How UK Aviation Looks to an External Cyber Security Scan

What a non-intrusive external assessment of 54 UK airports and 51 of the organisations they depend on found, and where the exposure actually sits

> **Purpose**
>
> To explain cyber security and cyber posture in plain English, place UK aviation in its regulatory context, report what our external assessment found in each of its two source cohorts, and set out realistic actions that operators, suppliers and boards can take.

Sources	Two separately assembled cohorts, reported separately throughout: **43 airport operator websites** representing 54 UK airports, and **51 supplier organisations** providing services into those airports.
Combined	The two lists were compared organisation by organisation and share nothing. No organisation appears in both, so they represent **94 distinct organisations** and may legitimately be added. The combined view is reported in section 7, after the sources.
Evidence	Single external assessment completed 2 September 2026. All 94 organisations produced a completed, scored result from one run. No evidence gaps.
Method	Non-intrusive external assessment using publicly observable information, websites, DNS, certificates, public threat intelligence and publicly reachable services. No logins, password attempts or intrusive probing.
Scope limit	The public web estate only. No airport operational technology, air traffic system, airline system, baggage system or security screening system was touched or assessed.
Prepared by	Huro Data Technologies Ltd / MyDomainRisk
Date	2 September 2026

Research and external assessment: MyDomainRisk | Huro Data Technologies Ltd

Why this matters now

On 27 August 2026, Manchester Airports Group disclosed that an unauthorised third party had taken approximately **8.7 million passenger records** across Manchester, Stansted and East Midlands. The data was email addresses, phone numbers, vehicle registrations and postcodes, taken from car park bookings, lounge bookings, Fast Track bookings and airport wi-fi sign-ups. No payment details were accessed. MAG said it had contained the risk, that passenger safety and aviation security were not compromised, and that operations were unaffected.[1]

Read that list of data sources again, because it defines half the subject of this report. **The breach was not on the aviation-operational estate. It was on the commercial, passenger-facing web estate**, the booking engines and sign-up forms that sit on an airport's website. An airport's security-critical systems are not reachable from the internet. Its car park booking page is.

Eleven months earlier, a different failure made the same point from the other direction. In September 2025, ransomware against Collins Aerospace's MUSE check-in software disrupted Heathrow, Brussels, Berlin and Dublin, with boarding passes failing at gates and airlines reverting to manual check-in for several days. RTX confirmed the ransomware in an SEC filing and the National Crime Agency made an arrest under the Computer Misuse Act.[2] No airport was breached. One shared supplier was, and four international airports stopped working normally.

> **Why this report has two halves**
>
> Those two incidents describe two different estates. One is the airport's own website. The other is the layer of organisations an airport depends on to run a passenger operation: lounges, parking, surface access, ground handling, passenger processing, screening, baggage and airfield systems.
>
> Assessing only the first would have missed Collins Aerospace entirely. So this study assembled both, assessed them on the same day with the same routine, and reports each separately before combining them. The result is that the two halves can be compared directly, and the comparison turns out to be the finding.

A way of picturing it

Imagine somebody walking down your street. They never go inside any building, never try a door. They simply walk past and notice what is visible from the pavement: a window left open, a side gate unlatched, a spare key under the mat where everyone knows to look. None of that means the house has been burgled. It means somebody passing by can see opportunities, and most of them take a minute to put right.

That is exactly what this assessment does. We looked at each organisation from the public internet, the way any visitor, or anyone with less good intentions, would see it. We did not log in anywhere, try any password, or look at anything that was not already on public view. Standing in the street also tells you nothing about the alarm system or the locks on the internal doors, which is why nothing here is a verdict on any organisation's security. It is an account of what is showing from outside.

Executive summary

The short version

The airports are in reasonable shape. The organisations they depend on are not, and **99% of the exposed employee credentials in UK aviation's public web estate belong to suppliers rather than to airports**.

Ten employee credential records sit across 54 UK airports. One thousand one hundred and fifty-two sit across 51 suppliers. Three of those suppliers appear in ransomware leak-site data, where no airport operator does. An assessment of airports alone would have produced a fair but seriously incomplete picture of this sector.

Two sources, assessed the same day

This study rests on two separately assembled lists, reported separately because they describe different kinds of organisation with different obligations.

Headline	Airport operators (43)	Suppliers (51)
Average score / median	69.2 / 71	65.3 / 67
Lowest score in the cohort	27	9
In the top band	16 (37%)	11 (22%)
Does not instruct rejection of forged mail	17 (40%)	17 (33%)
Risky reachable service	2 (5%)	5 (10%)
Database port answering	1 (2%)	4 (8%)
Ransomware leak-site mentions	0	3 (6%)
Employee credential records on own domain	10	1,152
No credential records in any bucket	19 (44%)	8 (16%)

99%
of exposed employee credentials sit with suppliers, not airports

92%
of employee credentials belong to the three supplier classes operating airside

0
ransomware mentions, breach records or browser-safety flags across all 43 airports

Put plainly: the sector's regulated, named, publicly accountable half is the healthier half. The exposure has collected in the layer that carries none of the regulatory obligation and holds much of the access. That gap between where the consequence lands and where the weakness lives is the structural finding of this report.

The one measure on which the airports are worse is email authentication. Forty per cent of them cannot stop a message being sent in their name, against 33% of suppliers. It is also the cheapest finding in either half to fix, and the airport name is by far the more attractive one to forge.

