Cyber Threats in Aviation Sector
Agenda:

1. Oman Civil aviation Authority (PACA) duties & responsibilities
2. Cyber Risks
3. Cyber Threats in Aviation Sector
4. Recommendations
5. Oman Aviation Group's Effort
Oman Civil aviation Authority (PACA) duties & responsibilities
Oman Civil aviation Authority (PACA) duties & responsibilities:

The (PACA) responsible for the implementation of the Oman Civil Aviation Law, in compliance with Chicago convention 1944, that include but not limited to:

- Regulation, supervision and oversight of the establishment and operation of civil airports, airfields, heliports and their facilities.
- Regulation and oversight of the safety and security of civil aviation, commercial air transport facilities, general aviation, air operators, air navigation services, meteorology and any other civil aviation activities.
- Issuance and publication of regulations as well as the National Civil Aviation Security Program, National Air Transport Facilitation Program, State Safety Program and any other national programs and monitoring of their implementation.
- Issuance of the necessary rules to ensure clear separation between the regulatory functions, and the operational functions relating to civil aviation activities as well as air navigation and meteorological services.
Cyber Risks’ Factors

- **85%** airline CEOs expressed their concerns about **Cyber Security Risk**\(^{(1)}\)
- **39 seconds** is the average time taken for a **Cyber Attack**\(^{(2)}\)
- **780,000 records** were **Hacked** per day in 2017\(^{(4)}\)
- **63%** of **Cyber Attacks** are result of compromised user passwords\(^{(5)}\)
- **Cybercrime**, 2\(^{nd}\) Most reported economic crime affecting organizations globally\(^{(1)}\)

Source: (1) PwC, (2) University of Maryland, (3) SITA, (4) McAfee, (5) Microsoft
Cyber Risks’ Factors

$600 billion global cost of Cybercrime in 2017

$1.5 trillion total revenue Cybercriminals coaxed worldwide in 2017

$3.8 million average cost of a Data Breach to a company

$158 billion consumers money lost globally due to Cybercrime in 2015

$6 trillion is annual projected cost of Cybercrime by 2021

0.8% of world GDP is lost to Cybercrime

Source: (1) McAfee, (2) RSA, (3) Symantec, (4) Cyber-Ventures
Cyber Risks’ Factors

Over the last three years, the percentage of reported incidents increased exponentially, and following are the Top Contributing Factors:

- 1,464 government officials in a state are using “Password123” as their password
- 2,000,000+ stolen identities used to make fake comments during inquiry into net neutrality
- $47,000 average total cost to a business from a single laptop loss
- 1,946,181,599 records containing personal and sensitive data compromised between Jan 2017 and Mar 2018
- $729,000 is average lost by a business executive phishing scam
- $3,500,000 average total cost to remediate a breach caused by human

Cyber Risks Impact in Aviation Sector

Airlines and airports have suffered some sort of a cyber attack that caused:

- **Customer Churn**: ~1 in 10 breaches result in > 20% customer churn
- **Recovery Time**: ~70 days is average recovery times Ranging from 7 to over 100 days
- **Brand & Reputation**: Brand and reputational damage
- **Share Price Decline**: Avg. 5% drop in share

Source: Associated Press, Open sourcing intelligence
Cyber Threats in Aviation Sector
Cyber Threats in Aviation Sector

Most of the reported breaches in the aviation sector targeted critical data:

- Personal Information
- Financial Data
- Flight Information
- Loyalty Program Data

Data Privacy Penalties
Financials impairments
Flight Operation Disruptions
Selling Free Miles in Dark web

Source: Associated Press, Open sourcing intelligence
Cyber Threats in Aviation Sector

- Intervention of aircraft control systems
- Disruption of airport systems and operations
- Disabling and blocking access into airlines’ and airports’ sites and web applications
- Airlines’ and Airports’ systems encryption by ransomware
- Compromising of security control systems and access to restricted area
- Compromising of data centers for currency mining
- Security breach of the baggage handling systems
- Security breach with the help from someone inside
# Cyber Threats in Aviation Sector

## Case Description
In 2017, an airlines was victim of a data breach caused by a flawed software.

<table>
<thead>
<tr>
<th>Type of Attack</th>
<th>Damage</th>
</tr>
</thead>
<tbody>
<tr>
<td>The cause is a vulnerability in the chat-bot application of a third-party vendor</td>
<td>Online chat service provider are on the receiving end of a proposed class action lawsuit</td>
</tr>
</tbody>
</table>

## Implemented Actions
After six months, the airline admitted the breach to the public.
Cyber Threats in Aviation Sector

**Case Description**
In 2018, two breaches compromised a total of almost 500,000 accounts for an airline.

<table>
<thead>
<tr>
<th>Type of Attack</th>
<th>Damage</th>
</tr>
</thead>
</table>
| The cause was probably an XSS attack. | • Stolen customer data.  
• Share price dropped by more than 4%  
• GDPR fine, up to another 4% of turnover |

**Implemented Actions**
Made an announcement through social media to the affected customers.
Cyber Threats in Aviation Sector

Case Description
In 2018, an airport information screens were taken offline early due to a massive cyber-attack.

