attacks**. Ransomware is one of the top threats facing the aviation industry with the European Organisation for the Safety of Air Navigation (Eurocontrol) reporting in 2023 that ransomware was the sector's leading attack trend in 2022, accounting for 22% of all malicious incidents. Disruptions caused by ransomware attacks may also cause major disruptions to operations on top of financial losses.

Case in point:
On 28 Feb 2024, Saudia Technic, the maintenance, repair, and overhaul (MRO) division of Saudi Arabian Airlines, became the target of a severe cyberattack staged by the notorious 8BASE ransomware gang. The gang encrypted essential files and demanded a ransom for decryption. Compromised targets may have included critical maintenance and operational databases, documentation and communication channels, disrupting essential Saudi Arabian Airline services. The impact was profound, potentially leading to significant disruptions in aircraft maintenance schedules, operational planning and communication systems.
This incident not only highlighted the vulnerabilities within critical aviation infrastructure but also raised concerns about the potential impact on aircraft maintenance and operational safety. It also illustrates the need for robust measures to protect essential data and ensure the continuity of operations.

6. **DDoS Attacks.** DDoS attacks, short for Distributed Denial-of-Service attacks, are deliberate efforts to render a system inaccessible by overwhelming it with a massive influx of traffic. DDoS attacks may prevent airports or users from using connected services on security screening or air traffic control systems, or block attempts to use passenger interfaces to access avionics and navigation systems onboard aircraft in mid-flight, leading to potentially catastrophic consequences.

Case in point:
On 12 Feb 2024, Los Angeles International Airport (LAX) fell victim to a DDoS attack conducted by a hacking group, Dark Strom Team. The massive surge in network traffic overwhelmed the servers, causing a temporary shutdown of the airport-la.com website and disrupted online services for both passengers and airport staff. Passengers relying on the airport's online services for flight information, bookings, and other essential functions were left in disarray. In response to the DDoS attack, the airport's cybersecurity team swiftly operationalised mitigation protocols traffic to restore normalcy to the affected online platforms.

The incident prompted a comprehensive review of the airport's cybersecurity infrastructure to fortify defenses against future attacks of this nature.

7. **Supply chain attacks**. The aviation industry's ecosystem is particularly vulnerable to supply chain attacks because it relies on a complex network of suppliers and vendors for everything from aircraft parts to software. Consequently, cyber-attacks on any part of the supply chain can trigger a cascading effect. A single breach can pave the way for infiltration and jeopardise various critical operations.

Case in point:
In 2023, attackers exploited a security vulnerability in MOVEit – a widely-used software used by organisations for file transfer – to steal data from the databases. More than 2,000 organisations were impacted by this attack campaign and affected more than 15 million individuals. Among those attacked included major carriers like British Airways, American Airlines, and Southwest Airlines. The breach was reported to be the result of a third-party vendor that manages pilot recruitment portals for a number of airlines. The stolen data is said to include staff names, staff ID numbers, passport numbers and national insurance numbers. The latter information is extremely valuable to identity thieves.
The Aerospace Industries Association expounded on threats to the sector's supply chain by stating "Civil Aviation has an enormously complex and globally connected supply chain". This globally diffuse complexity means that cyber-attacks can "impact nearly everything in the supply chain, from the data used to build physical structures, … to the electronic hardware itself."

CYBER RISK MANAGEMENT GUIDELINES

8. Global regulatory bodies like the International Civil Aviation Organisation (ICAO) and International Air Transport Association (IATA) have put forth measures and regulations to ensure that the civil aviation industry remains resilient and prepared against cyber-attacks. These include:

a. **Developing Standards and Recommended Practices (SRP) for all airlines**. The Chicago Convention provides a framework for international cooperation and regulation in aviation, including aspects related to safety, security, and efficiency. While the convention was primarily focused on traditional aviation concerns when it was established, the evolution of technology has necessitated its adaptation to address cybersecurity challenges. For example, ICAO has adopted a set of standards and practices to address cybersecurity in the aviation sector. This includes, amongst others, Recommended Practice 4.9.2 of Annex 17 to the Chicago Convention which highlights the importance of protecting critical systems and data. It mandates contracting states to implement measures to safeguard identified assets. These measures aim to fortify the resilience of aviation operations against unauthorised access, manipulation, or disruption. In addition, three ICAO Assembly Resolutions have been adopted since 2016 to address the challenges posed by cyber-attacks in the aviation sector.

