

Bridewell

Cybersecurity. **Where it Matters.**

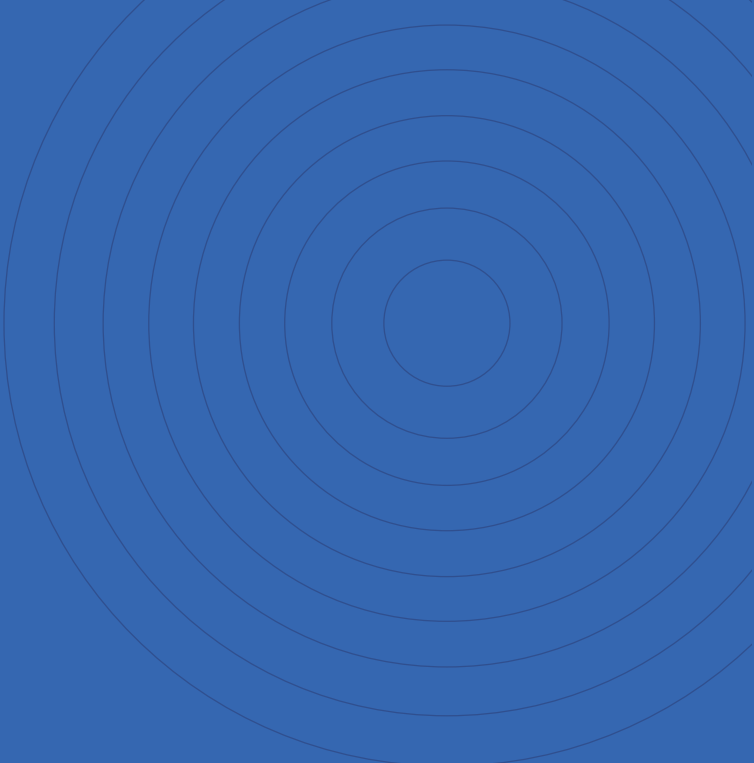
Cybersecurity in Aviation: 2026

Turning risks into a runway for cyber resilience



Contents

Foreword	3
Executive Summary	4
The Scale of the Threat	5
Impact and Cost	6
An Industry Exposed?	7
Perception and Experience	8
AI as a Threat	9
AI as a Line of Defense	10
Rising Budgets, Scarce Skills	11
Getting to Grips with Regulatory Compliance	12
Looking Forward	13



Foreword

// The aviation industry has changed dramatically over the past two decades, and it's now fundamentally dependent on interconnected digital systems. This increased interconnectivity has brought massive improvements for airlines, airports, and passengers. Airlines and airports operate more efficiently, sophisticated systems help manage growing demand, and data can be shared in real time. However, this also widens the attack surface, creating more opportunities for cyber criminals to exploit.

Airlines, airports, manufacturers and suppliers now all operate on interconnected technologies so cyber resilience cannot be achieved by individual organizations working in isolation.

We commissioned this research to get a first-hand account of what cybersecurity professionals in the aviation industry are experiencing, what they're investing in and changes in their priorities.

What we're seeing is that the aviation industry is under sustained pressure and experiencing significant financial losses as a result. At the same time, organizations are also having to balance immediate threats with longer-term concerns around skills shortages, changing regulations, and emerging technologies.

As artificial intelligence, automation, and increasingly connected infrastructure continue to reshape aviation, understanding the industry's cyber maturity is essential. This report provides insight into how organizations are responding, where priorities are changing and where further focus will be needed to build a resilient aviation sector for the years ahead. //

Kelechi Onyedebelu,

Director Security Solutions Presales at Bridewell U.S

Executive Summary

Successful cybersecurity breaches in the aviation industry threaten to cause immediate and wide-scale disruption. Few other industries carry a comparable risk profile.

A single compromised system can threaten public safety and organizational sustainability by grounding fleets, stranding passengers and spreading almost instantly through a connected network of airports, airlines, and handlers.

This potential for damage and disruption attracts a virtually unparalleled range of malicious actors. Financially motivated criminal groups, state-sponsored actors, and hackers are just some of those seeking to capitalize on the vast attack surface and data available through a successful breach.

Bridewell surveyed 250 cybersecurity professionals in the aviation industry to understand the impact of risks and breaches on their operations. The findings reveal a varied and volatile threat landscape.

Our 2026 report uncovers:

- **100% of respondents** reported **financial losses** as a result of a breach in the last 12 months
- **Mean losses** from an attack or breach were **\$1,433,059**
- **46% of respondents** reported an increase in the volume of attacks against their organization in the past 12 months
- **88% of respondents** experienced **malware, credential theft** and **DDoS attacks**
- **Compromised credentials** were the most common attack entry point (**30%**)



The Scale of the Threat

It's not so much the innovation of attacks on aviation organizations that poses a significant threat as the sheer volume.

Phishing was the most prominent attack type, with 90% of respondents reporting at least one attack in the past 12 months and organizations suffering a mean of 3.85 phishing attacks during the past 12 months. Malware, credential theft, and DDoS attacks were also widespread, with 88% of respondents experiencing at least one of each. Organizations also detected and stopped a mean of 3.82 nation-state or APT attacks.

Almost half (46%) of respondents reported that the volume of attacks against their organization has increased in the last year, compared with just 28.4% reporting a decrease.

Effective defense depends on knowing where attackers are actually getting in, not just where an organization looks vulnerable. Compromised credentials were the most common entry point for 30% of respondents, followed by phishing or social engineering at 27.2%.

