Week commencing 7 September 2026

ClearPath Partnership

COVERAGE
24 August – 6 September 2026

AUDIENCE
Accountable managers · IT and security leadership

HANDLING
Internal use — not for onward distribution

IF YOU JUST REMEMBER ONE THING FROM THIS BRIEFING…

The fortnight's largest breach hit systems nobody was watching hardest: car parking, Wi-Fi and lounge bookings, not flight operations.

Manchester Airports Group's backend booking platform gave up 8.7 million customer records across three airports; the data was published on 2 September after MAG refused to pay. Ask your team: do our "ancillary" customer platforms get the same assurance testing as operational systems, or less.

FORTNIGHT IN REVIEW

Incidents and sector activity

PRIORITY

1–2 SEP

SonicWall SMA1000 zero-day chain gives unauthenticated code execution on remote-access gateways

SonicWall confirmed active exploitation of two chained SMA1000 flaws on 1 September: CVE-2026-83548, an unauthenticated SSRF (CVSS 10.0), and CVE-2026-83549, an OS command injection, together giving remote code execution. Both reached the CISA KEV catalogue the next day — the third exploited SMA1000 zero-day since December.

So what: SMA1000 units terminate VPN and remote-maintenance access across many estates. Treat any internet-facing unit as compromised until patched.

PRIORITY

28 AUG

Manchester Airports Group breach exposes 8.7 million customer records, then gets published

An unauthorised third party accessed a backend system handling car park, lounge, Fast Track and Wi-Fi bookings across Manchester, Stansted and East Midlands airports. MAG refused the ransom; FulcrumSec published roughly 640GB of the data on 2 September, including emails, phone numbers and vehicle registrations. Payment data and operations were unaffected.

So what: ancillary customer platforms now carry the same regulatory exposure as core systems. Confirm they receive equivalent testing and monitoring.

WATCH

2 SEP

Storm ransomware group lists Boeing and Airbus supplier Star Aviation

Storm, a ransomware group active since August, listed Kentucky supplier Star Aviation Inc on its leak site on 2 September, claiming theft of technical schematics and employee ID data — one of roughly 44 to 48 victims claimed since it surfaced, amid intensifying extortion focus on aviation suppliers.

So what: check what schematics or engineering data your tier-2/3 suppliers hold, and whether contracts require prompt breach notification.

WATCH

1 SEP

Zelensky warns Russian airspace unsafe as GNSS jamming intensifies

On 1 September President Zelensky warned airlines that Russian airspace is no longer safe, citing GPS jamming severe enough to make aircraft disappear from radar, alongside expanding drone and air-defence activity. It follows August's confirmed growth of Baltic spoofing infrastructure and EASA's revised Safety Information Bulletin.

So what: reassess routing and diversion planning near Russian and Baltic airspace; confirm crews hold current GNSS-denied procedures.

PATCH QUEUE

Vulnerabilities to act on this fortnight

IDENTIFIER	PRODUCT	WHY IT MATTERS HERE	ACT BY
CVE-2026-83548	SonicWall SMA1000	Unauthenticated SSRF on remote-access gateway. First link in RCE chain.	Immediate
CVE-2026-83549	SonicWall SMA1000	Command injection chained with above for full remote code execution.	Immediate
CVE-2026-8452	Citrix NetScaler ADC/Gateway	Perimeter VPN and load balancer. Remote denial of service.	Overdue
CVE-2026-85046	Chromium / browsers	V8 type confusion. Staff, crew and kiosk browsers.	7 days
CVE-2026-81578	PaperCut NG/MF	Auth bypass on print management used in back-office and boarding docs.	7 days

Identifiers are as published in the CISA KEV catalogue. Confirm applicability against your own asset inventory — this list is a prompt, not a substitute for it.

REGULATORY AND SECTOR WATCH

What changed, and what is coming

In force now

- National aviation authorities have begun the first round of Part-IS "cyber-audits" under Part-CAMO and Part-145, testing critical information asset registers against documented policy.
- No new EASA Part-IS guidance published this fortnight.

Approaching

- Cyber Resilience Act reporting obligations begin 11 September — manufacturers must file a 24-hour early warning and 72-hour full notification for exploited flaws via the new Single Reporting Platform.

UK. No new CAA cyber information notice this fortnight; the CAP 1753 oversight cycle continues unchanged. No NIS2 enforcement action confirmed against an aviation entity.

Standing watch — GNSS interference. Baltic spoofing infrastructure keeps expanding and Zelensky's 1 September warning adds a new front; EASA's Safety Information Bulletin revision 4 remains the operative guidance.

RECOMMENDED

Three things to do before next Monday

- Patch or isolate internet-facing SonicWall SMA1000 and Citrix NetScaler gateways today; treat both as exploited now.
- Confirm manufacturer suppliers are ready for the Cyber Resilience Act's 11 September reporting deadline.
- Check assurance coverage of ancillary customer platforms matches core operations, with supplier leak-site notification clauses in place.

OUTLOOK — NEXT FORTNIGHT

We assess it is likely further aviation or aerospace suppliers appear on ransomware leak sites before the next edition, given the pace of listings this fortnight. It is a realistic possibility another European airport discloses a comparable ancillary-system breach, given the low barrier FulcrumSec described in the MAG case.

NEXT EDITION

Monday 21 September 2026. Send additions, corrections or sector intelligence to your ClearPath engagement lead.

ClearPath Partnership