1. Cyber security in plain English

Cyber security is the practice of protecting an organisation's people, accounts, data, systems and reputation from unauthorised access, misuse, disruption or loss. For most organisations in this study it is not primarily about sophisticated attackers or expensive technology. It is about making common attacks harder, limiting the damage if something does go wrong, and being able to recover quickly.

The National Cyber Security Centre frames this as risk management supported by practical controls. Its guidance focuses on securing email and important accounts, protecting devices, backing up data and spotting attacks; its 10 Steps guidance adds identity and access management, vulnerability management, incident management and supply-chain security.[3]

What 'cyber posture' means

Cyber posture is the condition of those defences at a point in time. A useful way to think about it is: if someone who knew nothing about your organisation looked at it from the public internet, what could they learn about your digital estate, your security controls and possible routes in?

> **Security is cumulative**
>
> A strong posture is rarely one product. It is the combined effect of many ordinary controls: strong authentication, sensible configuration, secure email, patched systems, limited internet exposure, good supplier information, clear reporting routes and a rehearsed response plan.

Common weaknesses identified in our assessment, and why they matter

Weakness identified	Why it matters
Stolen or reused credentials	Addresses and session data can be harvested from infected devices. Multi-factor authentication, resets and session revocation reduce their value. This is the largest single finding in this study.
Weak email authentication	If a domain does not tell receiving mail systems to reject forged messages, criminals have more scope to impersonate a trusted airport or supplier to passengers and to each other.
Unnecessary internet-facing services	Database, file-transfer, remote-access and administration services should not be publicly reachable unless there is a clear need and strong protection.
Out-of-date or incomplete configuration	Missing security headers, weak transport settings and poorly maintained certificates can enlarge the attack surface or confuse passengers.
Limited visibility of suppliers	An airport may know a supplier is contracted but still not know exactly what data that supplier holds, what access it has, or how quickly it could provide an incident breakdown.
No route to report a problem	If a researcher or member of the public spots a weakness, they need an obvious, safe way to tell the organisation. Almost nobody in this study provides one.

> **One abbreviation, two meanings**
>
> In this report **CAA records** means Certification Authority Authorization, a DNS record naming which certificate authorities may issue certificates for a domain. The aviation regulator is written out in full as the **Civil Aviation Authority**. The two are unrelated.

2. The regulatory picture

UK airports are designated critical national infrastructure within the statutory Network and Information Systems regime. The Civil Aviation Authority is the competent authority for air transport and assesses operators against the NCSC's Cyber Assessment Framework.[4] That obligation is real, it is enforced, and it is one reason the operator half of this study looks as healthy as it does.

The obligation does not travel evenly down the supply chain. A ground handler, a parking reseller or a lounge operator is not an airport, and most of the 51 organisations in the supplier cohort sit outside the aviation designation entirely. Nine in ten of them are independent third parties over which an airport has contractual influence and nothing more.

That is changing. The Cyber Security and Resilience Bill amends the NIS Regulations and extends the regime to managed service providers and designated critical suppliers. Air transport is one of the five sectors already in scope.[5] The direction of travel is that the supplier layer measured in this report comes inside the perimeter rather than remaining outside it.

> **Why the timing makes this report useful**
>
> The Bill will require airports and their designated suppliers to demonstrate supply-chain security. This study is a measurement of that supply chain taken before the requirement bites, using only information any regulator, journalist or attacker could gather for themselves. It establishes where the sector is starting from.

What we did differently

Most sector cyber statistics are surveys. They ask organisations what happened to them and what they have in place, and they depend on what respondents know and are willing to report. This study asked nobody anything. Every figure is an observation taken from outside, on one day, using the same routine on every organisation.

The two approaches answer different questions and neither replaces the other. A survey tells you what a sector believes about itself. An external assessment tells you what a sector is showing to the world. Where this report and a survey disagree, they are probably both right about different things.

3. What we measured

Each organisation's public web estate was assessed against the same set of external checks and given a score from 0 to 100. *Good* is 75 and above, *needs improvement* is 50 to 74, and *at risk* is below 50. A single serious finding can hold a website below a band ceiling regardless of how much else is correct, which is why an organisation with good practice in most areas can still sit in the middle band.

Coverage is complete, and this has been verified rather than assumed

All 94 organisations produced a completed, scored result on 2 September 2026, from a single run rather than a blend of dates. There are no evidence gaps, so no percentage in this report is diluted by an unassessed website, and no figure mixes a fresh reading with an older one.

Assessment coverage	Operators	Suppliers	Combined
Websites in cohort	43	51	94
Completed and scored	43 (100%)	51 (100%)	94 (100%)
Evidence gaps	0	0	0
Appearing in both cohorts	0, verified organisation by organisation		0
Distinct organisations	**43**	**51**	**94**

> **Why the non-overlap is stated rather than assumed**
>
> Two cohorts that look different can still share members, and adding them then produces a population that does not exist. In this firm's charity sector work, two lists of 220 and 236 organisations shared 76 members, and the honest combined figure was 380 rather than 456.
>
> Here the two lists were compared organisation by organisation and share nothing. No airport appears in the supplier cohort and no supplier appears in the airport cohort. The addition to 94 is therefore a true sum rather than an estimate, and it was checked rather than presumed from the fact that the lists look different.

