THE NATIONAL AVIATION CONFERENCE 2026

Status of Aviation Cybersecurity in South Africa:

Harnessing Technology and Resilience of the South African Skies

6-7 MAY 2026 | EMPEROR'S PALACE

SACAA
SOUTH AFRICAN CIVIL AVIATION AUTHORITY
Keeping you safe in the sky

top EMPLOYER South Africa 2026
FOR A BETTER WORLD OF WORK

Presented by:
Aviation Security Risk Management Specialist
Given SHINGANGE

THE AVIATION CYBERSECURITY LANDSCAPE

DEFINITION

The conditions shaping cyber risk across civil aviation at any given time, encompassing the threat actors targeting aviation systems, the vulnerabilities introduced by aviation's increasing dependence on networked and software-defined technologies, and the regulatory standards and oversight frameworks governing how states and operators are expected to manage that risk.

WHO

State-sponsored actors, organised ransomware groups, hacktivists, and insider threats, all with demonstrated aviation sector interest

WHAT

Networked avionics, air traffic management systems, airport IT, passenger processing platforms, and increasingly, software supply chains

HOW

Regulations, standards, oversight frameworks, incident reporting, and the capacity to audit and enforce compliance across a complex ecosystem

2019: When the Framework Was Built

When ICAO endorsed its Aviation Cybersecurity Strategy in 2019 and published the first Cybersecurity Action Plan in 2020, the threat environment looked broadly like this:

Opportunistic criminal actors

Largely reactive, financially motivated threat groups without consistent sector focus

Isolated ransomware incidents

Individual organisations targeted; limited aviation-specific operational impact

Phishing targeting aviation staff

Credential theft campaigns; primarily IT-layer risk, not safety-critical systems

Emerging GPS interference concern

Documented but still viewed as edge risk; not yet at IATA's scale of 430,000 incidents per year

Three Things Changed Simultaneously

01

FREQUENCY

430,000

GPS spoofing incidents in 2024 (IATA)

6,320 cyber events against aviation identified by EUROCONTROL EATM-CERT. Attacks on aviation up 131% between 2022 and 2023.

02

NATURE

600%

increase in aviation attacks 2024–2025 (Thales)

Shift from opportunistic criminals to persistent ransomware groups, state-sponsored interference, and deliberate supply chain targeting.

03

CAPABILITY

72 min

from intrusion to data theft in 2025

AI has reduced the expertise threshold and expanded attack scale. Down from 285 minutes in 2024. Attribution harder than ever.

Incidents That Define This Moment

JUL 2024 — THIRD-PARTY DEPENDENCY

CrowdStrike Global Outage

A faulty software update from a trusted cybersecurity vendor caused a global IT outage. One airline cancelled over 7,000 flights. The threat was a trusted supplier, not a hostile actor.

SEP 2025 — SUPPLY CHAIN

Collins Aerospace Ransomware

Ransomware hit Collins Aerospace's MUSE passenger processing platform. Heathrow, Brussels, and Berlin disrupted simultaneously. 217 flights cancelled. One vendor, one attack, three countries.

NOV 2025 — GNSS INTERFERENCE

Delhi GPS Spoofing

800+ flight operations disrupted at India's busiest airport. Nav Integrity Category dropped to zero. Most likely military electronic warfare spillover from the Middle East — aviation as collateral damage.

Q1 2026 — PERSISTENT THREAT

EATM-CERT Assessment

Ransomware against aviation described as stable at an elevated baseline. Groups Qilin, Play, INC Ransom and TheGentlemen recurring. Supply chain underweighted in most risk models.

Closer to Home

SA Weather Service · 2025

RansomHub ransomware attack on 26 January 2025, the second attempt in two days after an initial failed attempt on 25 January. Systems went down, disrupting aviation and marine forecast services.

Polmed · 2026

Ransom demand received directly from the attackers on 25 March 2026. The threat actor is ShinyHunters. Compromised data included health records, financial data, home addresses, occupational designations and SAPS employee numbers.

South African Airways · 2025

Website, mobile app, and internal operational systems disrupted. Restored same day. Reported to SSA, SAPS, and the Information Regulator under POPIA.

Standard Bank & Liberty · 2026

1.2TB exfiltrated over three weeks. Attacker traversed SharePoint, OneDrive, Oracle SQL and multiple platforms undetected before disclosure.

Stats SA · 2025

HR database breached by XP95. Ransom demanded. Government data compromised.

National Health Laboratory Service (NHLS) — 2024

NHLS was attacked by ransomware. The cyberattack rendered the NHLS website inaccessible, halting laboratory systems, document access, and electronic sample testing, disrupting critical health services.

Closer to Home

MTN Group — 2025

In April 2025, MTN Group disclosed a data breach affecting its South African subscribers. The breach escalated into a criminal investigation. MTN is one of Africa's largest telecoms operators and the breach affected multiple countries.

Department of Justice — September 2021

Ransomware encrypted all departmental systems on 6 September 2021. Email, bail services, letters of authority, and the website went down for several weeks. Child maintenance payments disrupted. No attacker named.

CIPC — March 2024

Security breach exposed personal information of employees and clients of the entity responsible for company and intellectual property registrations. No attacker named publicly.

TransUnion — 2022

Attacker N4ughtysecTU gained access using a compromised client credential with the password "password." At least 3 million South Africans' ID numbers, contact details, vehicle finance data and credit scores exposed. $15 million ransom demanded. TransUnion refused to pay.

