As a cybersecurity expert, I foresee several emerging cyber threats that are likely to target airline companies globally. Airlines are critical infrastructure and heavily reliant on interconnected systems, making them attractive targets for cyber criminals and hacktivist groups. In my years of experience, I and being directly involved in the IT Cyber Security, I see the following cyber threats coming up in the near future (2 to 3 years) that would impact the airline industry.

1. Ransomware Targeting Critical Infrastructure

Ransomware attacks are definitely not new, however they are now evolving at "light speed" and are not only majorly targeting the financial but evolving to target other critical sectors like transportation, including airlines. In a ransomware attack, hackers encrypt crucial systems and demand a ransom for their decryption. Airlines rely on real-time data for flight management, ticketing, cargo handling, and customer information. A ransomware attack on any of these systems go beyond getting financial reward, they extend into the following:

- **Flight cancellations and delays**: Hackers could take control of scheduling systems, ground operations, or even aircraft maintenance systems, causing absolute chaos.
- **Supply chain disruptions**: Interference with supply chain management and logistics could affect cargo flights and ground services.
- **Reputation damage**: Airlines could suffer immense repetitional harm if they are unable to ensure passenger safety and operational continuity.

Emerging Trends: Attackers are shifting towards a double extortion ransomware, where they not only encrypt data but also threaten to release sensitive customer and corporate information if the ransom is not paid. Airlines, handling sensitive passenger data and confidential cargo information, are high-value targets.

2. Deepfake-Assisted Social Engineering

Deepfakes, powered by AI, are becoming a new tool for cyber criminals to perform advanced **social engineering attacks**. For airlines, this can manifest in several ways:

- **Impersonating executives**: Hackers could use deepfake audio or video to impersonate airline CEOs or CFOs, convincing employees to make unauthorised financial transfers or change sensitive operational data.
- **Fake communications with passengers**: Hackers could generate convincing messages or videos from an airline's customer service, offering fake refunds or rescheduling flights, leading to phishing attacks on customers.

As airlines rely heavily on human interaction in customer service, operations, and vendor management, deepfake phishing could compromise internal decision-making and damage trust with passengers.

3. Supply Chain Attacks on Aviation Technology

Airlines depend on a vast ecosystem of third-party vendors, from IT service providers to aircraft maintenance software. Attackers could infiltrate these **supply chains** to introduce malware, backdoors, or compromise the systems that manage critical aviation operations. Supply chain attacks could lead to:

- **Operational sabotage**: An attacker could alter aircraft software or maintenance logs, leading to operational delays or even putting aircraft safety at risk.
- **Data breaches**: Through compromised vendors, attackers can access sensitive data related to flight schedules, crew rosters, and maintenance records.

Airlines are increasingly using IoT devices, real-time tracking, and predictive maintenance technologies that are often outsourced. This makes the attack surface larger and more vulnerable to supply chain attacks.

4. Targeted DDoS (Distributed Denial of Service) Attacks

DDoS attacks aim to overwhelm and disrupt online services by flooding website servers them with high volumes of data traffic. Airlines rely on their websites and mobile apps for flight bookings, check-ins, and customer support. A well-executed DDoS attack could lead to:

- **Service outages**: Disrupting flight booking, ticketing systems, or online customer support.
- **Passenger frustration**: Inability to access flight information or process payments could cause significant customer dissatisfaction.
- **Financial losses**: Prolonged downtime can result in millions of dollars in losses due to flight cancellations, compensations, and operational disruptions.

"Black Hat[1]" Hackers are now using **AI-enhanced botnets** that can dynamically adapt to overcome traditional defences, making these attacks more difficult to mitigate.

5. Attacks on Aircraft Systems and Avionics

With the increasing digitization and connectivity of modern aircraft, **cyberattacks on avionics systems** are a growing concern. Modern planes are equipped with internet-connected systems like onboard Wi-Fi, cockpit systems, and in-flight entertainment, which could be exploited if not properly secured. Potential threats include:

- **Hijacking aircraft communications**: Hackers could intercept or manipulate **ACARS (Aircraft Communications Addressing and Reporting System)** messages, which are used for air-to-ground communications.
- **Compromising flight control systems**: Although difficult, advanced attacks could attempt to exploit vulnerabilities in flight management systems or the onboard network, potentially impacting flight safety.

