unosecur

WHITEPAPER

Identity Security in Civil Aviation

Map key aviation cyber threats and outline mitigation strategies

Table of contents

Executive summary

The global civil aviation ecosystem is an interlinked system of various business subsectors: airlines, manufacturers, airports, MRO, support services, regulators, economic/environmental agencies, GDSs, alliances (i.e., Oneworld, Star Alliance), and general aviation. Their interdependence and the large public-facing interfaces in each create a broad attack surface.

Drawing on publicly available sources published between 1 January 2024 and 30 June 2025, including incident disclosures, news reports, regulatory publications, and analytical studies, the research consolidates sector-wide threat intelligence.

- The most severe and recurrent cyber threats across segments are credential theft, ransomware, malware, DDoS, GPS spoofing, and supply-chain attacks amplified by rapid digitalization, AI, cloud adoption, and IoT connectivity.
- Less centralized domains such as general aviation and oversight bodies face elevated risk due to fragmented defenses and their critical compliance roles.

An identity-centric taxonomy categorizes incidents into three stages: those that lead to compromise (such as phishing, supply chain, and IoT vulnerabilities), those that constitute active compromise (including credential theft and unauthorized access), and those that result from compromise (such as ransomware, data breaches, and operational disruption). Several documented cases demonstrate how third-party platforms and social engineering tactics can bypass internal defenses, highlighting vendor risk as a persistent point of exposure.

As for any infosecurity issue, there are apt solutions for identity security-related problems outlined in the following sections.

When viewed holistically, applying continuous least-privilege enforcement (ISPM), real-time detection and response (ITDR), and non-human identity governance (NHI Management) enables organizations to significantly reduce their attack surface, cut detection and response times to minutes, and minimize downstream business impact - placing them well ahead of most cyber threats.

Together, these capabilities enable aviation stakeholders to move from reactive compliance toward proactive identity resilience.

Constituents of the global civil aviation sector

The civil aviation sector is a broad field encompassing all non-military aviation. The following table lists the main constituents of the civil aviation sector, ranked by the estimated size of their global business (market value). The figures reflect approximate market sizes for 2024–2025.

Segment	Market size ($Bn)	Description
Air Transport Services (Airlines)	$760-763	The largest segment includes scheduled passenger and cargo airline operations.
Aircraft Manufacturing	$420	Covers commercial aircraft, engines, avionics; steady demand in deliveries reported by Boeing, Airbus.
Airport Infrastructure	$110-120	Includes airport operation revenues and capital investments, essential for air transport.
Maintenance, Repair, and Overhaul (MRO)	$66-70	Significant ongoing fleet maintenance market, roughly estimated from fleet size and spending growth.
Ground Handling Services	$45-50	Baggage, ramp, fueling, catering services are a smaller but critical support function.
Pilot and Aviation Training	$10-12	Includes commercial pilot training, airport check-in, and simulations; niche but growing segment.
Regulatory and Compliance	$8	Smaller in direct market size, mostly government or quasi-government expenditure on regulation.
General Aviation & Private Flying	$5-6	Private flying, business jets, recreational aviation; fragmented and smaller market share.
Global Distribution System	$19	Reservation systems, check-in, and passenger processes.

The figures are based on aggregated market research reports synthesizing industry revenue data, company financials, segment-specific analyses, and forecasting models covering commercial aviation activities. Each of these segments works together to enable the safe, efficient, and sustainable operation of civil aviation globally and within nations.

Top cybersecurity issues reported in each segment

Unosecur analyzed the following publicly available sources of information to determine the common attack vectors in each category of civil aviation. All of them were published between January 1, 2024 and June 30, 2025. The dataset synthesizes sources from the public domain, including:

Incident alerts:

Including 27 major ransomware attacks tracked and multiple airline data breach disclosures involving millions of passenger records.

News and media:

53 reports from industry news outlets describing specific attacks, trends, and sectorwide assessments.

Company disclosures:

14 official statements, including direct breach notifications and statements mentioning cybersecurity posture and responses.

Regulatory publications:

8 publications by government regulators across the world, including frameworks, mandates, and advisories from aviation regulatory bodies emphasizing cybersecurity roles and risk management.

News and media:

53 reports from industry news outlets describing specific attacks, trends, and sectorwide assessments.

Segment	Common attack vectors / Risks
Air Transport Services	Credential theft/unauthorized access (71%); ransomware attacks; DDoS on online services; GPS spoofing/jamming; social engineering (e.g., the Qantas breach); malware/ransomware disrupting operations; broader digitalization expanding the attack surface.
Aircraft and equipment manufacturing (AEM)	Software supply chain attacks (flight planning, maintenance, avionics); IoT/AI/cloud integration risks; vulnerable maintenance data systems; IP/design data theft.
Airport and nfrastructure	Attacks on management systems (kiosks, check-in, baggage); ransomware on operational networks; smart airport digitalization vulnerabilities; data exposure; threats to air navigation/ATC.