Transnet — July 2021

Ransomware brought South Africa's state port and freight operator to a standstill. Durban, Cape Town and other ports declared force majeure, halting exports and imports. One of the most operationally significant attacks on South African critical infrastructure to date.

The Gap

The problem is not the quality of the framework. The problem is the speed at which the threat environment has moved.

Amendment cycles assume stability

ICAO amendment cycles, national regulatory development, and audit frameworks were designed for a threat environment that changes incrementally. That assumption no longer holds.

Incidents outpace frameworks

CrowdStrike was not anticipated in any regulatory framework. Collins Aerospace exposed supply chain risk that audit checklists are not designed to detect. Delhi showed that full regulatory compliance does not prevent disruption from military activity thousands of kilometres away.

Indicators expire — actor behaviour persists

EATM-CERT Q1 2026: the sector's defensive posture concentrates heavily on indicators of compromise. Indicators expire. Actor behaviour persists. The regulatory equivalent is a framework that responds to last year's incidents.

Domestic Progress

Regulatory Alignment

Proposed aviation cybersecurity regulations developed and aligned with ICAO's Cybersecurity Action Plan. CARCom approval obtained. Regulations are awaiting the Minister's signature before formal gazetting.

CSIRT Engagement Initiated

December 2024: SACAA Aviation Security Division convened a formal engagement with DCDT Cybersecurity Hub and CSIR Cybersecurity Research Group to initiate a sector-specific CSIRT for civil aviation.

Incident Reporting Demonstrated

SAA's May 2025 incident demonstrated that when an attack occurs, disaster management protocols activate and mandatory reporting to relevant department and agencies happens.

International Engagement

Active engagement with ICAO on cybersecurity capacity development, alignment with the ICAO Cybersecurity Action Plan pillars, and participation in ICAO Cybersecurity Panel and Working Groups.

South African Regulatory Framework

Outgoing Cybersecurity Regulations:

(1) A/An _____ shall identify critical information and communication technology systems and data used for aviation purposes in accordance with risk assessment, develop and implement the following measures, to prevent unlawful interference and protect the confidentiality, integrity and availability of identified critical systems—

(a) security by design;
(b) supply chain security;
(c) network separation; and
(d) protection and limitation of any remote access capabilities.

(2) A/An _____ shall develop procedures for—

(a) testing of cyber-security;
(b) cyber-security response;
(c) cyber-security incident analysis; and
(d) cyber-security incident reporting.

(3) A/An _____ shall report any cyber-security incident to the Director within 48 hours of occurrence.

South African Regulatory Framework

Incoming Cybersecurity Regulations:

(1) A/An _____ shall –

(a) identify and secure its critical information and communication technology systems and data used for aviation purposes to ensure cybersecurity, privacy and resilience as prescribed in Document SA-CATS 000;

(b) ensure that its cybersecurity measures are in accordance with a risk assessment and threat levels;

(c) implement cybersecurity measures as prescribed in Document SA-CATS 111; and

(2) report cybersecurity incidents as prescribed in Document SA-CATS 111 to the Director within 48 hours of becoming aware of an incident

Honest Challenges

01 Designated Officials Without Cyber Qualifications

Most designated aviation security officials are not qualified cybersecurity practitioners. This creates a structural gap between oversight responsibility and technical capacity to assess, audit, and enforce cybersecurity compliance.

02 ICT Departments Outside the Regulated Space

Most aviation entities have their IT/ICT departments sitting outside the civil aviation regulated space and not accountable to designated officials or aviation regulations. This limits the ability to enforce compliance at the system level.

03 Extraterritorial ICT Operations

Several entities have their ICT offices located in other countries, operating under those countries' regulations. When compliance is requested, entities produce foreign regulations rather than South African ones, creating accountability gaps that existing frameworks do not resolve.

04 Operational Technology Oversight

Current audit frameworks were built for physical security threats. They cannot assess whether flight management systems, dispatch platforms, or crew management infrastructure are adequately secured against sophisticated intrusion.

Three Directions

Continuous, Threat-Informed Oversight

Regulators need to move from periodic compliance audits toward dynamic risk assessment informed by real-time threat intelligence. The audit cycle assumes the threat picture is stable between reviews. It is not.

AI Capability Has Changed the Calculus

Anthropic's Project Glasswing (April 2026) demonstrated that AI can now autonomously identify and chain together previously unknown vulnerabilities across major operating systems. If available to defenders, it is available to adversaries. The regulatory implication is immediate.

Information Sharing as a Core Function

EATM-CERT Q1 2026: tracking known actors at the Technics, Tactics and Procedures (TTP) level provides more durable value than indicator-based approaches. South Africa's participation in international aviation cybersecurity information-sharing arrangements is not optional. It is foundational.

Conclusion

The challenges we have discussed today are not uniquely South African. Every civil aviation authority in the world is grappling with a threat environment that moves faster than the regulatory cycle. Developed country regulators face the same questions about supply chain visibility, operational technology oversight, and the limits of periodic compliance audits. No state has fully solved this.

The work is not finished. The threat will not slow down to give us time. But South Africa is in this conversation, contributing to it, and building the capacity to stay ahead of it. That is where we intend to remain.

Text

THANK YOU

THE NATIONAL AVIATION CONFERENCE 2026

Presented by:
Aviation Security Risk Management Specialist
Given SHINGANGE