Thales' Security Operations Centre. Image: Thales

Preventing the breach

Preventing cyber-threats is no longer an IT issue, it's an airport-wide operational priority. With increased digitalisation and reliance on shared data and systems, airports – as high-value targets – are increasingly vulnerable to cyber-attacks. Paul Sillers investigates.

Cyber-attacks last September at Heathrow, Brussels and Berlin Airports targeting Collins Aerospace MUSE (Multi-User System Environment) check-in software have shown how a single breach can disrupt flights and paralyse operations across multiple territories.

Then on 14 October, concourses at four North American airports – Harrisburg (PA), Windsor (ON), and Kelowna and Victoria (BC) – reverberated to the menacing din of anti-Western propaganda as hackers seized control of PA systems.

At Kelowna, the breach also disrupted flight information screens and an airport advertising service.

Cyber-penetrations such as these not only cause operational nightmares and undermine passenger confidence – they also push up security expenditure for airports and airlines (and raise ticket prices) while exposing the aviation sector to legal liabilities after breaches.

Attackers exploit both human and technical weaknesses through phishing – a cyber-attack that sees criminals impersonate trusted entities to trick people into revealing sensitive information or clicking malicious links.

Then there are DDoS attacks (Distributed Denial-of-Service), which make online services unavailable to legitimate users by flooding the system with excessive and malicious internet traffic and ransomware, targeting everything from admin systems to flight operations.

Airport IT systems also face rising risks from data theft, account takeovers and loyalty programme fraud — all of which erode public trust and open the door to deeper breaches.

THE SCALE OF THE PROBLEM

Thales' *2025 Data Threat Report*, produced with S&P Global Market Intelligence 451 Research, found that 39% of critical national infrastructure (CNI) organisations use more than 500 Application Programming Interfaces (APIs) and one in five operates over 1,000. APIs are digital bridges that let different software systems talk to each other.

"Every one of these APIs represents an extension of the attack surface if inadequately secured," says Tim Ayling, VP EMEA, Cybersecurity Specialists, at Thales.

Ayling notes that "disruption to the aviation industry through cyber-attack represents a major national security threat, with repercussions being felt across entire economies, businesses, as well as individual passengers."

He argues that cyber-resilience must now be viewed as a form of critical infrastructure protection.

"This isn't just about protecting an airport's own system – as we've seen from attacks earlier in the year, it's also about working with the many third-party systems that are in place with access, as they represent other sources of risk."

THE AI CONUNDRUM

Emerging technologies are reshaping the cyber landscape, as Ayling explains.

"Another threat area growing in concern is that posed by AI and quantum," he tells *Regional Gateway*. "Seventy-three per cent of respondents [to questions in Thales' *Data Threat Report]* say the fast-changing AI ecosystem is their leading AI-related security challenge.

"Offering the ability to help make attacks more frequent and sophisticated, AI can probe thousands of possibilities to look for flaws, as well as adapt and evolve to become more effective."

Despite this, many incidents still originate from preventable weaknesses.

"The vast majority of incidents still stem from misconfigurations and software vulnerabilities that can be prevented with stronger governance and secure-by-design approaches," says Ayling.

He adds that building resilience into systems – and regularly auditing them – is the only way to ensure services remain available when they're needed most.

To help airports and airlines respond to these evolving risks, Thales has developed cybersecurity solutions designed for critical infrastructure.

"Thales offers a range of technologies and services to protect both applications and the sensitive data inside them," says Ayling.

In the UK, the company supports government and infrastructure operators with "real-time anomaly detection, automated containment, proactive testing, and layered controls to lock down information and guard the pathways into it".

For aviation, Thales delivers tailored cybersecurity services that protect passenger data, operational systems, and flight continuity – an approach recognised by the Frost & Sullivan Cybersecurity for Airports Award.

All solutions are powered by the Thales Cyber Threat Intelligence Team, which "continuously monitors the ever-changing threat landscape" to improve AI-driven detection and rapid response.

Two flagship platforms anchor this approach: the CipherTrust Data Security Platform and Imperva WAAP and API Security.

"Identifying, encrypting and monitoring where data resides and is accessed, as well as protecting the applications that are running off that data, is vital to ensure services stay up and running where they're needed most," Ayling concludes.

> **"AI has changed the tempo. You no longer have time to detect, investigate and respond. You need to block as much as possible before the attack begins."**
>
> Charlotte Wilson, Head of Enterprise, Check Point Software Technologies

BUILDING COMMUNITY IN CYBER-DEFENCE

For Charlotte Wilson, Head of Enterprise at Check Point Software Technologies, cybersecurity isn't just about technology – it's also about people.

"Across every industry right now, and especially in critical national infrastructure, the UK is being heavily targeted – and we're all on the same side," she says.

Check Point has been running leadership summits that bring together cyber professionals, airport executives and infrastructure operators to share real-world experiences and lessons learned from breaches.

