Navigating the Skies of Cybersecurity: Unveiling Real-World Attacks and Risk Management in Aviation

Saif AL Ghafri, Cyber Security Inspector

Aviation's Digital Journey

- Analog to Digital Transition – Analog instruments consolidated into integrated digital display systems
- Connectivity - Passengers wanting more Services
- Data Collection & Analysis (Big Data)
- Automation & Fly-by-Wire (Previously manual flight controls)
- Digital Twin Tech
- AI & Machine Learning

Aviation's Digital Journey Challenges

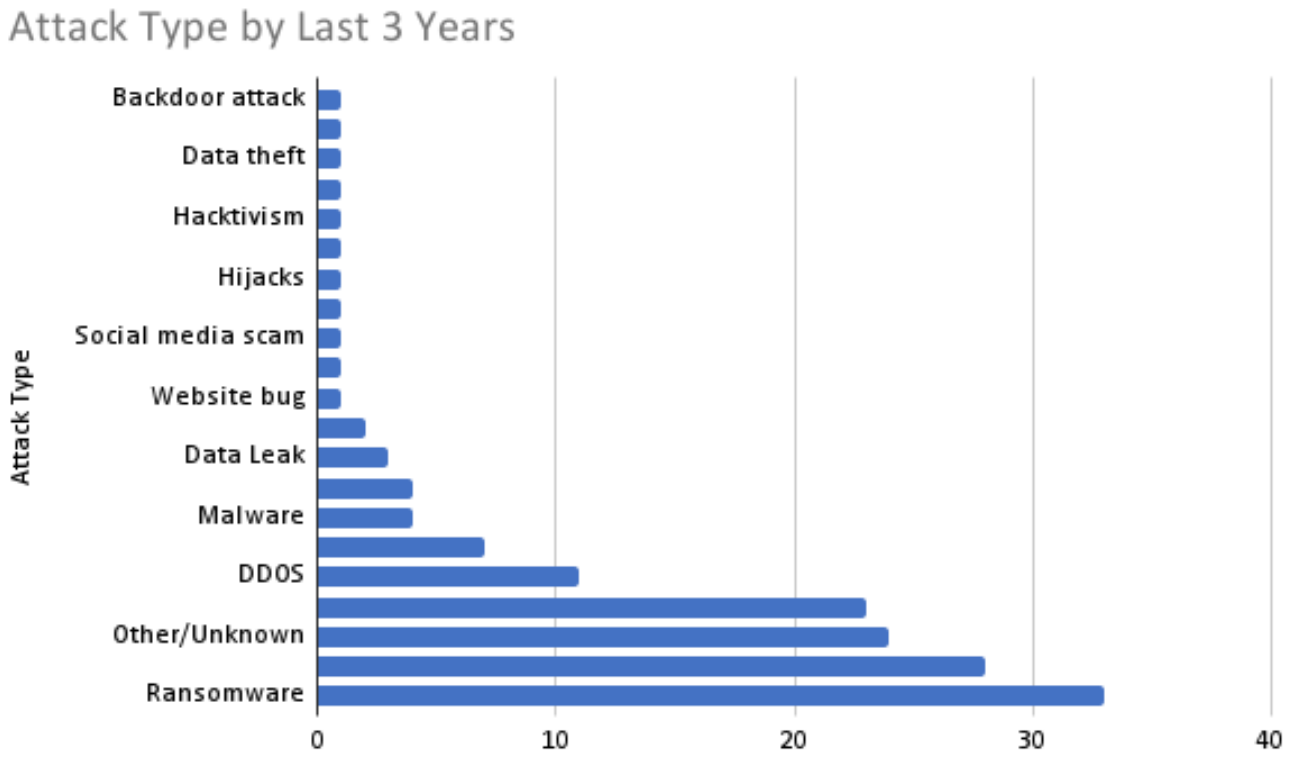
- Cybersecurity (Front & Center)
- Legacy Systems Integration
- Regulation & Standardization
- Talent Shortage
- Privacy
- Reliability
- Tech Development

AI Generated Image

Existing Vulnerabilities

- Legacy Systems
- Integrated Digital Tech
- 3rd Party Vendors (Supply Chain)
- Human Factor (Staff, Passengers, Crews)

Attack Types Targeting The Aviation Industry



https://socradar.io/top-cyber-threats-faced-by-the-aviation-industry/

Aviation Cyber Attacks

- In 2020 there were 52 reported attacks
- In 2021 there were 48 reported attacks
- In 2022 there were 50 reported attacks (End of August)
- Seven Aviation attacks in August 2022 that had some serious effects
- Eight military-related incidents were reported.

- https://socradar.io/top-cyber-threats-faced-by-the-aviation-industry/

Aviation Cyber Attacks

- Most entities are constantly under attack all the time but in a passive way such as port scans, pings, and traffic monitoring
- It is the results of these passive attacks that allows the attacker to find open ports and protocols
- Cyber attacks on the Aviation Industry have been on the rise, increasing by 24% worldwide in the first half of 2023

Real-World Impact

- Consequences of August 2022 successful cyber-attacks
- Grounded flights with knock on effects for connecting flights and massive delays
- Compromised passenger data (names, Addresses, and Passport numbers)
- Financial repercussions can extend into the millions
- Potential of causing catastrophic Aircraft Mishaps and crashes

Real-World Examples

- **Russian flight booking system suffers ‘massive’ cyberattack - September 2023**

  A "massive" DDoS attack on the local airline booking system Leonardo was carried out lasting about an hour affecting the operation of several Leonardo customers, including Russian air carriers Rossiya Airlines, Pobeda and flagship airline Aeroflot. The incident caused delays of up to an hour for departures the country’s busiest airport in Moscow

