PTE WORLD

CONFERENCE

March 17-19, 2026

Excel London

Reinventing airport security: From control to intelligence

Conference report: **Security**

www.pte-world.com

Table of contents

Executive summary: Rethinking the foundations of airport security

Airport security has spent two decades building robust compliance frameworks, with high compliance scores and consistent audit performance. Recent experience has also tested the limits of those frameworks. When Seattle-Tacoma International Airport experienced one of the most significant ransomware incidents recorded at an airport, full recovery extended across 18 months. When Heathrow identified a cyber exposure originating with a third-party supplier outside its direct contractual chain, existing information-sharing frameworks were stretched. And when a Haneda checkpoint redesign surfaced high turnover among security staff, the industry began examining how its own processes affect workforce wellbeing alongside external threats.

What emerged from the Security talks at PTE World Conference 2026 was a clear signal of an industry at a turning point. Several discussions pointed to the same structural opportunity: the aviation industry has built a security apparatus shaped by past threat patterns, governed by regulations developed in earlier eras, and supported by a workforce facing growing pressures that merit renewed attention.

The sessions revealed an industry at an inflection point. The threats have evolved – hybrid, cyber-physical, supply-chain-mediated, insider-enabled. The technology has evolved – CT scanners, biometric corridors, AI-driven surveillance. But the institutional architecture connecting them has not. The result is a security ecosystem that is simultaneously more capable and more fragile than at any point in its history.

This report argues that the path forward lies less in process for its own sake and more in security intelligence: the ability to see threats before they materialise, share information before it expires, design checkpoints for humans rather than against them, and treat inclusion as a performance requirement rather than a regulatory afterthought.

Seven key findings

1. **Compliance and assurance are distinct.** The SeMS panels highlighted that point-in-time compliance, on its own, offers limited insight into ongoing security posture. Airports that pass periodic audits but lack continuous assurance mechanisms may have an incomplete view of outcomes between assessments.

2. **Cyber recovery can extend across years, not weeks.** Seattle's 18-month restoration timeline, even as core operations resumed within roughly six weeks, illustrates the difference between restored visible operations and full system resilience.

3. **Information sharing faces structural constraints.** GDPR considerations, reputational sensitivities, and investigation confidentiality can limit the collaboration that speakers identified as the most important capability to strengthen.

4. **The checkpoint has been re-equipped, and redesign is the next step.** CT scanners are delivering 45-50% throughput gains, but the lanes, training models, and operational concepts around them were designed for 2D X-ray behaviour.

5. **Hybrid threats are an emerging priority for aviation.** Pharmaceuticals and finance are further developed on insider threat detection, offering models aviation can learn from. GPS jamming is a daily occurrence in northern Norway. Drone incursions have disrupted multiple European airports in 2025.

6. **One-stop security works but cannot scale.** The UK-US agreement saves passengers 45 minutes per connection, but the infrastructure incompatibilities at most hub airports make expansion a years-long engineering problem.

7. **Workforce retention is an industry-wide priority.** The high turnover observed during a Haneda checkpoint proof-of-concept points to broader workforce dynamics that technology alone cannot address.

1. **Compliance scores** and the limits of tick-box assurance

The UK Civil Aviation Authority's Peter Drissell opened the Security track with a perspective that resonated with airport security leaders in the room:

"Compliance doesn't mean good security. It just means you've complied to the standard without any understanding of what you were required to do."

Peter Drissell, director aviation security, Civil Aviation Authority

This reflects a considered regulatory perspective. Since 2014, the regulator has comprehensively reshaped the UK's aviation security oversight – replacing 15 inherited inspectors with 130 new colleagues, transforming a workforce that was 95% male with approximately 4% ethnic minority representation into one that is 20% ethnic minority, and establishing a cybersecurity oversight regime that has existed for only six years.

The SeMS (Security Management Systems) panel reinforced the point with concrete detail. Edinburgh Airport processes 17 million passengers a year through 8 security lanes, operates a Phase 2B SeMS with a team of three, and achieves high compliance scores. As Edinburgh's head of security noted:

"I've never been asked by an airline if I have a SeMS – and I find that really disappointing. We have 43 airlines at Edinburgh, from all around the world, and nobody's ever asked."