About credentials

Credential figures are read from structured provider data rather than inferred from report text. The provider reports three separate buckets which are routinely confused with one another, and which this report keeps apart and ranks. Section 8 sets out the three in full and explains why the order matters more than the totals.

In short: **employee** records are staff accounts on the organisation's own domain, and are the ones that matter. **Outside-service** records are the organisation's own work identities appearing on somebody else's platform, and are a close second. **Account-holder** records concern members of the public who hold an account on the site, and rank far below the other two. **The three are quoted independently and are never added into a single exposure figure.**

4. Source one: the 43 airport operator websites

The first cohort is the 43 public websites of UK airport operators. Between them these websites represent **54 airports**, because two websites each serve more than one airport: one serves a group of eleven Highlands and Islands airfields, and one serves two Channel Island airfields. Every other website serves a single airport.

The distinction is used throughout. Counting websites answers how many web estates need work. Counting airports answers how much of UK aviation sits behind them. **A finding on the Highlands and Islands website is one website finding and eleven affected airports**, and neither number should be used without the other.

Band	Websites	Share
Good, 75 and above	16	37%
Needs improvement, 50 to 74	22	51%
At risk, below 50	5	12%
Assessed	**43**	**100%**

The average score is **69.2** and the median **71**, against a range running from 27 to 90. Just over one in three UK airport websites is in good order, half sit in the middle band where the gaps are real but routine, and five are in the lowest band. Those five are where a disclosure conversation should begin.

Priority observations

Observation	Operators	Share
Cannot stop email being sent in their name	17	40%
Do not instruct browsers to use a secure connection every visit	20	47%
Certificate or transport-security finding	9	21%
Own identities exposed on outside services	10	23%
Employee credentials on their own domain	4	9%
No credential records in any of the three buckets	19	44%
Risky service or database port reachable	2	5%
Ransomware, known-breach or browser-safety findings	0	0%

The last two rows describe overlapping and measured sets respectively. Two operators carry a risky service or a database port, not three: one carries both. The zeroes are measured zeroes, meaning the check ran and found nothing.

Forged email in the operator's name is the largest single gap and the cheapest to fix. Seven operators publish no policy at all and ten publish one set to take no action. An airport is an unusually attractive name to forge, because passengers expect messages about bookings, parking, delays and disruption. Publishing an enforcing policy requires no change to any airport system.

The credential volumes are low and that is itself the finding. Ten staff records across 54 airports is a small number in absolute terms and materially better than most sectors this firm has measured. Section 5 is where that number changes.

Source one continued: what shapes the operator result

Ownership tracks with outcome, though not decisively

Operator type	Websites	Average	Median	Good	At risk
Private capital	31	71.0	74	14	3
Public sector	12	64.5	66	2	2

The gap of roughly six and a half points is consistent with what this firm sees in local government work, and the likeliest explanation is resourcing rather than attitude: the smaller publicly owned airfields are running lean web estates with little dedicated security capacity. **The finding should not be read as carelessness in the public sector.** Two of the five lowest-scoring websites are privately held, and the single lowest score in the cohort is not a public-sector site.

Half of this estate's visible network surface is not its own

Twenty-three of the 43 operator websites, 53%, are served through a large content-delivery or reverse-proxy provider. For those websites the address, the open ports and the services visible from the internet describe the provider's shared edge, not the airport's own infrastructure, and the same address answers for unrelated organisations with nothing to do with aviation.

This changes how the port and service findings above should be read. Where a fronted website appears to expose an unusual set of ports, that is the provider's platform being observed through the airport's name, and it is not a misconfiguration the operator can correct. **No operator in this cohort carries a risky-service or database-port finding that arises from its provider's edge**, so the small numbers above are genuine, operator-owned findings.

Two limits stated rather than buried

Two scores are floors, not readings. On two websites the homepage did not fully serve to the scanner, so part of the assessment could not be completed. For those two the true score can only be the same or higher, never lower. They are counted in every figure above and their position should be treated as provisional rather than as a finding against the operator.

Ownership attribution is partly unresolved. The cohort marks 31 of the 43 operator attributions as verified and twelve as uncertain, including one unresolved following a corporate restructuring. Attribution is not a security finding, but it decides who receives a disclosure and who funds a fix, so the uncertain entries should be settled before any remediation programme is scheduled.

5. Source two: the 51 supplier organisations

The second cohort is 51 organisations that provide services into UK airports: lounges and private terminals, surface access, parking, passenger processing, ground handling, security and assistance, screening technology, baggage and airfield systems. None of them is an airport. They are assessed here because an airport's passengers, staff and data reach them, not because any airport is answerable for their websites.

> **What the supplier cohort is, and what it is not**
>
> It is a dependency map, not a procurement list. Inclusion means the organisation provides a service into one or more UK airports according to public sources: the airport's own website, the vendor's client list, published contract reporting, or incident reporting. It does not mean any particular airport holds a contract with it today.
>
> **Ownership is overwhelmingly independent.** Forty-six of the 51, 90%, are independent third parties. Three are airport-owned commercial arms and two are airport-owned businesses that are not themselves airports.