"These aren't product events," Wilson emphasises. "They're about creating a community that collaborates. One of our guests recently said their biggest concern wasn't tools – it was that vendors in their supply chain were competing instead of talking openly about protection."

According to Wilson, that culture of openness is essential as cyber incidents increasingly move beyond IT disruption to affect passengers, airlines and airport operations.

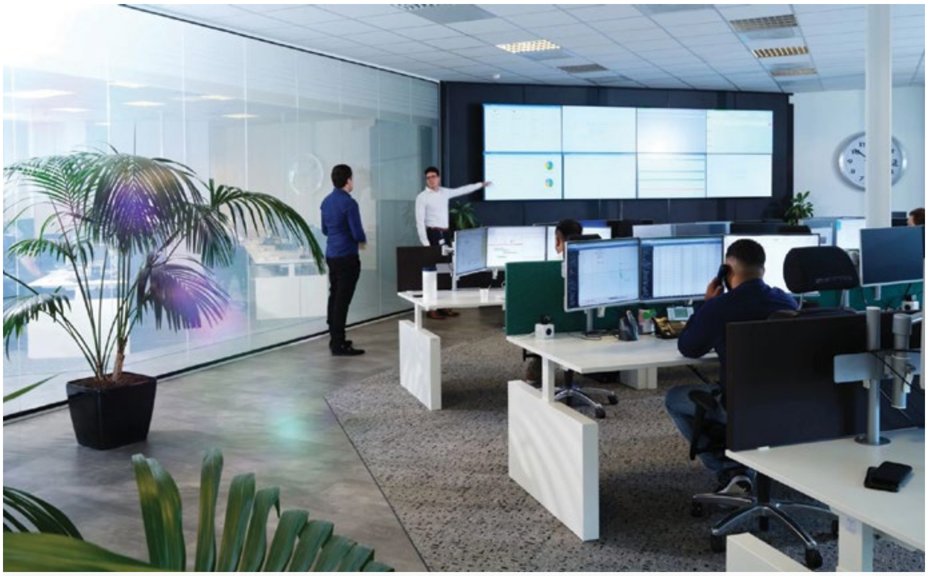
"Airports sit at the intersection of safety, commerce and national security," she adds. "They're complex environments – a mix of IoT devices, operational technology, cloud infrastructure, and third-party systems. And each of those is a potential entry point for attackers."

AI, ETHICS AND THE EXPANDING ATTACK SURFACE

Wilson's own area of expertise is governance and ethics around artificial intelligence.

"AI brings both opportunity and risk," she says. "Attackers are already using AI to make spear-phishing more convincing and to automate intrusion attempts."

Spear-phishing is a targeted cyber-attack whereby attackers research a specific individual or organisation to craft personalised, convincing messages that trick the victim into divulging sensitive information.


The use of APIs potentially extends the 'attack surface'. Image: Thales

"We're seeing threat actors like Nimbus Manticore using fake recruitment portals to target aviation workers directly," adds Wilson.

Check Point's response combines prevention-first design with AI-powered monitoring. Its ThreatCloud AI platform uses more than 55 machine-learning engines to detect and block attacks in real time, drawing intelligence from global threat teams and dark web monitoring.

"AI has changed the tempo," says Wilson. "You no longer have time to detect, investigate and respond. You need to block as much as possible before the attack begins."

In September, Check Point acquired Lakera, a leading AI-native security platform for Agentic AI applications. These are AI systems that can think, plan, and execute tasks autonomously to achieve goals, rather than just respond to single prompts or commands.

The acquisition enables Check Point to deliver a full end-to-end AI security stack designed to protect enterprises as they accelerate their AI journey.

Wilson says: "Many airports and airlines are exploring AI for operational efficiency – but they also need to be confident that sensitive data isn't being exposed or manipulated."

NOT FORGETTING THE HUMAN FACTOR

Wilson is clear that aviation security depends as much on collaboration as it does on code.

"You're only as strong as your weakest connection," she notes. "Airports and airlines are highly networked across suppliers, concessionaires and logistics partners. A breach in one area can ripple across all of them."

Check Point takes a partner-first approach, combining its platform solutions with consultancy, simulations,

The cyber-threat targeting aviation

Check Point Research reports that it has been tracking a sophisticated campaign by the IRGC state-backed threat group "Nimbus Manticore", which is targeting aviation and aerospace sectors in Europe and the Middle East.

The group impersonates companies like Boeing, Airbus, Rheinmetall and flydubai, sending fake job offers in spear-phishing emails.

Nimbus Manticore tricks victims into downloading infected files that secretly install malware through "DLL side-loading" – a hacking method whereby attackers disguise malicious code as a trusted file under legitimate digital certificates and trusted cloud platforms.

This enables cyber-criminals to bypass security, hide their activity, and maintain access to systems.

With activity spreading across Western Europe, Nimbus Manticore poses a persistent and strategic threat to Europe's aviation supply chains and critical infrastructure.