Ian Gregory, security regulation and compliance manager, Edinburgh Airport

The distinction between compliance and assurance is significant. Compliance is a snapshot; assurance is a culture. Edinburgh invests approximately $150,000 annually in its SeMS against $15 million per month in security operations. The panel drew an explicit parallel with safety management. Aviation's safety culture is built on radical transparency – airlines share incident data immediately, without competitive hesitation. Cybersecurity has tended to operate differently, with greater emphasis on confidentiality, reputation management, and institutional caution.

"I wish cyber had learnt the same thing, because cyber operates in a completely different way."

Peter Drissell, director aviation security, Civil Aviation Authority

Australia's voluntary adoption of SeMS alongside its mandatory airport security programme offers a transitional model for markets that cannot yet mandate the framework. But the panel's consensus was clear: the transition from compliance to assurance is not optional. It is the difference between airports with continuous visibility into their security posture and those relying primarily on periodic checks.

Looking Ahead: The next frontier is airline accountability. No airline currently asks whether the airports it operates into have a functioning SeMS. When that question becomes routine – as IOSA audits are for airline safety – the compliance-assurance gap will narrow. Until then, high compliance scores are best read alongside continuous assurance measures.

2. Cyber recovery timelines: Lessons in resilience beyond initial restoration

In mid-August 2024, Seattle-Tacoma International Airport – the 12th largest in the United States, processing 53 million passengers annually – suffered what McCarthy Construction's Mark Crosby described as "the largest ransomware event at an airport in the world."

Core operations resumed within about six weeks, while full system restoration continued well beyond that point.

Stephanie Warren, Sea-Tac's assistant director of information security, gave a notably detailed account of the incident and its recovery. Full restoration took 18 months:

"22 months later, we still have applications not back up in production, that was still down from the event. 22 months."

Stephanie Warren, assistant director of information security, Port of Seattle

The incident surfaced vulnerabilities that routine compliance audits had not captured. Some IT systems were running mission-critical databases on file servers outside standard backup protections. Shared local credentials remained active for systems whose owners had left the organisation. Payroll was temporarily reduced from 300 coding options to 25 and managed manually on spreadsheets.

"What do you mean you were running a mission-critical database off a file server that's not backed up the same as a server?"

Stephanie Warren, assistant director of information security, Port of Seattle

Perhaps most troublingly, the forensic investigation revealed that other threat actors had been in the environment before the attack – "little stops and starts, nothing significant, nothing that raised a flag." The ransomware was not the first intrusion. It was the first one that was noticed.

The recovery itself generated its own lessons. Project managers – not IT staff – proved indispensable because they held undocumented tribal knowledge of system interdependencies. The union-managed aviation IT team and the corporate IT team, which had operated in structural separation, were forced into the same room for the first time. Risk communication that had previously disappeared "into the ether" through multiple management layers was rebuilt as a direct channel to executives.

Looking Ahead: Every airport should ask itself the question Sea-Tac was forced to answer: do you have a plan for total data centre loss? Not individual system recovery – total loss. If the answer is no, Seattle's 18-month timeline is your minimum exposure. The airports that invest in organisational continuity and resiliency portfolios as standing programmes will define the next standard.

3. Aligning regulation and collaboration in information sharing

Every session on Security surfaced the same structural challenge: the information that could help prevent the next attack is held in fragments across airports, airlines, police forces, governments, and regulators, and current rules can make assembling it difficult.

The cybersecurity collaboration panel made this concrete. When a cyber incident struck Collins Aerospace – a third-party supplier to Heathrow, Brussels, Dublin, and other European airports simultaneously – informal trust networks complemented the formal information-sharing mechanisms.

Paris Airports' Eric Vautier quantified the attack surface that makes collaboration essential: ADP operates with approximately 2,000 supplier companies. Heathrow has 2,000 partners. When a third-party supplier is compromised, the affected airports may have no contractual relationship with the breached entity.

The panel identified three structural blockers. First, regulatory disclosure requirements: the moment a cyber incident becomes a criminal investigation, formal information sharing is legally constrained at precisely the time intelligence is most needed. Second, reputational risk: press coverage incorrectly identified Heathrow as suffering a direct attack. Third, GDPR considerations.