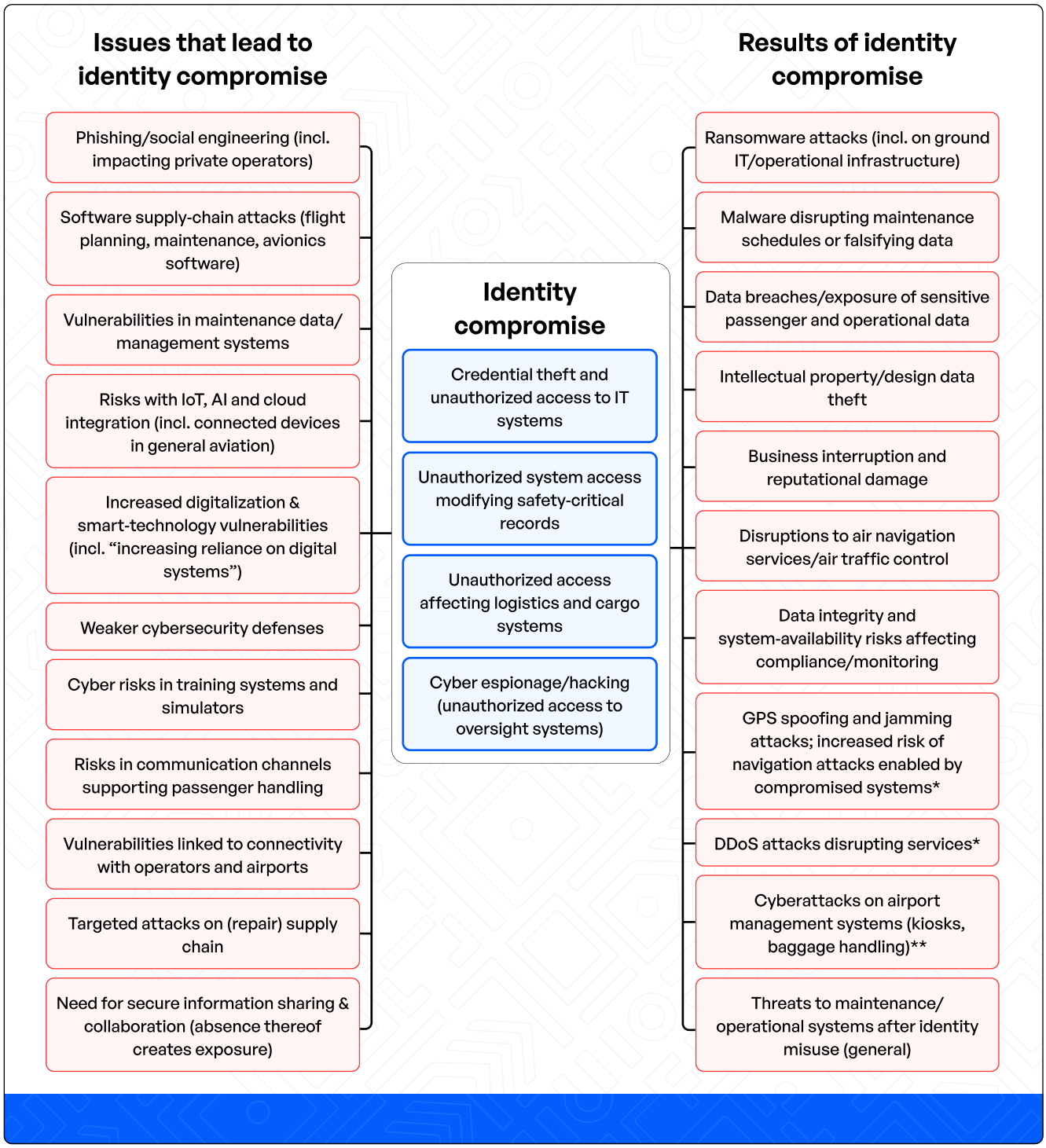
Maintenance, Repair, and Overhaul (MRO)	Compromised maintenance management systems; malware disrupting or falsifying maintenance data; unauthorized access altering safety records; supply-chain attacks on repair parts.
Ancillary and support services	Phishing/ransomware on ground IT; compromised training/simulator platforms; unauthorized access to logistics/cargo systems; insecure communication channels for passenger handling.
Regulatory and administrative bodies	Data breaches of sensitive records; cyber espionage/hacking of oversight systems; lack of secure inter-agency information sharing.
Economic and environmental agencies	Data integrity/system availability risks affecting compliance monitoring; interconnectivity vulnerabilities with operators/airports.
Private flying and general aviation	Weak/fragmented defenses; unauthorized avionics access & GPS spoofing; phishing/social engineering of clubs/operators; insecure IoT/connected devices.
Global Distribution System	Credential theft, data breaches, ransomware (systems interruption could generate full disruption of the ecosystem)

