

IATA CYBERSECURITY SUMMIT

Geneva, Switzerland
28-29 October 2026

PROGRAM



IATA CYBERSECURITY SUMMIT

Wednesday, 28 October 2026

08h00 – 09h00	EVENT REGISTRATION & WELCOME COFFEE
09h00 – 09h10	Welcome & Introduction ▪ Ewa Pilat, Chief Information Security Officer, IATA
09h10 – 09h25	Keynote Address
09h25 – 09h40	2027 Aviation Cyber Threat Outlook As aviation continues to embrace digital transformation, the cyber threat landscape is evolving at an unprecedented pace. This session examines the key cybersecurity trends, emerging threats, and adversary tactics expected to shape the aviation sector in 2027. Drawing on current intelligence, industry developments, and evolving attack patterns, the discussion will explore risks ranging from AI-enabled attacks and identity compromise to supply chain threats, operational technology targeting, and cyber-safety concerns. Attendees will gain a forward-looking perspective on the trends, challenges, and threat actors likely to influence the aviation cybersecurity landscape in the years ahead.
09h40 – 10h05	Session Placeholder
10h05 – 10h30	Cybersecurity Best Practices for Electronic Flight Bags (EFBs) Electronic Flight Bags (EFBs) have become mission-critical tools that support modern flight operations, making their security essential to both operational continuity and flight safety. This keynote examines the evolving cyber threats facing EFB environments, including device compromise, credential theft, supply chain risks, insider threats, and insecure network connectivity. Drawing on operational experience and regulatory implementation, the session will present practical security controls, deployment strategies, and governance approaches that help airlines protect EFB ecosystems while balancing usability, regulatory compliance, and operational resilience. ▪ Christos Ringas, Chief Information Security Officer (CISO), Blue Bird Airways S.A.
10h30 – 11h00	NETWORKING BREAK
11h00 – 11h25	Social Engineering the Flight Deck: Targeting the Captain's Judgement, Not the Aircraft As GNSS interference and electronic warfare activity continue to increase, aviation faces a new category of cyber-safety risk that extends beyond traditional technology disruption. This keynote examines how adversaries can manipulate signals, information, and uncertainty to influence flight crew decision-making, turning ambiguity itself into a weapon. Through the lens of hybrid warfare and real-world interference scenarios, the session explores emerging threats targeting the human element of aviation operations and discusses how technology, procedures, and training can strengthen resilience against attacks aimed not at the aircraft, but at the captain's judgement. ▪ Serge Christiaans, CISO & Airline Captain, Aviation Cyber Academy

IATA CYBERSECURITY SUMMIT

Wednesday, 28 October 2026

11h25 – 12h05

Connected Skies, Shared Risk: Who Owns Aviation's Expanding Attack Surface?

As aviation becomes increasingly connected through digital platforms, cloud services, operational technologies, airports, and aircraft systems, the boundaries of responsibility for cybersecurity continue to blur. How can organizations effectively manage risk across an ecosystem where critical services are shared among numerous stakeholders? This panel explores emerging attack vectors, shared responsibility models, and the collaborative approaches needed to strengthen cybersecurity across the aviation value chain.

Moderated by **Adam Battams**, Cyber Security Consultant, SecureTeam Ltd.

12h05 – 12h30

No Airline Flies Alone: The Case for Collective Cyber Defense in Aviation

Aviation operates within a highly interconnected ecosystem where passenger data, operational systems, and digital services extend far beyond the boundaries of any single organization. This session examines the challenges of investigating and responding to threats that originate outside an organization's direct visibility and explores why traditional security approaches alone are no longer sufficient. Drawing on a real-world investigation into an industry-wide passenger data exposure claim, the presentation highlights the critical role of intelligence sharing, industry collaboration, and collective defense in improving detection, response, and resilience across aviation.

12h30 – 14h00

LUNCH BREAK

14h00 – 14h25

When the Attacker Becomes an Agent: Offensive AI and the Future of Aviation Cybersecurity

Artificial intelligence is rapidly transforming offensive cybersecurity, enabling AI agents to perform tasks previously requiring significant human effort, including reconnaissance, vulnerability discovery, attack-path analysis, and lateral movement. Drawing on hands-on experimentation, this keynote examines what offensive AI agents can realistically do today, their limitations, and how they may change the economics of cyberattacks. Focusing on the broader aviation ecosystem, the session explores how increasingly capable AI agents may reshape the threat landscape and future attack chains. Attendees will gain practical insights into what this evolution means for defenders preparing for an environment where attackers increasingly delegate tasks to autonomous systems.

- **Georg Ph. E. Heise**, Head Business Dev., Research & Innovation, Lufthansa Group
- **Christian Pappas**, Expert Offensive Security Consultants, Lufthansa Group

14h25 – 15h05

AI at 35,000 Feet: How Much Control Should We Give Algorithms?