The Traffic Light Protocol provides a functional framework, and the Aviation ISAC offers a community structure. But the most effective sharing happened outside these structures, through bilateral trust relationships built long before the crisis:

Looking Ahead: The industry needs a pre-competitive intelligence-sharing framework that operates outside the constraints of criminal investigations and reputational management. Aviation safety solved this decades ago – airlines share incident data immediately, transparently, and without competitive hesitation. Cybersecurity must follow the same path, or the information asymmetry between attackers (who collaborate freely) and defenders (who collaborate more cautiously) will continue to widen.

4. CT scanners and the case for redesigning the checkpoint

The technology question is largely settled. CT scanners are delivering measurable results. Heathrow is installing fewer lanes than its pre-CT configuration yet seeing a 45-50% increase in passenger flow. Rome's deployment detected 100 additional prohibited items per month above the pre-CT baseline while increasing throughput by 10%. CATSA is a third of the way through a national rollout across 20-30 Canadian airports.

The business case, however, remains incomplete. No airport has yet achieved a cost reduction from CT deployment. Staffing levels are the same or higher. Alarm rates at Gatwick went up after deploying new detection algorithms, not down. The real return on investment hinges on Automated Prohibited Item Detection Systems (APIDS) – technology that is certified but not yet widely deployed.

The deeper problem is that the checkpoint itself was designed for a different machine:

"CT is no longer the bottleneck. But how do I really create a checkpoint environment that facilitates the throughput the airport is looking for? There are 5 different gears in your car because you need them. Why are you always operating the checkpoint at the same pace?"

Gunther van Adrichem, executive director, Point FWD

Copenhagen's eight-year checkpoint transformation illustrates both the promise and the pain. Twenty new lanes, 550 staff to retrain, a COVID shutdown that wiped out the knowledge base, and a change-management challenges the project team openly acknowledged.

The CT scanner is not an updated X-ray machine. It is a data platform. The airports that treat it as such will extract value that goes far beyond prohibited item detection.

Looking Ahead: The next three to five years will see the checkpoint redesigned around the CT scanner, not the other way around. Dynamic ConOps – variable staffing models and operational "gears" that adjust throughout the day – are the near-term efficiency gain. APIDS is the inflection point that justifies the capital investment. And the eventual inversion of equipment economics, where data value exceeds hardware cost, will reshape the vendor-airport relationship entirely.

5. **Hybrid threats:** An emerging priority for aviation security

The evidence is accumulating, and industry response is developing in parallel. Drone-related disruptions hit Amsterdam, Denmark, Brussels, and other European airports in 2025. Norway's Avinor, operating 43 airports from Oslo at 30 million passengers to the smallest at 20,000, experiences GPS jamming and spoofing daily in its northern operations near the Russian border:

"We cannot rely on satellite systems for navigation alone. We also keep conventional and traditional navigation systems in place."

Tarald Johansen, director - safety, security and contingency, Avinor

The hybrid threats panel highlighted a capability gap that merits industry attention, Heathrow's Mathew Mileham was clear.

Heathrow now has a dedicated team of four focusing on insider threats – up from zero. The UK's Steve Luxford described the recruitment pattern: individuals travelling two hours to get low-level airport access as cleaners, shop staff, or baristas when equivalent jobs exist locally. Avinor confirmed that dark web tenders for airport intelligence and proxy agents are an emerging and documented threat.

The regulatory landscape is compounding the problem. NIS2, the CER Directive, and other EU frameworks overlap without coordination, increasing compliance burden while reducing operational clarity. Finland's Finavia has responded with structural change: its CISO now has matrix reporting to both IT leadership and the security lead.

"Do not try to think that you can make a world where nothing would ever happen. But try to make sure that when incidents happen, you can recover from those very fast."

Leyla Akgez-Laakso, CIO, Finavia

Looking Ahead: Aviation must actively import insider threat capability from pharmaceutical and financial services rather than waiting for aviation-specific solutions. The Norwegian Total Defense model – civil airports legally embedded in national defence infrastructure with regular joint military exercises – deserves study as a framework for high-risk countries. And the industry must shape regulation proactively rather than absorbing overlapping directives designed without operational input.