Band	Websites	Share
Good, 75 and above	11	22%
Needs improvement, 50 to 74	33	65%
At risk, below 50	7	14%
Assessed	**51**	**100%**

The average score is **65.3** and the median **67**, against a range running from 9 to 86. Only one supplier in five is in good order and two-thirds sit in the middle band. The weakest score in this cohort is **9**, far below anything seen among the operators. One score is a floor rather than a reading, on a website whose homepage did not fully serve.

Priority observations

Observation	Suppliers	Share
Own identities exposed on outside services	27	53%
Employee credentials on their own domain	21	41%
No credential records in any of the three buckets	8	16%
Cannot stop email being sent in their name	17	33%
Risky service reachable	5	10%
Database port answering	4	8%
Certificate problems	4	8%
Ransomware leak-site mentions	3	6%
Known-breach or browser-safety findings	0	0%

Five organisations carry a risky service or a database port, not nine: four of the five carry both, so those rows overlap and must not be added. Thirty of the 51 supplier websites, 59%, are fronted by a shared content-delivery platform, and three of the exposure findings describe that shared edge rather than the supplier's own systems.

Source two continued: where the supplier weakness sits

The supplier average of 65.3 conceals a spread that matters far more than the average does. Sorted by dependency class:

Dependency class	Suppliers	Average	Median	Good	At risk
Passenger commercial, lounges and private terminals	6	69.3	70.5	2	0
Parking	12	68.7	71.0	5	1
Equipment, airfield and platform technology	8	68.6	71.5	1	1
Surface access	8	67.9	68.0	1	1
Passenger processing	5	64.8	63.0	2	1
Security and assistance	5	60.6	65.0	0	1
Ground operations	**7**	**53.1**	**58.0**	**0**	**2**

Ground operations is the weakest class in the cohort by a clear margin, covering handling, cargo, catering and fuel. Its average of 53.1 sits sixteen points below the sector's best class, no organisation in it reaches the top band, and two of its seven are in the lowest. Security and assistance, which includes screening and assistance for passengers with reduced mobility, is second weakest at 60.6 with none in the top band.

The pattern is consistent and uncomfortable. **The consumer-facing classes that most resemble an airport's own website are the healthiest, and the classes that operate airside are the weakest.**

Holding passenger data does not predict a better score

Holds passenger data	Suppliers	Average	Good	At risk
Yes	32	66.8	9	4
Partial	8	65.2	1	1
No	11	61.2	1	2

The suppliers that hold passenger data score slightly higher than those that do not, which is the opposite of the intuitive result and is reported here because it is what was measured. The likeliest explanation is that consumer-facing businesses maintain consumer-facing websites, while an engineering supplier's site is a brochure nobody has revisited. **It should not be read as reassurance.** Four of the seven lowest-band websites in the cohort belong to organisations that hold passenger data.

6. What the two sources show when compared

Because both cohorts were assessed on the same day with the same routine, the two halves can be set against each other directly. On every measure except one, the suppliers are behind the airports they serve.

Measure	Operators (43)	Suppliers (51)	Direction
Average score	69.2	65.3	Suppliers worse
Median score	71	67	Suppliers worse
Lowest score	27	9	Suppliers worse
In the top band	37%	22%	Suppliers worse
In the lowest band	12%	14%	Suppliers worse
Risky service reachable	5%	10%	Double
Database port answering	2%	8%	Four times
Ransomware leak-site mentions	0	3	Suppliers only
Employee credential records	10	1,152	Two orders
No records in any credential bucket	44%	16%	Suppliers worse
Cannot stop forged email	40%	33%	Operators worse

The last row is the only one that runs the other way, and it deserves its own point rather than an asterisk. Email authentication is the cheapest control in this entire report to put right, it requires no change to any operational system, and it is the one control on which the regulated half of the sector is behind the unregulated half. Forty per cent of UK airports cannot instruct a receiving mail system to reject a message forged in their name.

> **Three suppliers in ransomware leak-site data, and no airport operator**
>
> A leak-site mention indicates the organisation has been named by a ransomware group. It is the single most consequential row in the table above and the only item in this report warranting same-week attention.
>
> It is reported prominently but deliberately not characterised further, because a leak-site listing can be stale, disputed, or concern a part of a corporate group with no UK aviation involvement. It is a trigger for a question, not a conclusion. The question is which UK airports use these three organisations, and what access those organisations hold.

What the comparison does not say

It does not say that suppliers are careless and airports are diligent. The operator cohort carries a statutory obligation, a named regulator and an assessment framework; most of the supplier cohort carries none of those. The most economical explanation for the gap is that regulation works, and that it currently stops at a boundary the risk does not respect.

7. The combined view: 94 distinct organisations

Because the two cohorts share no members, the combined population is 94 distinct organisations and the figures below are true sums rather than estimates.

Measure	Operators (43)	Suppliers (51)	Combined (94)
Average score	69.2	65.3	67.1
Median score	71	67	68
Good, 75 and above	37%	22%	29%
Needs improvement, 50 to 74	51%	65%	59%
At risk, below 50	12%	14%	13%
Risky service reachable	5%	10%	7%
Database port answering	2%	8%	5%
Cannot stop forged email	40%	33%	36%
No records in any credential bucket	44%	16%	29%
Employee credential records	**10**	**1,152**	**1,162**

Aggregating 94 organisations gives an average of 67.1, which is unremarkable. **That average is the least useful number in this report**, because it blends two populations that behave differently and hides the distribution carrying the risk. It is included so nobody has to derive it, then set aside.