Artificial intelligence is transforming aviation through applications ranging from predictive maintenance and operational planning to customer service and security operations. As organizations become increasingly reliant on AI-driven systems, important questions emerge around trust, governance, accountability, and human oversight. This panel explores where AI can safely support decision-making, where human intervention remains essential, and how organizations can balance innovation with security, safety, and operational resilience.

IATA CYBERSECURITY SUMMIT

Wednesday, 28 October 2026

15h05 – 15h30

Humans Are Too Slow: Defending Aviation in the Era of Agentic AI

As Agentic AI enables adversaries to operate at unprecedented speed, scale, and autonomy, aviation organizations must rethink cyber risk and resilience. This session examines the growing gap between machine-speed attacks and security processes designed for human-paced decision-making. Attendees will explore how organizations can adapt security and operational processes, strengthen foundational controls, and leverage AI defensively while governing it as a critical business asset. The session offers a strategic perspective on building resilient aviation organizations capable of defending critical operations at the speed of AI.

- **Melania Haro**, Partner, Deloitte

15h30 – 16h00

NETWORKING BREAK

16h00 – 17h00

The Weakest Link: Managing Aviation's Supply Chain Cyber Risk

Supply chain cyber risk remains one of aviation's most complex challenges, with vulnerabilities and disruptions potentially cascading across organizations and operations. This interactive roundtable invites participants to share experiences and perspectives on managing third-party risk, securing software supply chains, identifying critical dependencies, and addressing attacks targeting trusted relationships. Through facilitated discussion and peer exchange, attendees will explore common challenges, lessons learned, and practical approaches to strengthening supply chain cyber resilience across the industry.

17h00 – 17h25

Beyond Third-Party Risk: Building Cyber Resilience Across the Aviation Supply Chain

Modern aviation depends on a highly interconnected network of suppliers and service providers, making cybersecurity a shared challenge across the ecosystem. This session explores how aviation organizations can move beyond traditional third-party risk management toward a more resilient, risk-based approach to supply chain security. Attendees will gain practical insights into identifying critical dependencies, prioritizing supplier risks based on operational impact, and strengthening collaboration, assurance, and continuity across the aviation supply chain.

- **Jochen Wargulski**, Head of IT-Security & Privacy Consulting, Lufthansa Industry Solutions AS GmbH

17h25 – 17h30

Cybersecurity Summit Day 1 Wrap-Up

17h30 – 19h30

NETWORKING RECEPTION

IATA CYBERSECURITY SUMMIT

Thursday, 29 October 2026

08h00 – 09h00

EVENT REGISTRATION & WELCOME COFFEE

09h00 – 09h25

EASA Part-IS: From Regulatory Compliance to Operational Resilience

As aviation organizations continue implementing EASA Part-IS, attention is increasingly shifting from understanding regulatory requirements to embedding information security into day-to-day aviation operations. This keynote will provide a regulatory perspective on the implementation of Part-IS, highlighting key considerations, challenges, and observations emerging across the aviation sector. The session will also explore how Part-IS fits within the broader cybersecurity regulatory landscape and how a risk-based approach can support not only regulatory compliance, but also stronger cybersecurity and operational resilience.

- **Angeliki Karakoliou**, Expert - Cybersecurity in Aviation, EASA

09h25 – 10h05

Global Cybersecurity Regulation in Motion: Trends, Priorities and Effective Industry Advocacy

As cybersecurity regulation continues to evolve across jurisdictions, aviation organizations face an increasingly complex landscape of requirements related to resilience, incident reporting, supply chain security, operational technology, and risk management. This panel brings together aviation cybersecurity and regulatory leaders from multiple regions to examine emerging regulatory trends, areas of convergence and fragmentation, and lessons learned from implementation efforts around the world. Panelists will discuss practical strategies for engaging with policymakers, promoting risk-based and harmonized approaches, reducing unnecessary compliance burdens, and helping shape regulations that strengthen both cybersecurity and operational resilience.

Moderated by **Adam Smith**, Executive Cybersecurity Advisor, Southwest Airlines

10h05 – 10h30

Aviation ATT&CK: Matrix for Cyber and Safety Risks

As aviation becomes increasingly connected, cyber threats can have growing operational and safety implications. This session introduces AV-ATT&CK, a framework for mapping and categorizing cyber-safety risks across the aviation ecosystem. Attendees will explore emerging threats, including AI-enabled attacks and geopolitical risks, and how individual techniques can form realistic attack chains affecting operations, critical information, and safety. The session will also present the framework's methodology and practical aviation scenarios to help organizations better understand and prepare for the evolving threat landscape.