6. One-stop security: A policy breakthrough and the path to scale

One-stop security between the UK and the US is, by every measure, a success. Delta moves approximately 2,000 connecting customers per week between Heathrow and Atlanta without re-screening. Each passenger saves roughly 45 minutes – 20 from eliminating bag reclaim, 25 from skipping carry-on and body re-screening. Customer satisfaction scores have risen substantially. American Airlines reports that 50% of its London-connecting customers flow onwards to British Airways in Terminal 5, all benefiting from the same elimination of redundant screening.

"The answer wasn't 'the same as us.' The answer was that we would end up with equivalent security outcomes."

Jason Hausner, managing director - passenger facilitation, Delta Air Lines

That distinction – requiring equivalent outcomes rather than identical processes – is what makes OSS theoretically scalable to a wider range of partner countries. But theory and practice diverge sharply. Most US hub airports are not configured for international arrivals that bypass TSA screening to enter sterile domestic concourses. Atlanta and Dallas had to engineer creative workarounds. The programme remains a pilot, and the scaling logic requires mutual benefit in both directions.

The playbook from the UK-US agreement is now replicable. The gap analysis methodology, the mutual inspection regime, and the equivalence framework all exist. The US Congress has authorised six last points of departure for pilot negotiations. But each new partner country introduces its own infrastructure incompatibilities and regulatory specificities.

"Complacency is the thing that will kill you – literally."

Peter Drissell, director aviation security, Civil Aviation Authority

Looking Ahead: OSS will expand, but slowly. The six authorised last points of departure will be added faster than the first, thanks to the established playbook. But the infrastructure reconfiguration required at receiving airports is a multi-year engineering challenge. The real prize – tail-to-tail baggage transfer unlocking domestic connection models at international hubs – will drive airline advocacy for expansion.

7. Workforce retention in airport security

Haneda Airport's Terminal.0 innovation lab produced many striking findings, but none more alarming than this: a proof-of-concept at its security checkpoint revealed that 50% of security staff quit. Twelve formal complaints were filed from a single checkpoint.

"The environment must soften human stress, to reduce human stress."
Yutaka Kuratomi, vice president, business marketing division, Japan Airport Terminal Co. Ltd

This is not a Japanese problem. It is an industry-wide crisis that technology is accelerating rather than solving. Copenhagen's eight-year checkpoint transformation required retraining 550 staff on new systems; only three people from the original project team remain. CATSA built custom emulators from hundreds of CT images because manufacturers' training materials were inadequate. Gatwick found that screeners' first instinct on new systems is to over-reject, requiring weeks of supervised confidence-building.

The disruptive passenger panel added another dimension. One cabin crew member at a UK airline documented 89 incidents of disruptive passenger behaviour in 12 months:

"After one altercation when somebody swears at you, calls you multiple names – that can impact your mental health so much that you just quit the job, or it creates a trauma for the rest of your life."
Diana Marta Ruka, ground instructor manager, airBaltic

Houston's Cliff Price highlighted a systemic pressure: TSA staffing was affected by a pay disruption during the conference period, with real-time operational implications across US airports.

Haneda's response is to redesign the sensory environment itself. Terminal.0's philosophy starts from a different premise:

"We believe airports should be more than transit points. They should move people emotionally. Technology should serve that experience, then quietly fade away."
Masaya Shimizu, associate, Innovation Lab member, Azusa Sekkei Co. Ltd

The UK CAA's workforce transformation offers a complementary model. When Trussell dropped all experience requirements for inspector recruitment and established a Level 7 training programme, 2,200 applicants competed for 30 posts. The inspector corps went from 95% male to 20% ethnic minority. The insight is structural: when you remove artificial barriers and invest in development, the talent pipeline is not the problem. The institutional design is.

Looking Ahead: The airports that solve security staffing will be the ones that treat the checkpoint as a human environment first and a technology deployment second. Haneda's sensory redesign, CATSA's custom training infrastructure, and the CAA's competency-based recruitment are three models addressing different dimensions of the same crisis. The industry cannot automate its way out of a 50% attrition rate. It must design its way out.