The infection chain starts with phishing links leading to fake job login pages impersonating firms like Boeing and Airbus. These pages use React templates (web frameworks that let attackers easily clone and customise company websites) and "career"-themed domains hidden behind Cloudflare (a service that masks a website's real server and location).

Each target receives unique login credentials, and only when these are entered does the site deliver a malware archive – demonstrating precise targeting, strong operational security, and state-level tradecraft.

To defend against Nimbus Manticore's attacks, organisations need and readiness planning.

The company helps airports align with EASA and NIS2 compliance frameworks – roadmaps that organisations use to ensure they meet EU cybersecurity laws covering prevention, response, governance, and accountability for digital resilience.

Despite the rising sophistication of attacks, Wilson remains optimistic.

"I see the cyber community working more closely together than ever before," she says. "When companies share their breach experiences openly – as we've seen some do – everyone learns, and the entire ecosystem becomes stronger. That's what real resilience looks like."

THE CYBER COST OF MAINTAINING OPERATIONS

Cyber-threats are a direct and costly challenge for airports, carrying significant financial and operational consequences.

Joshua Cole, Chief Technology Officer at Assura, says: "Airports probably understand their average revenue per hour and therefore have a powerful data point to quantify cyber-risks. Millions of pounds per hour of lost revenue for a large airport like Heathrow is a compelling 'so what' when it comes to articulating the financial consequence of cyber-risk."

Assura provides tailored cybersecurity services to help aviation clients mitigate these threats, offering Virtual Chief Information Security Officer support (vCISO), Security Operations Centre-as-a-Service (SOCaaS), penetration testing, vulnerability management and bespoke services – all underpinned by its AuditArmor compliance and audit defence guarantee.

Cole tells *Regional Gateway* about a critical incident in which Assura's monitoring identified a faulty firewall rule that could have exposed a client's entire network to attackers.

"Fortunately, we caught the issue quickly," he says. "Our threat detection and response tools were already in place, so any exploitation would have been stopped, but it could have become a very bad situation."

For airports, proactive monitoring, independent oversight and continuous protection reduce disruptions, safeguard passenger flow, and maintain trust – critical in an industry where even minor delays can cascade through airlines and schedules.

Despite growing awareness, Cole warns that many airports are still underinvesting in cybersecurity.

"For every airport that invests adequately, 10 do not and have appallingly low maturity in this area," he says, noting that many lack the skills to analyse cyber-risk.

These gaps can lead to costly delays and data exposure, while third-party systems add further complexity.

Regarding the cyber-events at Heathrow, Brussels and Berlin airports, Cole says: "It's not their fault, but it is their burden."

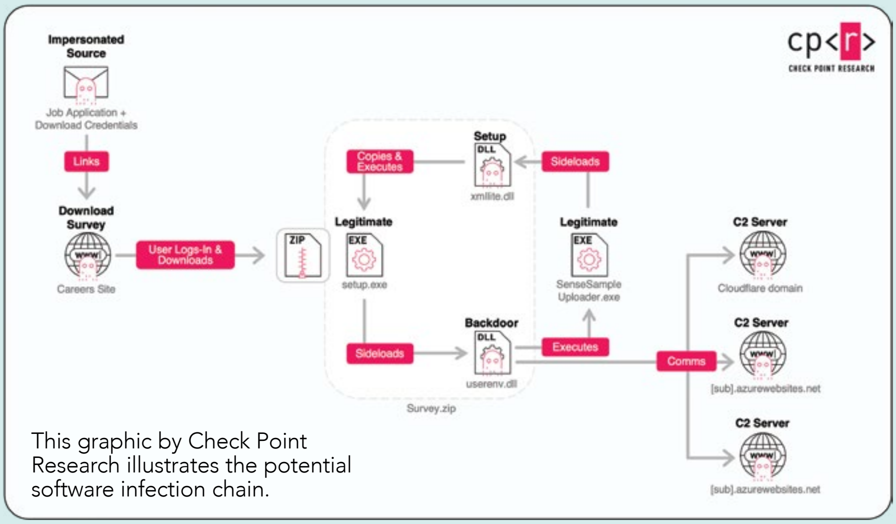
Passengers rarely distinguish between airport and supplier failures, highlighting the need for robust third-party cyber-risk management.

With complex systems spanning operational technology, baggage handling, IoT devices and cloud platforms, protecting the wider ecosystem is now just as vital as securing an airport's internal network. Both are essential to keeping flights, schedules and passengers moving safely. ■

multi-layered protection that stops threats before they reach users or systems.

Check Point Harmony Email & Collaboration blocks phishing emails, fake job sites, and malicious attachments; Harmony Endpoint protects devices if malware bypasses initial defences; and Quantum Network Security prevents malicious traffic, downloads and data theft at the network level.

Together these solutions create a comprehensive shield against sophisticated cyber campaigns.



This graphic by Check Point Research illustrates the potential software infection chain.