<table>
<thead>
<tr>
<th>Type of Attack</th>
<th>Damage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ransomware.</td>
<td>Airport reputation</td>
</tr>
<tr>
<td>Caused several computer systems, the Wi-Fi and website to run slower and impacted the accuracy of security wait times and flight information online</td>
<td>Arrival and departures delays and reputation damage to affected airlines</td>
</tr>
<tr>
<td></td>
<td>Corruption of some critical databases</td>
</tr>
<tr>
<td></td>
<td>Possible financial liability</td>
</tr>
<tr>
<td></td>
<td>Privacy and personal data protection failure</td>
</tr>
</tbody>
</table>

Implemented Actions
Flights were unaffected, but contingency measures and "manual processes", including whiteboards and marker pens, had to be used in place of display screens.
Recommendations
1 - Implementation

ISMS (Information Security Management System) is a systematic approach to provide a reasonable assurance over the protection of the confidentiality, integrity, and availability of the group’s critical information assets.

- Aligning information security goals with business goals
- Improving information security posture
- Adopting renowned Information Security Standards
- Monitoring compliance level with legal and regulations
- Protecting both Physical and Logical Assets
1- Implementation

ISMS

Existing best practices, international standards and strategic objectives based on:

- NIST
- ISACA
- CObIT 2019
- ISO 27001
- ISO/IEC 38500
2- Cyber Security Awareness

- 90% of cyber-attacks were traced back to human error (1)
- 60% of employees do not know about critical Information Security Controls (2)
- 50% of Internet users receive at least one phishing email a day (3)
- 97% of the people in the world cannot identify a phishing email (3)
- 88% of employees positively answered about the need of information security awareness training (4)
- 72% of security incidents at financial services organizations actually involved either a current or former employee (5)

Source: (1) Verizon enterprise, (2) Schneier, (3) DarkReading, (4) SC Magazine, (5) PWC
2- Cyber Security Awareness

Phishing Email Simulations

Cyber Security Knowledge Testing

Cyber Security Awareness sessions

Information Security Awareness Email

Information Security Awareness

Posters and Trinkets
3- Cyber Resilience

- Regular Cyber Security Assessment
  - Black Box
  - Grey Box
  - White Box

- Supply Chain Management
  - Cyber Security Supply Chain Management

- Continuity and Recovery
  - Business Continuity Management Framework
  - Incident Responses Management
4- International and Sector Collaborations

World-wide aviation collaborations for the following domain:

- Workshops aimed at civil aviation authorities (legislators) and other professionals to build a secure and effective legislation and effective implementation of procedures to mitigate aviation related cyber risks and threats.

- Aviation tailored and integrated Information Security Management System (ISMS) to ensure best practices and procedures for data protection and systems used at the airports.

- Cyber incidents in aviation sector and coordination between different parties at national and international level to ensure recovery and prevention from cyber-aviation disasters internationally.
5- Cyber Security Investment Priority

Most adopted technologies by firms¹

<table>
<thead>
<tr>
<th>Technology</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Security</td>
<td>69%</td>
</tr>
<tr>
<td>Big Data</td>
<td>67%</td>
</tr>
<tr>
<td>Cloud</td>
<td>60%</td>
</tr>
<tr>
<td>Artificial Intelligence</td>
<td>56%</td>
</tr>
<tr>
<td>3D Printing</td>
<td>50%</td>
</tr>
</tbody>
</table>

Cybersecurity spend in Aviation

- % of airline and airports CIOs plan a major program around cybersecurity initiatives in the next three years: 89%
- % of IT budget spent on cybersecurity:
  - 2017: 7 Airline, 10 Airport
  - 2018: 9 Airline, 12 Airport

¹ Percentage based on panel of 1,000 interviews made to senior IT and business decision makers of companies with >1,000 employees and >$500 Bln $ revenues.
² Percentage based on surveys made to a panel of senior IT and business leaders of the corresponding sectors.

Oman Aviation Group Efforts
Oman Public Authority for Civil Aviation (PACA) foresaw the eminent risks from cyber domain, and mandate the establishment of a cyber security unit. Following are some of the efforts:

- NIST and COBIT Maturity Assessment
- ISMS Implementation
- Comprehensive Cyber Security Assessment
- Cyber Security Strategies and Roadmap
- Group Wide Cyber Security Awareness
Thank You