- **Shaya Feedman**, Cyber Security Expert, CYVIATION

10h30 – 11h00

NETWORKING BREAK

IATA CYBERSECURITY SUMMIT

Thursday, 29 October 2026

11h00 – 11h25

Quantum-Safe Aviation: A Risk-Based Roadmap for Cryptographic Discovery, Prioritization and Migration

Quantum computing presents a growing cybersecurity challenge, requiring aviation organizations to prepare well before cryptographically relevant quantum computers become a reality. This keynote explores a practical, risk-based approach to identifying cryptographic dependencies, prioritizing risks, and planning migration to quantum-safe security. Attendees will gain insights into strengthening crypto-agility, protecting long-lived sensitive data, engaging suppliers, and developing a phased roadmap toward post-quantum cryptography and long-term resilience.

- **Yunus Emre Sert**, Application Security Engineer, Turkish Technology

11h25 – 12h05

When Digital Meets Physical: Securing the Convergence of IT, OT and AI

The convergence of enterprise IT, operational technology, and AI-enabled systems is creating new opportunities for efficiency and innovation across aviation. At the same time, this convergence introduces complex security challenges that can directly impact operational safety and service delivery. This panel examines how organizations can manage interconnected environments, reduce cyber risk, and implement effective governance as digital and physical systems become increasingly integrated.

12h05 – 12h30

SKOP (Swiss Knife of the Pentester): End-to-End Penetration Testing with Human-Gated AI Agents

Artificial intelligence is changing penetration testing by enabling greater automation while maintaining human oversight and control. This keynote presents SKOP, an AI-driven framework developed and deployed by Turkish Airlines across booking, cargo, and airport systems. Drawing on more than thirty real-world engagements, the session explores how AI agents can support reconnaissance, testing, verification, and reporting within a human-gated governance model. Attendees will gain practical insights into the benefits, limitations, and safeguards of integrating AI agents into offensive security activities in aviation environments.

- **Muhammed Bilal Kan**, Senior Penetration Tester, Turkish Airlines

12h30 – 14h00

LUNCH BREAK

14h00 – 14h25

Session Placeholder

14h25 – 15h05

From Detection to Recovery: Building Aviation-Specific SOC Capabilities

Security Operations Centers are evolving beyond traditional monitoring and alert management to become critical enablers of resilience. Aviation organizations face unique challenges in protecting highly interconnected environments while maintaining uninterrupted operations. This session explores how modern aviation SOC's can integrate threat intelligence, automation, incident response, and recovery planning to improve both security outcomes and operational resilience in a rapidly changing threat landscape.

IATA CYBERSECURITY SUMMIT

Thursday, 29 October 2026

15h05 – 15h30

Ready for Recovery: Validating Cyber Resilience in Aviation Operations

Recovery plans often rely on assumptions that backups, procedures, and teams will perform as expected during a major cyber incident. This session explores how a production-validated digital twin can continuously verify recovery capabilities in operational technology environments. Using an airport baggage handling system as an example, attendees will learn how organizations can rebuild systems from backups, test realistic failure scenarios, and validate operational readiness. The session demonstrates how recovery can become a measurable, repeatable capability that strengthens resilience against ransomware and other disruptive cyber incidents.

- **Michal Kotyza**, Chief Information Security Officer, Dimark S.A.

15h30 – 16h00

NETWORKING BREAK

16h00 – 16h25

Beyond Intelligence Sharing: Building Aviation Cyber Resilience Through Community Action

As cyber threats continue to evolve across an increasingly interconnected aviation ecosystem, effective defense depends on more than technology alone. This keynote explores how trusted communities enable organizations to transform isolated observations into actionable intelligence, shared expertise, and coordinated defense. Drawing on insights from Aviation ISAC and industry collaboration initiatives such as ASCENT, the session will examine emerging cyber threats, lessons learned from community-driven intelligence sharing, and practical approaches to strengthening resilience across airlines, airports, manufacturers, and the broader aviation supply chain.

- **David Nieto**, VP Member Success, Aviation ISAC

16h25 – 16h50

Measuring What Matters: Reframing Cyber Success as Operational Resilience

Traditional cybersecurity metrics often focus on activities such as patching vulnerabilities, detecting threats, and improving maturity scores. In aviation, however, the true measure of success is the ability to continue operating safely and effectively during a cyber incident. Drawing on lessons learned from one of North America's largest airports, this keynote explores how organizations can shift from measuring cyber activities to measuring operational resilience. Attendees will gain practical insights into linking cybersecurity capabilities, crisis response, resilience testing, and third-party dependencies to the protection of critical aviation operations.

- **Ernest Eustace**, Head of Cyber Defense and Operations (Deputy CISO), Greater Toronto Airports Authority

16h50 – 17h15

Session Placeholder

17h15 – 17h30

IATA Announcements and Closing Remarks: Looking Ahead to 2027 and Beyond

- **Ewa Pilat**, Chief Information Security Officer, IATA

17h30

Adjourn