- **Cathay Pacific Airways – 9.4M Breached Records - 2018**

  The most serious data breach in airline history to date. The attack affected 9.4 million Cathay Pacific passengers. The stolen data included passport details, birth dates, frequent flier numbers, phone numbers and credit card information. The breach ran for a few months (March to May 2018 and beyond)

- https://therecord.media/russia-flight-booking-system-leonardo-ddos
- https://www.bbc.com/news/business-45974020

Real-World Examples

EasyJet Admits Data Of Nine Million Hacked – January 2020

EasyJet was the victim of a cyber-attack in which hackers obtained the credit-card information of 2,208 customers. The carrier did not notify passengers of the attack until 4 months after the incident, in May 2020 and as a result they are now facing a class-action suit from 10,000 passengers, seeking around £18 billion in damages

Russia's Air Transport Agency Affected By Cyberattacks – March 2022

In what appears to have been a retaliatory strike in response to Russia's invasion of Ukraine, an unidentified group (presumed to be the Anonymous Hacking Group) carried out an extremely effective attack on the Russian Federal Air Transport Agency. As part of the attack, all aircraft registration data and emails, totaling approximately a massive 65 terabytes of data, were deleted from the Agency's servers. The attack was so successful that until back-up copies of the electronic data could be found the Agency was forced to resort to using pen and paper and to sending information in hard copy through the post

- https://www.bbc.com/news/technology-52722626
- https://www.securitymagazine.com/articles/97340-russias-air-transport-agency-affected-by-cyberattacks

Strengthening Aviation Infrastructure Resilience

- **Strengthen the digital perimeter**
  Encryption, firewalls, and intrusion detection
- **Cross-sector Collaborations**
  Airlines, tech providers, airports, and Govt's.
  Sharing of threats and solutions information
- **Regulations & Industry standards**
  Standardized Cybersecurity measures
- **Scenario Driven Analytics and Drills**
- **Restrict data access based on an end users' 'business need to know'**
- **Implement Technology That Detects Suspicious Log-ins, Particularly From Unanticipated Geographical Regions**
- **Security-by-Design**

Strengthening Aviation Infrastructure Resilience

- **Leveraging Tech Solutions**
  AI – Monitoring and Detection
  Blockchain secure data transactions (ground to ground and Ground to Air)

- **Risk Based Approach/Assessments/Management**
  Threats are not equal
  Prioritize Risks based on severity, Impact, and probability
  Evaluate Resource allocation effectiveness

- **Shore up the weakest link (Human Factor)**
  Awareness Training, embrace a culture of vigilance

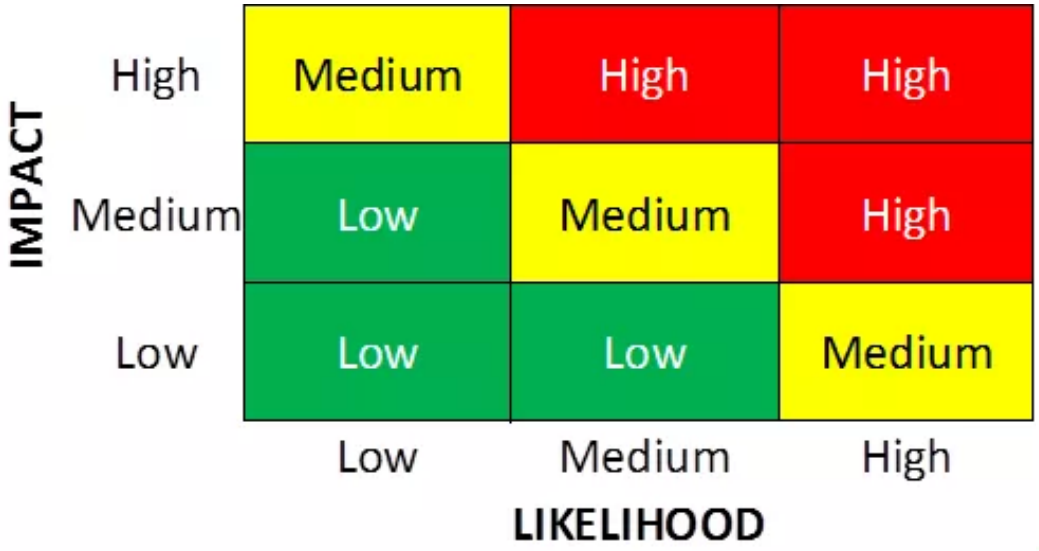
- **Redundancy (Avoid/prevent single points of Failure)**

Cybersecurity Risk Management & Assessment

- **What's the difference? Identification vs Mitigation**
- **Benefits**
  - More efficient and consistent operations
  - Identify and avoid unapparent risks
  - Improving overall resiliency and cyber posture
  - Establish a baseline of cybersecurity measurements

Cybersecurity Risk Assessment Steps

- **Identify and Document Network Asset Vulnerabilities**
  Hardware/Software, Vendor, Internal/External Interfaces, Access, Date of Last Update
- **Identify and Use Sources of Cyber Threat Intelligence**
  National & International sources
- **Identify and Document Internal and External Threats**
  Administrative privileges on a network or hardware, activity logs of users with granted access
- **Identify Potential Mission Impacts**
  Shared resources & dependencies
- **Use Threats, Vulnerabilities, Likelihoods, and Impacts to Determine Risk**
  Assumptions of High, Medium, and Low
- **Identify and Prioritize Risk Responses**
  List of identified personnel and groups



Conclusion

- **Cyber Criminals Are Exploiting New Technologies**
- **Cybersecurity Is A Concern For All Parties**
- **Framework Unites All In A Common Goal**
- **Do Not Forget About The Weakest Link**

  All the firewalls in the world will not help if you let the fundamentals of Info Sec fall to the wayside

  Training and Awareness are Essential

THANK YOU