> **Why the combined view still earns its place**
>
> Two findings exist only at the combined level and are invisible in either half alone. The first is the employee credential asymmetry in section 8: it is a ratio between the two cohorts, so neither report can state it by itself. The second is the shared platform dependency in section 10, which spans both estates and is recorded on the risk register of neither.
>
> Everything else in this section is better read in the source sections above.

The configuration baseline is a sector fact, not 94 failures

Gap	Organisations	Share
No opt-out signal support for privacy preferences	94	100%
No stated policy on which authorities may issue certificates	91	97%
No published route for reporting a security problem	90	96%
No enforced security for email in transit	86	91%
No DNS integrity protection	85	90%

A finding shared by 96% of a sector is not 90 individual failures. These are baseline settings a mature aviation estate would be expected to hold, and their near-universality makes them a candidate for coordinated guidance rather than 94 separate projects. **Ninety of 94 organisations publish no route by which a researcher can report a problem privately**, which is a substantial part of why findings in this sector surface publicly.

8. Credentials: three buckets, in order of consequence

Credential exposure is reported in three separate buckets. They describe different people, carry different consequences and are fixed by different parties, so **they are quoted independently and never added into a single exposure figure**. The three reconcile exactly to the provider's total on all 94 assessments, and are set out below in order of how much they matter, which is close to the reverse of their size.

Bucket	Who it concerns, and who can fix it	Operators	Suppliers	Combined
1. Employees	Staff accounts on the organisation's own domain. Fixed by the organisation, through reset, revocation and multi-factor authentication.	10 4 orgs	1,152 21 orgs	1,162 25 orgs
2. Outside services	The organisation's own work identities appearing on somebody else's platform. Fixed by the organisation, but through a reset on that platform.	44 10 orgs	1,167 27 orgs	1,211 37 orgs
3. Account holders	Members of the public holding an account on the site. Cannot be fixed by the organisation at all. Only the individual can act.	4,807 22 orgs	38,577 40 orgs	43,384 62 orgs
No records at all	**Organisations with nothing in any of the three buckets. A measured zero, not an absent answer.**	**19 (44%)**	**8 (16%)**	**27 (29%)**

Why the order matters more than the size

An employee record is a credential to the organisation's own systems. It is the one an attacker would use, the organisation issued it, and the organisation can revoke it this afternoon. It is the bucket that belongs at the top of a board paper.

An outside-service record is the same person's work identity on a third-party platform, an identity provider, a service desk, an expense or recruitment tool. Real, actionable, one step further out. It follows the employee bucket closely because a work address reused across platforms is how one compromise becomes several.

An account-holder record is a member of the public whose own personal device carried malware. It is not access to anything the organisation runs, nobody there can reset it, and it carries no weight in any score. It is a consumer-protection question rather than an access-control one, and ranks well below the other two.

What 'outside services' does not mean

It counts **the organisation's own email identities appearing on somebody else's platform**. It is **not** a count of suppliers holding credentials into the organisation, which is close to the opposite direction. In a report about supply-chain risk that inversion would assert exactly the thing this analysis has not measured, so the bucket is never described as a supplier count anywhere in this document. The platform breakdown is published on only some affected organisations, so it evidences the pattern rather than accounting for every record.

Bucket one: where the employee exposure sits

This is the result the whole study was built to test, and it is the reason assessing airports alone would have been misleading.

Where the 1,162 employee records sit	Records	Share
Suppliers, passenger processing	536	46%
Suppliers, ground operations	365	31%
Suppliers, equipment, airfield and platform technology	167	14%
Suppliers, security and assistance	75	6%
Suppliers, surface access, parking and lounges	9	1%
All 43 airport operators combined	10	1%
Total	**1,162**	**100%**

More than nine in ten of every exposed employee credential in UK aviation's public web estate, 92%, belongs to a supplier operating airside. The organisations running common-use check-in and boarding platforms, ground and cargo handling, and airfield and baggage systems account for 1,068 of the 1,162 records between them. The whole airport operator sector, plus every consumer-facing supplier in the cohort, accounts for nineteen.

1,152 / 1,162	**6 of 7**	**815**
of employee credentials belong to suppliers, which are 54% of the population	ground operations suppliers are affected, and 7 of 8 in equipment and platform technology	of the 1,152 supplier records sit with just three organisations

Two further points sharpen it. **These are not one bad apple in a healthy class, they are whole classes.** Six of the seven ground-operations suppliers are affected, and seven of the eight in equipment and platform technology. And **ground operations is also the weakest class by score**, at an average of 53.1 with no organisation in the top band and two of seven in the lowest. The class with the worst configuration is also the class with the second-largest employee exposure.

> **What this establishes and what it does not**
>
> These are public-source credentials associated with each organisation's own domain, most commonly harvested by malware on an individual's device. This assessment cannot see whether any credential is still valid, and none of this is evidence that any airport system has been accessed. We did not try, and could not have.
>
> What it establishes is that the material exists, in volume, against precisely the organisations whose access is worth most to an attacker. A credential from a ground handler or a check-in platform is worth considerably more than a credential from a parking reseller, and the measured distribution runs exactly the wrong way. That is a reason for each of these organisations to check, not a conclusion about any of them.