Emerging Threat: As **satellite communications** (SATCOM) is supporting aircraft, attacks on satellite uplinks or GPS spoofing could interfere with flight navigation, leading to rerouting or operational confusion.

6. Data Breaches and Privacy Violations

Airlines collect and process vast amounts of personal and financial data from passengers, including passport information, travel itineraries, payment details and sometimes health information. **Data breaches** targeting these could lead to identity theft, credit card fraud, or large-scale privacy violations. With increased regulatory scrutiny under laws like **GDPR**, **NIS2** and **CCPA**, airlines are at risk of facing:

- **Hefty fines**: Non-compliance with data protection regulations due to breaches, as well as with the new NIS2 legislation for essential and important entities that have now this mandatory law to abide to.
- **Class-action lawsuits**: From affected passengers who suffer from data breaches.
- **Loss of customer trust**: Frequent breaches can lead passengers to lose faith in the airline's ability to secure their personal information.

Hackers may also target **biometric data** as airlines adopt facial recognition for boarding and check-in. Biometric data breaches could be highly sensitive and difficult to remediate.

[1] A **black hat hacker** is a cybercriminal who exploits vulnerabilities in systems or networks for malicious purposes

7. IoT and 5G Vulnerabilities

The integration of **IoT** devices in airline operations—such as sensors for predictive aircraft maintenance, real-time baggage tracking, and in-flight systems—expands the attack surface for cybercriminals. Many IoT devices have limited security features, making them vulnerable to exploitation. With the deployment of **5G networks**, airlines are expected to enhance their connectivity, but this also brings new vulnerabilities:

- **Real-time sabotage**: Attacks on IoT-enabled sensors could lead to false readings or operational errors, disrupting flight operations or ground services.
- **Compromising smart airports**: As more airports adopt IoT for smart security, baggage handling, and automated check-ins, the risk of cyberattacks on these interconnected systems grows.

5G's higher bandwidth and low latency enable greater connectivity across devices, but this also means that attacks can spread faster and be harder to isolate.

8. Cyber Espionage and Nation-State Attacks

Airlines are often targets of **cyber espionage** conducted by nation-states looking to gather intelligence on passengers, trade routes, and geopolitical strategies. Airlines carry business executives, government officials, and sensitive cargo, making them attractive targets for espionage activities. Potential risks include:

- **Stealing flight manifests**: Nation-states could monitor the travel patterns of government officials, defence contractors, or corporate executives for intelligence purposes.
- **Disruption of international flights**: State-sponsored groups could target international flights to disrupt trade, commerce, or diplomatic relations.
- **Targeting corporate espionage**: Airlines involved in corporate deals or mergers may be targeted in order to steal sensitive information related to business operations.

Recommendations for Mitigating Emerging Cyber Threats in Airlines

Given the wide range of emerging threats, airlines must take proactive steps to boost their cybersecurity posture:

1 **Adopt a Zero-Trust Security Model**: Airlines should enforce a zero-trust model, ensuring that every access point, whether from within or outside the network, is authenticated and verified.

2 **AI-Based Threat Detection**: Incorporate AI-driven security systems that can detect anomalies in real-time, especially for ransomware, deepfake-based attacks, and supply chain compromises.

3 **Regular Audits and Penetration Testing**: Continuously audit critical systems, avionics, and operational technologies. Simulated cyberattacks (penetration tests) should be conducted frequently to identify vulnerabilities before attackers exploit them.

4 **Multi-Layered Defences**: Use a multi-layered cybersecurity defence, including encryption, multi-factor authentication (MFA), intrusion detection systems (IDS), and endpoint protection.

5 **Cybersecurity Training**: Airlines should regularly conduct cybersecurity awareness training for staff at all levels, particularly to recognise phishing, social engineering, and deepfake threats.

6 **Collaboration and Intelligence Sharing**: Join industry-wide cybersecurity consortiums & coalitions to share threat intelligence, best practices, and insights on emerging cyber threats.

7 Reach out to **FAA** to schedule Periodical sessions (trainings and otherwise) to learn from past attack attempts and prepare for future ones.

Conclusion

Airlines are becoming a prime target for cyberattacks as they integrate advanced technologies to improve efficiency and customer experience. From ransomware attacks and deepfake phishing to IoT vulnerabilities and supply chain compromises, airlines face an evolving and complex cyber threat landscape. By adopting a proactive and multi-layered security strategy, the airline industry can reduce the impact of these emerging threats and ensure the safety and trust of passengers worldwide.