8. Inclusive security by design

King Salman International Airport in Riyadh, currently serving 40 million passengers with a master plan targeting 100 million by 2030, is pioneering an approach few airports of its scale have taken: embedding inclusive design at the strategic planning stage rather than retrofitting it into finished buildings.

"We don't want to give special treatment. We want one journey for all. It doesn't matter if you are with a disability, PRM, traveling with kids, traveling for the first time – which is a lot of people in our region."

Mark Van Doorne, VP airport masterplanning and strategy, King Salman International Airport Development Company

Foster & Partners' Suzan Ucmaklioglu named the systemic failure:

"Generally, when we talk about inclusive design, it's in technical language. When we talk about accessibility, it's always about: is our building code compliant? In turn, that begins to objectify the people we're trying to design for."

Suzan Ucmakliolgu, associate partner and inclusive design specialist, Foster + Partners

At KSIA, 17 specialist parties are working alongside Foster & Partners across 7 major assets and 6 runways. A lived-experience user panel has been engaged multiple times across all assets. The results are tangible: seating placement, sensory space adjacency, lift button design, plug socket heights, and boarding zone sequencing have all been shaped by user feedback in addition to KSIA inclusive design standards, international guidance and code minimums. Across the industry, wheelchair users and families who board first are consistently placed at the back of the gate area. KSIA's layout solves this at the architectural level.

Over 2.2 billion people globally have some form of vision impairment. Haneda's Terminal.0 is exploring personalised wayfinding that appears only when needed, for the specific person who needs it, then fades – information architecture rather than information addition. The digital twin backbone being designed into KSIA from day one will enable similar personalised assistive layers without the retrofitting burden.

"Technical compliance is really important. What it doesn't get at is the end-to-end journey. If someone experiences a barrier at any point in their experience, the journey as a whole is not an inclusive experience."

Nuala O'Sullivan, principal accessibility and inclusive design consultant, Mima

Looking Ahead: KSIA will be the test case for whether inclusive design at scale delivers not just better accessibility but better security. When every passenger can navigate the terminal independently, the pressure on staff decreases, throughput improves, and the security process becomes more predictable. Inclusion is not a concession to equity. It is a performance variable.

From control to intelligence: What happens next

The Security topics at PTE World Conference 2026 described an industry in transition – from a security model built on control (checkpoints, compliance, containment) to one that must be built on intelligence (threat prediction, information sharing, adaptive design).

The transition is not smooth. The regulations that govern information sharing were written before supply-chain cyberattacks became the dominant vector. The checkpoints that house CT scanners were designed for X-ray machines. The staffing models that train security officers were built before 50% attrition became normal. The insider threat programmes that protect financial institutions have no aviation equivalent. The inclusive design principles that KSIA is pioneering from greenfield are nearly impossible to retrofit.

But the direction is clear. Queen Alia International Airport in Amman – the last major airport open in its region, with Damascus, Tel Aviv, Beirut, and others closed around it – grew 11% year-on-year while replacing 60 X-ray machines in a live operation and integrating AI-driven surveillance into a unified security management system. Crisis, as the Jordan team demonstrated, is the accelerant that routine conditions delay.

The certification and testing pipeline, 30 years old and structurally misaligned with technology development velocity, is being reformed through the TAG Union of Tests approach – but remains years behind where the technology already is. The Einstein project's fast-track corridor, processing 15 persons per minute at TRL 7-8, demonstrates what is technically possible. The gap between "ready" and "deployed" is institutional, not technological.

Five Imperatives

1. Build trust before you need it.

The airports that navigated cyber incidents most effectively were those with pre-existing bilateral trust relationships. You cannot build the sharing framework during the crisis.

2. Design for total loss.

Seattle's experience proves that partial recovery plans are insufficient. Every airport needs a tested plan for complete infrastructure failure, not just individual system outage.

3. Import capability from adjacent industries.

Pharmaceutical and financial services are ahead on insider threat detection. Aviation does not need to invent solutions; it needs to adapt them.

4. Redesign the checkpoint, not just the scanner.

CT is a platform, not a point solution. Dynamic ConOps, data-driven feedback loops, and full ergonomic redesign are the next phase.

5. Treat people as the system, not the weakness.

From Haneda's sensory redesign to the CAA's competency-based recruitment to KSIA's lived-experience panels, the most effective innovations were human-centred, not technology-centred.