Buckets two and three: identities elsewhere, and the public

Outside services: 1,211 records across 37 organisations

Ten operators and 27 suppliers carry work identities on third-party platforms, 1,211 records in total. The volume is close to the employee bucket and the distribution is wider: **more than half the supplier cohort is affected, against just under a quarter of the operators**.

The action is different from bucket one and should not be confused with it. These credentials do not unlock the organisation's own systems, so revoking an internal account does nothing about them. They are a password-reset exercise on the platforms concerned, plus the harder governance question of how many third-party services staff have signed into using a work address, and whether anybody holds a list.

That question is worth asking precisely because the answer is usually no. An organisation that can enumerate its own systems frequently cannot enumerate the outside platforms its staff have registered on, and this bucket is the visible edge of that gap.

Account holders: 43,384 records, and a different problem entirely

The largest number in this analysis by an order of magnitude concerns members of the public. Sixty-two organisations across both estates carry account-holder records: 4,807 at the airports and 38,577 at the suppliers, **89% of the total sitting with suppliers** and concentrated in the consumer-facing classes that sell parking, lounges and transfers.

> #### Why the biggest number ranks lowest
>
> These are people who bought airport parking or a lounge pass, and whose own personal device was later infected with malware that harvested their saved passwords. The credential is theirs, on their machine. It grants access to a booking account and to nothing operational. Nobody at the airport or the supplier can reset it, and it carries no weight in any security score.
>
> It is reported here for two reasons and no others. It is a consumer-protection and notification matter in its own right. And 43,384 is not a number a board should first learn about from somebody else.

There is one point at which this bucket touches the rest of the report. The MAG disclosure of August 2026 concerned exactly this population, the people who had booked parking, a lounge or Fast Track. **Account-holder credentials and forged email in an airport's name are the two halves of the same attack**: the data to write a convincing message, and the absence of a control that would stop it being delivered. Section 9 covers the second half.

9. Impersonation and passenger trust

Thirty-four of the 94 organisations, 36%, do not instruct receiving mail systems to reject messages forged in their name. Seventeen of them are airports.

This matters more in aviation than in most sectors, and the reason is behavioural rather than technical. A passenger travelling next week is expecting email. They are expecting it about a car park booking, a lounge reservation, a flight time change, a disruption notice, a baggage query. A convincing message from a familiar airport name lands in an inbox that is already primed for it, and it is acted on quickly and without much scrutiny.

The MAG breach makes this concrete rather than hypothetical. Approximately 8.7 million records of email addresses, phone numbers, vehicle registrations and postcodes, tied to specific bookings at specific airports, are now in circulation, alongside the 43,384 account-holder credential records in section 8. **That data is exactly what is needed to write a convincing forged message**, and the control that stops it being delivered under the airport's own name is a published policy that costs nothing to set.

> **The cheapest item in this report**
>
> Publishing an enforcing email policy requires a change to one DNS record. It touches no operational system, no airline system and nothing airside. It is externally verifiable, so an airport can confirm its own status in under a minute and so can anyone else. Seventeen UK airport operators and seventeen suppliers have not done it.

Near-universal findings are a capacity signal

When a gap appears in 90% or more of a sector, it stops describing individual organisations and starts describing the sector's shared assumptions about what is standard practice. Five of the baseline gaps in section 7 are in that territory, and the security-contact route is the starkest: **only four organisations out of 94 publish one.**

The practical consequence is that a researcher who finds a problem at a UK airport or one of its suppliers has, in almost every case, no obvious way to tell them privately. Findings then surface in public, which is worse for everyone including the passenger. A single file on a website fixes it.

10. Concentration: two kinds, both invisible

Two forms of shared dependency run through this sector. Neither appears on any individual organisation's risk register, and both would spread an incident across organisational boundaries.

One website, eleven airports

Within the operator cohort, one website serves eleven Highlands and Islands airfields and another serves two Channel Island airfields. This is sensible and almost certainly better resourced than eleven separate estates would be. It also means a single finding, a single outage or a single compromise reaches eleven airports at once, and that any percentage in this report understates or overstates the passenger consequence depending on which of the thirteen websites it falls on.

The rule this report follows throughout is that **a website count and an airport count are always given together**. One is the size of the remediation job. The other is the size of the exposure. Using either alone produces a misleading sentence.

A shared platform underneath both estates

Fifty-three of the 94 organisations, 56%, serve their websites through a large content-delivery or reverse-proxy provider, 53% of the operators and 59% of the suppliers.

There are two consequences and the second is the more important. **For the analysis**, port and service findings on a fronted website must be read as observations of a platform the organisation neither owns nor can change; treating them otherwise attributes to an airport a surface it cannot correct. Three findings across the combined population are attributable to that shared layer rather than to the organisation named, and are identified as such.

For governance, a majority of UK aviation's public web presence, both the airports and their suppliers, rests on a small number of shared platforms. That is normal, sensible and probably safer than the alternative. But it is a dependency the sector holds in common, it is invisible on any individual organisation's risk register, and a serious incident at that layer would not respect the boundary between an airport and its supply chain. No document reviewed for this analysis records it as a sector-level dependency.

> **The supplier layer contains its own concentration**
>
> The dependency map behind the supplier cohort shows the same pattern one level down. A single airport ecommerce platform sits behind the parking and ancillary booking of five UK airports in the operator cohort, one of which is itself the eleven-airport website. Ground handling across the large UK airports is effectively four names. Special assistance at the two largest London airports is three.
>
> None of this is unusual or improper. All of it means that the number of independent points of failure in UK aviation is considerably smaller than the number of organisations.