Points to Note

- The most prevalent and severe threats across all sectors include credential theft, ransomware, malware, DDoS attacks, GPS spoofing, and supply chain attacks.
- Increasing digital transformation, AI integration, cloud adoption, and IoT connectivity amplify vulnerability and attack surfaces.
- Regulatory and economic bodies face significant cyber risks given their crucial role in security and compliance.
- Specialized and less centralized segments like general aviation have distinct challenges due to fragmented cybersecurity approaches.
- The adoption of zero-trust security models and AI-based threat detection are emerging critical defenses industry-wide.

Classification of incidents based on identity security perspective

The following table presents a taxonomy of cyber incidents through an identity security lens, categorizing threats by their origin, vector, and operational impact across the aviation ecosystem. It highlights how identity-related vulnerabilities propagate through interconnected systems, from human access misuse to non-human identity exploitation.



Rising concern: Third-party risks

Civil aviation organizations are increasingly integrating external vendors and SaaS platforms into core operations — from passenger service systems and customer support to flight planning, logistics, and maintenance. This shift to the public cloud, along with automated file exchanges between alliance members and frequent flyers, as well as GDS PNR updates, enhances operational efficiency but also creates identity blind spots, where oversight and security for external identities are significantly reduced.

Root cause and breach vector

Airlines, airports, and MROs frequently interact with:

- Passenger service platforms (e.g., GDS, CRMs, reservations)
- Customer support portals (Zendesk, other SaaS helpdesks)
- Operational logistics (flight/crew scheduling, supply chain)
- Maintenance/engineering systems (technical data, analytics)

Integrations create entry points for attack via delegated credentials, API tokens, or service accounts, many outside centralized enterprise IAM.

Case in point: Salesforce-related credential compromise (2025)

Incident overview:
Several large enterprises experienced data breaches after attackers obtained valid Salesforce credentials through phishing, credential stuffing, or other account takeover techniques. These compromised accounts allowed unauthorized access to sensitive customer records, business data, and integrated applications connected via Salesforce's API ecosystem.

Third-party integration impact:
The nature of Salesforce as a cloud CRM means extensive connections to downstream platforms, including marketing tools, support portals, and analytics vendors, amplified the blast radius of the attack. Once inside Salesforce, attackers leveraged integrations to move laterally or access data held by external partners. It shows how one compromised identity can expose complex partner chains.

Recurring identity risk patterns

- Over-privileged accounts: Vendor/service GDS accounts often accumulate excessive privileges, especially if not reviewed regularly.
- Machine identity and token sprawl: API keys and non-human accounts are rarely rotated or fully inventoried, giving attackers persistence.
- Inconsistent governance: Third-party vendors may use separate identity stacks, leading to broken audit chains and lack of visibility.
- Vendor lifecycle management issues: GDS user accounts can remain active after contract changes or offboarding, leaving residual access to critical systems despite improvements in access review practices.
- Operational disruption: Identity compromise at external service providers may cause outages in passenger communications, check-in systems, or baggage handling, leading to financial loss and reputational damage.

- Regulatory and compliance risks: Data leakage by third-party platforms can trigger mandatory breach disclosures, legal penalties, and additional scrutiny under regulations such as GDPR, CCPA, and aviation-specific mandates.
- Strategic and financial consequences: Public breaches involving vendor platforms erode customer trust, causing loss of bookings and long-term attrition.

Identity-centric solutions for third-party risks

Issue	Control approach	Description
Over-privileged vendor/ SaaS accounts	Cloud Infrastructure Entitlement Management (CIEM)	Enforces least privilege for service accounts and periodically reviews entitlements
Compromised API tokens, secrets, and service accounts	Secrets Management + Machine Identity Governance	Inventories and governs all non-human identities, automates rotation and detection, and integrates with CIEM where available.
Credential/ session hijacking via third-party platforms	Identity Threat Detection & Response (ITDR)	Monitors for identity anomalies; remediation for aviation is usually manual due to legacy integration and complexity; do not claim universal automated rollback.
Weak vendor governance	Federated identity + vendor risk management	Monitors for identity anomalies; remediation for aviation is usually manual due to legacy integration and complexity; do not claim universal automated rollback.
Vendor offboarding gaps	Automated deprovisioning	Increasing adoption of integrated deprovisioning aligned with offboarding workflows.