The $2 trillion being invested in airport infrastructure globally will reshape terminals, runways, and transport connections. Whether it reshapes security with equal ambition depends on whether the industry can move from a culture of compliance to a culture of intelligence. The threats have already made that transition. The question is whether aviation's defences will follow.

Appendix: Sessions referenced

REPORT SECTION	SESSIONS
Section 1: Compliance	From Assessment to Assurance: Risk Management and SeMS Working as One – A Regulator's Standpoint (Civil Aviation Authority); Panel: From Assessment to Assurance (Edinburgh Airport, Melbourne Airport)
Section 2: Seattle	Seattle Airport Cyberattack: Lessons Learned (Port of Seattle; McCarthy Building Companies)
Section 3: Collaboration	Panel: Cleared for Takeoff – Elevating Cybersecurity Through Collaboration (AVIATION ISAC, Heathrow Airport, Groupe ADP, IATA); Panel: Hybrid Attacks – Dare to Discuss (Copenhagen Security Excellence, Heathrow Airport, Finavia, Avinor, NPCC Aviation Security and Airport Policing Portfolio)
Section 4: CT Scanners	Copenhagen's Checkpoint Transformation (Copenhagen Airports, Vanderlande); Panel: CT Scanner Challenges (ADR Security, Heathrow Airport, Canadian Air Transport Security Authority, London Gatwick); Panel: Optimizing the Checkpoint (Analogic, Point FWD, Amazon Web Services, Royal Schiphol Group, Delta Air Lines)
Section 5: Hybrid Threats	Strengthening Airports Against Hybrid Threats in Europe (Copenhagen Security Excellence, ACI Europe); Panel: Hybrid Attacks – Dare to Discuss (Copenhagen Security Excellence, Heathrow Airport, Finavia, Avinor, NPCC Aviation Security and Airport Policing Portfolio)
Section 6: One-Stop Security	Panel: One-Stop Security – Raising Global Standards (Delta Air Lines, Civil Aviation Authority, American Airlines)
Section 7: Staff Attrition	Terminal.0 Haneda (Japan Airport Terminal Co. Ltd, Azusa Sekkei Co. Ltd); Copenhagen's Checkpoint Transformation; Panel: Crime Prevention and Disruptive Passengers (NPCC Aviation Security and Airport Policing Portfolio, Changi Airport Group, airBaltic); Panel: When the Circus Comes to Town (Los Angeles World Airports, Houston Airports)
Section 8: Inclusive Design	Panel: End-to-End Inclusive Passenger Experience – King Salman Intl Airport (King Salman International Airport Development Company, Mima, Foster + Partners); Terminal.0 Haneda (Japan Airport Terminal Co. Ltd, Azusa Sekkei Co. Ltd)
Conclusion	Security Planning Amid Regional Instability (Airport International Group - AIG); Security Equipment Testing and Certification (Defence Science and Technology Laboratory, Heathrow Airport, Canadian Air Transport Security Authority); Einstein: Secure ID Management (JSCP, CERTH-ITI); Aviation Security from Pakistan (Airports Security Force, Ministry of Defense); Staff Access Control Using Biometrics (Changi Airport Group); Panel: When the Circus Comes to Town (Los Angeles World Airports, Houston Airports)

For more exclusive market insights, **subscribe to *PT World*** – the airport sector's leading international communication platform

www.ukimediaevents.com/recard/passenger-terminal.php

THE LEADING INTERNATIONAL PUBLICATION FOCUSED ON PASSENGER TERMINAL FACILITIES, DESIGN AND TECHNOLOGY

Discover how *PT World* can support your marketing needs!
Reach our international audience via:

- Tailored editorial packages/exclusive interviews;
- Targeted e-blasts;
- E-newsletter and website promotion;
- Fully supported webinars and unique video content.

Promote your company's expertise – contact **aboobaker.tayub@ukimediaevents.com** for further information!

UKi Media & Events, Parsonage House, Parsonage Square, Dorking, Surrey, RH4 1UP, UK. Tel: +44 (0) 1306 743744

Get the latest news and exclusive web features online:
www.passengerterminaltoday.com