11. Recommended order of work

Ordered by consequence rather than by ease. Items 1 and 2 cross the boundary between the two estates, which is why they belong in a combined report rather than in either half.

1	**Establish which airports use the three ransomware-mentioned suppliers, and what access they hold** The only item in this report warranting same-week attention. Verify whether the mention is current and what the organisation's UK aviation connection actually is before drawing any conclusion.
2	**Ask ground-handling, passenger-processing and airfield-technology suppliers what credential hygiene they operate** Three classes hold 1,068 of the 1,162 employee records, and in two of them almost every organisation is affected. The question is answerable without a security specialist on either side.
3	**Publish an enforcing email policy** Thirty-four organisations across both estates, seventeen of them airports. One DNS record, no operational system touched, externally verifiable in under a minute.
4	**Publish a security contact route** Ninety organisations have none. A single file on the website gives a researcher somewhere to send a finding privately instead of publicly.
5	**Reset and rotate the employee credentials, bucket one first** Prioritise the three supplier organisations accounting for 815 of the 1,152 supplier records. Reset, revoke sessions and confirm multi-factor authentication on every affected account.
6	**Work through the outside-service records, and find out what staff have signed into** 1,211 records across 37 organisations, resolved by resets on the third-party platforms concerned. The governance half of the job is establishing which outside services staff use a work address on, which most organisations cannot currently answer.
7	**Validate the twelve lowest-band websites privately** Five operators and seven suppliers. Confirm each finding is live before any of it is treated as fact or disclosed.
8	**Close the reachable services and database ports** Seven organisations, not twelve: five carry both findings, so those rows describe overlapping sets. Exclude the three attributable to a shared platform first.
9	**Record the shared-platform dependency as a sector-level risk** Establish who at each organisation would be told if that layer had an incident, and settle the twelve uncertain operator attributions so a disclosure reaches the right organisation.
10	**Adopt the section 7 baseline as a sector standard** Coordinated guidance rather than 94 separate remediation projects. Inexpensive, externally verifiable, no operational risk.

Conclusion

Assessing airports alone would produce a materially misleading picture of UK aviation's exposure. The operator estate is respectable: an average of 69.2, credential volumes an order of magnitude below most sectors this firm has measured, and nothing at all in ransomware, known-breach or browser-safety data. A board or a regulator reading only that half would reasonably conclude the sector is in reasonable order, and would be reading a fair account of the wrong thing.

Adding the 51 organisations that airports depend on moves every risk indicator in the same direction, and moves the employee credential figure by two orders of magnitude. It also relocates the finding. The exposure is not spread thinly across a supply chain; it has collected in three classes that operate airside, in two of which nearly every organisation is affected.

> **The structural finding**
>
> The risk does not sit where the accountability sits. Airports carry the regulatory obligation, the public name and the passenger relationship. Nine in ten of the suppliers holding the exposure are independent third parties over which an airport has contractual influence and nothing more.
>
> That gap is not a failure by anybody in this study. It is a boundary drawn in 2018 around a risk that has since moved across it, and the Cyber Security and Resilience Bill is the mechanism for redrawing it.

The cheapest fixes are also the largest gaps. Email authentication, a security contact route and the transport-security baseline account for most of the distance between this sector and a good score across both estates, and none of them requires touching an operational system, an air traffic system or anything airside. That is an unusually favourable position: the work is inexpensive, externally verifiable and carries no operational risk.

Two things this analysis deliberately does not claim. It does not claim any airport system has been accessed. It could not see inside one and did not try. And it does not rank organisations: the value is in the class-level pattern, and a league table of named estates would be both less useful and unsafe to circulate.

About this report

This analysis was conducted using the MyDomainRisk.com analysis tool, a solution developed by Huro Data Technologies Ltd. Every observation was made externally using information available from public websites, DNS, certificates, public threat intelligence and publicly reachable services. Nothing was logged into, no password was tried and no vulnerability was exploited.

How to read the figures

Bands and what a score is

Good is 75 and above, *needs improvement* is 50 to 74, and *at risk* is below 50. A single serious finding can hold a website below a band ceiling regardless of how much else is correct. **A score of this kind is a floor, not a verdict.** It records what could be seen from outside on one day, not internal controls, operational technology, air traffic systems, baggage or screening systems, patch governance, incident readiness or regulatory compliance.

Two denominators, both stated

Website counts size the remediation work; airport counts size the exposure. Where this report gives an airport figure it is because one website serves several airports, and the multiplier is stated in the same sentence.

Counting

Every prevalence figure counts **organisations, not findings**. An organisation with five instances of the same issue counts once. Percentages are of the 43, 51 or 94 assessed websites as each row states, and rows within a table are different views of the same evidence that must not be summed. The two populations do not overlap, so combined figures are true sums rather than estimates. We report distributions and counts and do not publish a league table, because summing findings gives equal weight to observations that are not comparable.

Floors, not readings

On three of the 94 websites the homepage did not fully serve, so part of the assessment could not run. For those three the true score can only be the same or higher, never lower. They are included in every figure and their position is provisional rather than a finding against the organisation.