Best practices for aviation third-party identity defense

- Inventory all vendor/service identities and machine accounts using centralized tools.
- Review privileges and entitlements regularly, targeting both human and non-human accounts.
- Automate credential rotation and secrets management where possible.
- Integrate vendor risk with federated identity governance for improved insight and control.
- Audit and monitor all external access, correlating identity activity (ITDR) and escalating irregularities for investigation.

Apt solutions for identity security-related issues

The preceding sections established how identity-centered attack paths emerge across aviation and classified them into three stages: precursors, active compromise, and downstream impact. Part 5 turns that analysis into action by mapping each issue to concrete identity-security capabilities so stakeholders can reduce risk with measurable speed and precision.

These solutions draw on unified controls - ITDR, ISPM, and Non-Human Identity (NHI) Management - to collapse detection and response time, enforce least-privilege continuously, and neutralize both human and machine identity abuse before operational damage escalates.

Issues that lead to identity compromise

Pre-compromise conditions - phishing, vulnerable systems, uncontrolled IoT/AI integrations, and weak governance - open the door to future misuse. In the table below, each of these vectors is paired with the preventive control that shrinks the attack surface, from least-privilege enforcement to real-time discovery of risky machine identities.

Compromise	How to address it
Phishing/social engineering	ITDR “spots and stops stolen or abused credentials,” enabling rapid quarantine after a phished login.
Aircraft and equipment manufacturing (AEM)	ISPM enforces least privilege and prevents privilege drift, limiting blast radius if an application vulnerability is exploited.
Risks with IoT, AI, and cloud integration (incl. connected devices)	NHI Management auto-discovers and governs machine/service identities (API keys, containers, bots) so their misuse via integrated cloud/AI/IoT systems is quickly contained.
Increased digitalization and smart-technology vulnerabilities	Unified pre-breach (live graph, anomaly flags) and inflight ITDR reduce the identity attack surface created by broader digitalization.
Weaker cybersecurity defenses	Platform adds a real-time layer (ITDR + ISPM + NHI) above existing IAM stack to close gaps in “weak” or incomplete defenses.

Identity compromise issues

Once an attacker has obtained or is abusing credentials, speed is decisive. Here are the most common active compromise scenarios. The table shows how rapid ITDR, anomaly detection, and one-click quarantine/rollback keep the mean time to detect and respond to around five minutes, cutting dwell time and lateral movement.

Compromise	How to address it
Credential theft and unauthorized access to IT systems	ITDR spots and stops stolen or abused credentials, enabling rapid quarantine after a phished login.
Unauthorized system access modifying safety-critical records	Real-time anomaly flags and rapid ITDR (pattern-matching to MITRE, rollback) identify and reverse unauthorized policy or record changes.
Unauthorized access affecting logistics and cargo systems	NHI Management auto-discovers and governs machine/service identities (API keys, containers, bots) so their misuse via integrated cloud/AI/IoT systems is quickly contained.
Cyber espionage/hacking (unauthorized access to oversight systems)	5-minute MTTD/MTTR via agentless ITDR limits dwell time for lateral movement/espionage.

Issues after identity compromise

Management has a hard time dealing with the post-compromise impacts: ransomware, data exfiltration, integrity loss, and so on. Here, we list the controls that contain and remediate them. By combining rollback, continuous least-privilege, audit-ready reporting, and unified monitoring, these measures reduce operational downtime and regulatory exposure following identity abuse.

Compromise	How to address it
Ransomware attacks (incl. on operational/ground IT)	Early detection of compromised credentials and rapid quarantine reduces the opportunity for ransomware deployment.
Malware disrupting maintenance schedules or falsifying data	Least-privilege (ISPM) and ITDR rollback remove excess rights and undo malicious identity-driven changes quickly.
Data breaches/exposure of sensitive passenger and operational data	The unified layer drives MTTD/MTTR to 5 minutes, stopping in-flight data exfiltration via compromised identities.

Intellectual property/ design data theft	Real-time anomaly flags and one-click quarantine restrict lateral movement to sensitive repositories.
Business interruption and reputational damage	Faster detection/response (“5-minute” benchmark) shrinks the incident impact window, limiting downtime
Data integrity and system-availability risks affecting compliance/monitoring	Audit-Proof IAM rightsizes access and provides audit-ready proof, reducing integrity/availability risks from over-privileged identities.
Threats to maintenance/ operational systems after identity misuse (general)	Pre-breach ISPM + in-flight ITDR provide continuous monitoring and remediation of abused identities before operational damage escalates.