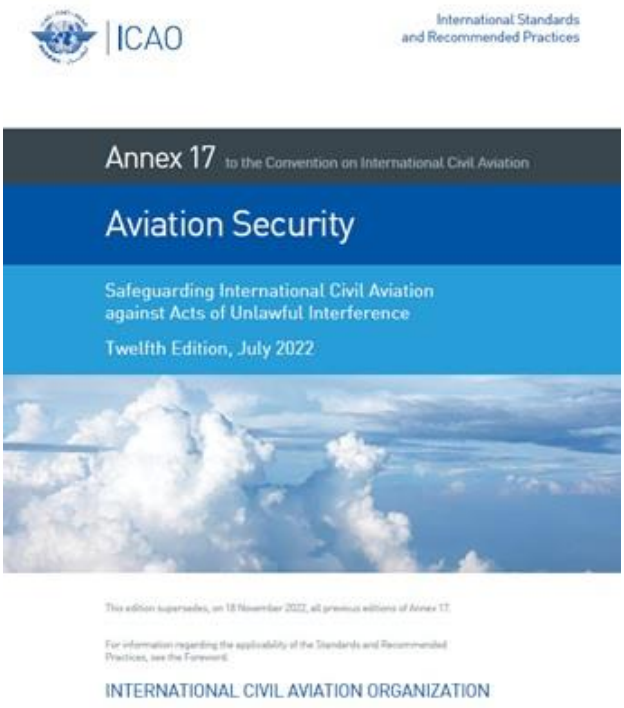

Fig 1: ICAO Annex 17 — Aviation Security (Source: ICAO)

b. **Supporting aviation cybersecurity discussions.** Global regulatory bodies have taken the lead in organising international forums, aimed at fostering knowledge exchange between states, international organizations and industry. Such forums bring together stakeholders to share best practices, exchange threat intelligence, and devise strategies to mitigate cyber risks effectively. This collective approach ensures that the industry remains vigilant, adaptive, and well-prepared to confront evolving cyber threats.

Fig 2: ICAO Council President addressing the UAE's High-Level Conference on Cybersecurity in Civil Aviation (Source: ICAO)

9. To bolster existing efforts in protecting the aviation sector from cyber risks, it is advisable to implement additional measures aimed at reinforcing security protocols and increasing resilience. These include:

a. **Regular testing of emergency response plans.** This is essential to refine plans and enhance the capabilities of responders. These tests should involve all relevant stakeholders and incorporate a mix of Table Top Exercises (TTX) and live simulations.

b. **Aircraft System Hardening and Redundancy.** To fortify aircraft systems, manufacturers and operators should use hardware-based security mechanisms such as trusted platform modules (TPMs) to protect critical system components from tampering and unauthorised access. Furthermore, it is crucial to ensure the adoption of up-to-date systems and software, with regular checks for vulnerabilities. Multi-factor authentication protocols should also be implemented for enhanced identity verification and access control management.

c. **Performing Supply Chain Mapping Exercises.** Organisations could conduct a supply chain mapping exercise so as to know exactly which companies are in their direct and indirect supply chains. This will allow companies to respond faster to any cyber-attacks and prevent a cascading effect on any downstream operations.

CONCLUSION

10. In conclusion, the aviation sector faces significant challenges in the realm of cybersecurity. While regulatory bodies have made strides in addressing these risks, further measures are essential to safeguard airports, airlines and passengers. Only through a concerted and vigilant approach to cybersecurity can organisations navigate the challenges of the digital age and secure aviation operations.

Contact Details

All reports can be retrieved from our website at www.acice-asean.org/resource/.

For any queries and/or clarifications, please contact ACICE, at ACICE@defence.gov.sg.

Prepared by:
ADMM Cybersecurity and Information Centre of Excellence

• • • •

References

1. Cyberattacks Are On The Up: What Are The Risks & Remedies For Aviation?
https://www.resilinc.com/in-the-news/cyberattacks-are-up-the-risks-remedies-for-aviation/

2. Cyber Threats Faced by the Aviation Industry - Security Boulevard
https://securityboulevard.com/2023/06/top-cyber-threats-faced-by-the-aviation-industry/

3. Resecurity | The Aviation and Aerospace Sectors Face Skyrocketing Cyber Threats
https://www.resecurity.com/blog/article/the-aviation-and-aerospace-sectors-face-skyrocketing-cyber-threats

4. Information on MOVEit Vulnerability CVE-2023-34362
https://news.sophos.com/en-us/2023/06/05/information-on-moveit-transfer-and-moveit-cloud-vulnerability-cve-2023-34362/

5. Annex 17 — Aviation Security
https://www.icao.int/Security/SFP/Pages/Annex17.aspx

6. ICAO UAE mission fosters new agreement and progress on aviation cybersecurity and innovation
https://www.icao.int/Newsroom/Pages/CAO-UAE-mission-fosters-new-agreement-and-progress-on-aviation-cybersecurity-and-innovation.aspx