Small classes are merged

Five dependency classes in the supplier source data contain three organisations or fewer, and are reported together as *equipment, airfield and platform technology* so that no line describes a single identifiable company. Supplier inclusion reflects a publicly evidenced dependency, not a contract, and no claim is made about any airport's current suppliers. The classification is editorial and is not a security measurement: where a supplier's class is arguable the score is unaffected, but its position in the class tables would move.

> **Publication rule**
>
> Do not describe an individual airport or supplier as 'at risk' on the strength of this kind of assessment alone. Every consequential finding requires private validation by the organisation first, and automated defences that refuse a scanner are themselves a security control.

Interpretation notes

- Every figure describes the single assessment of 2 September 2026. No trend against an earlier run is reported and none should be inferred.
- The three credential buckets are quoted independently and never summed. Account-holder records are not scored and relate to travellers, not to operator or supplier infrastructure.
- Twelve operator attributions in the source cohort are marked uncertain and are reported as such rather than resolved silently.
- A zero in this report is a measured zero, meaning the check ran and found nothing, never that a check failed to produce an answer.

Sources and notes

[1] Manchester Airports Group data security incident, disclosed 27 August 2026

Approximately 8.7 million passenger records taken across Manchester, Stansted and East Midlands: email addresses, phone numbers, vehicle registrations and postcodes from car park, lounge and Fast Track bookings and airport wi-fi sign-ups. No payment details accessed. MAG stated it had contained the risk, that passenger safety and aviation security were not compromised, and that operations were unaffected. Reported by International Airport Review and Aviation Business News, 27 and 28 August 2026.

[2] Collins Aerospace MUSE ransomware, September 2025

Ransomware against Collins Aerospace check-in software disrupted London Heathrow, Brussels, Berlin and Dublin from 19 September 2025, with boarding passes failing at gates and airlines reverting to manual check-in; disruption at Heathrow continued to 23 September. RTX confirmed the ransomware in an SEC filing and ENISA confirmed it publicly. The National Crime Agency arrested a man in West Sussex under the Computer Misuse Act on 23 September 2025; he was released on conditional bail. Reported by TechCrunch and Cybersecurity Dive, 24 September 2025.

[3] National Cyber Security Centre

Vulnerability disclosure toolkit; *Email security and anti-spoofing*, including staged DMARC implementation from monitoring-only to enforcement; *External attack surface management*; *Multi-factor authentication for corporate online services*; *10 Steps to Cyber Security*. Free plain-English guidance requiring no specialist security team.

[4] The Network and Information Systems Regulations 2018, SI 2018/506; Civil Aviation Authority; NCSC Cyber Assessment Framework

UK airports are designated critical national infrastructure within the statutory NIS regime. The Civil Aviation Authority is the competent authority for the air transport sector and assesses operators against the NCSC's Cyber Assessment Framework.

[5] DSIT, *Cyber Security and Resilience Bill: policy statement*, 1 April 2025; UK Parliament Bill 4035

The Bill amends the NIS Regulations, which cover transport, energy, drinking water, health and digital infrastructure, and extends the regime to managed service providers and designated critical suppliers. Air transport is one of the five sectors already in scope.

[6] MyDomainRisk / Huro Data Technologies Ltd. *UK airport operators, external security posture, full assessment, 2 September 2026*

Source cohort one. External assessment of the 43 websites representing 54 UK airports; methodology, scoring caveats, coverage and all measured findings reported in sections 4 and 6 of this report.

[7] MyDomainRisk / Huro Data Technologies Ltd. *UK airport suppliers, external security posture, full assessment, 2 September 2026*

Source cohort two. External assessment of 51 organisations providing services into UK airports, with dependency classification, passenger-data status and ownership category taken from a supplier dependency map compiled from operator websites, vendor client lists, published contract reporting and incident reporting.

[8] MyDomainRisk / Huro Data Technologies Ltd. *UK aviation web estate, combined analysis, 2 September 2026*

The consolidation of cohorts one and two reported in sections 7 to 10. Every figure in this report and in both source assessments is produced by one measurement routine over the same records, so the per-estate views and the combined view cannot disagree with one another. Every field the analysis reads was proven present before any count was taken; the routine refuses to report rather than allow a failed lookup to be counted as a measured zero.

Provenance and disclosure

This analysis was produced with MyDomainRisk, a product of Huro Data Technologies Ltd, which has a commercial interest in the analysis, declared here so that readers can weigh it. It is not independent certification, an audit, legal advice or regulatory advice.

No organisation is named in this report. The findings are aggregate by design: a named estate beside its weakness is a document that cannot safely be circulated, and the value of this analysis is in the sector pattern rather than in any individual result. Per-organisation detail exists and is available privately to the organisation concerned, or to a party it authorises.

Every named finding should be rechecked immediately before responsible disclosure, because public-facing configuration changes continuously. Aggregate figures may be used with the cautions in this report. This document contains aggregate counts only, no passwords, personal credential records, raw provider records, exploit instructions or named organisation detail.

A note on scope, stated once more because it matters in this sector: this assessment covered public websites, DNS, certificates and publicly reachable services. It did not touch, test or assess any operational technology, air traffic management system, airline system, baggage system or security screening system, and makes no claim about any of them. A finding is not evidence that any organisation has been compromised. Credential findings commonly originate from malware on an individual's device and may concern an outside service where a work email address was used.