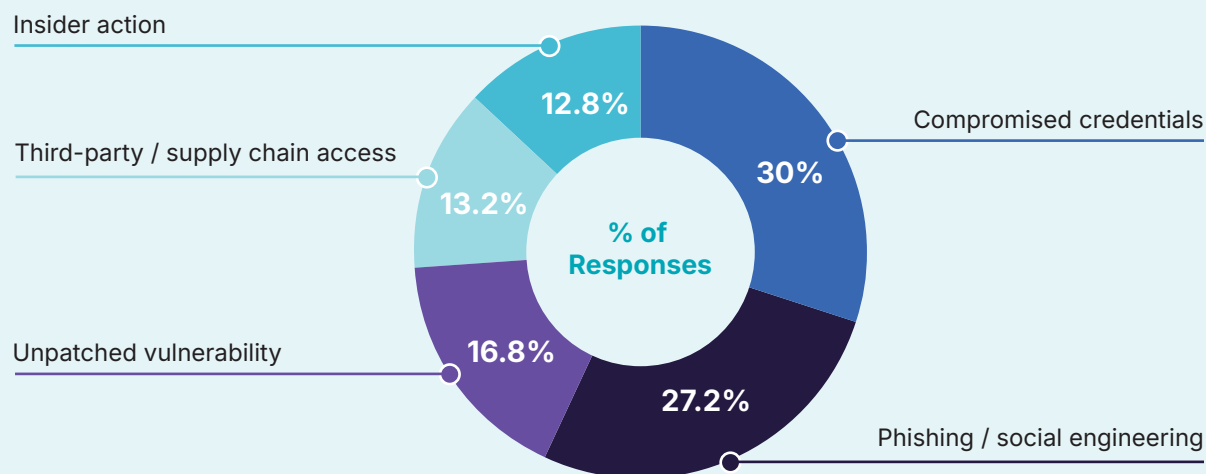
3.85

The number of phishing attacks experienced per organization in the past 12 months

3.82

The number of nation-state or APT attacks detected and stopped per organization

Primary Entry Point for Most Significant Attack (Past 12 Months)



Impact and Cost

Considering the volume of attacks alone risks underestimating the problem facing organizations. In the aviation industry, a single successful breach can cause lasting damage, with immediate operational disruption turning into significant financial losses.

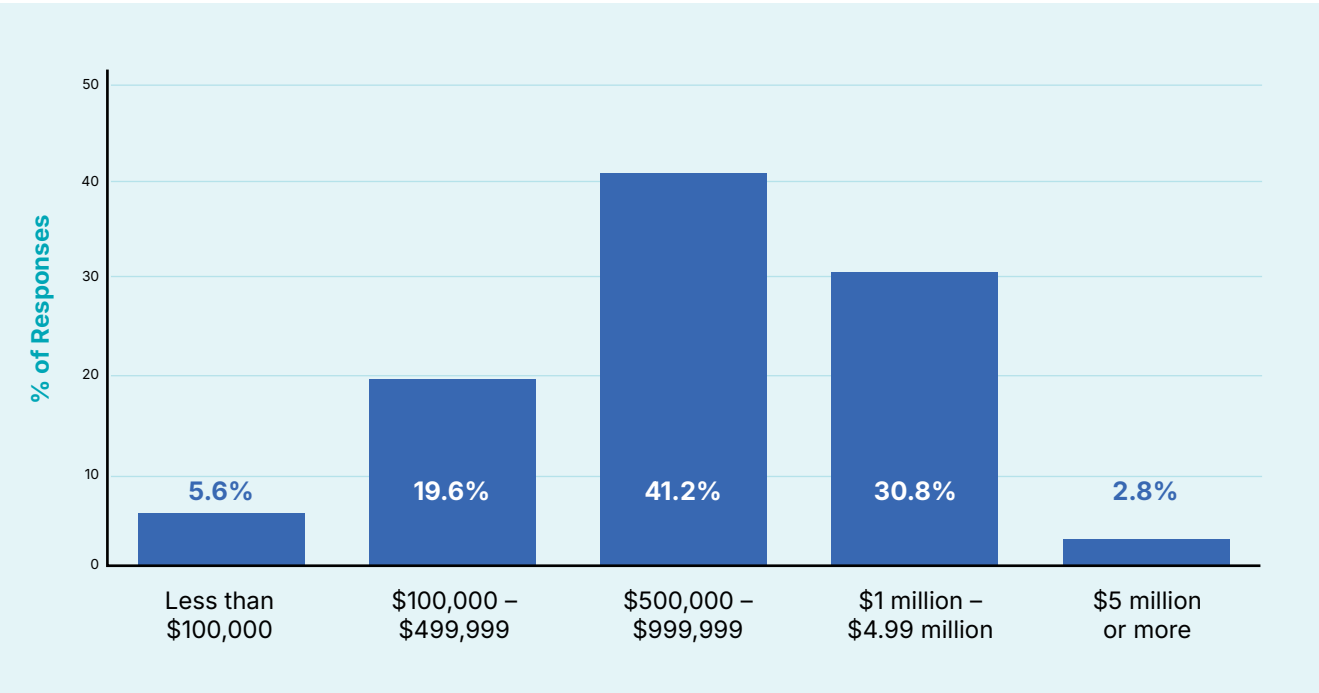
Almost half of respondents (45.2%) described their most significant attack as having a high or critical impact on their organization, while 40% rated it as moderate and just 14.8% said it caused a low or negligible impact.

Beyond delays, disruption, and damage to reputation, 100% of respondents also reported experiencing a financial impact from an attack or breach during the past 12 months.

100%
of respondents reported a financial impact from an attack or breach in the past 12 months

\$1,433,059
Mean estimated financial impact of an attack or breach

Total Estimated Financial Impact of Cyber Incidents (Past 12 Months)



An Industry Exposed?

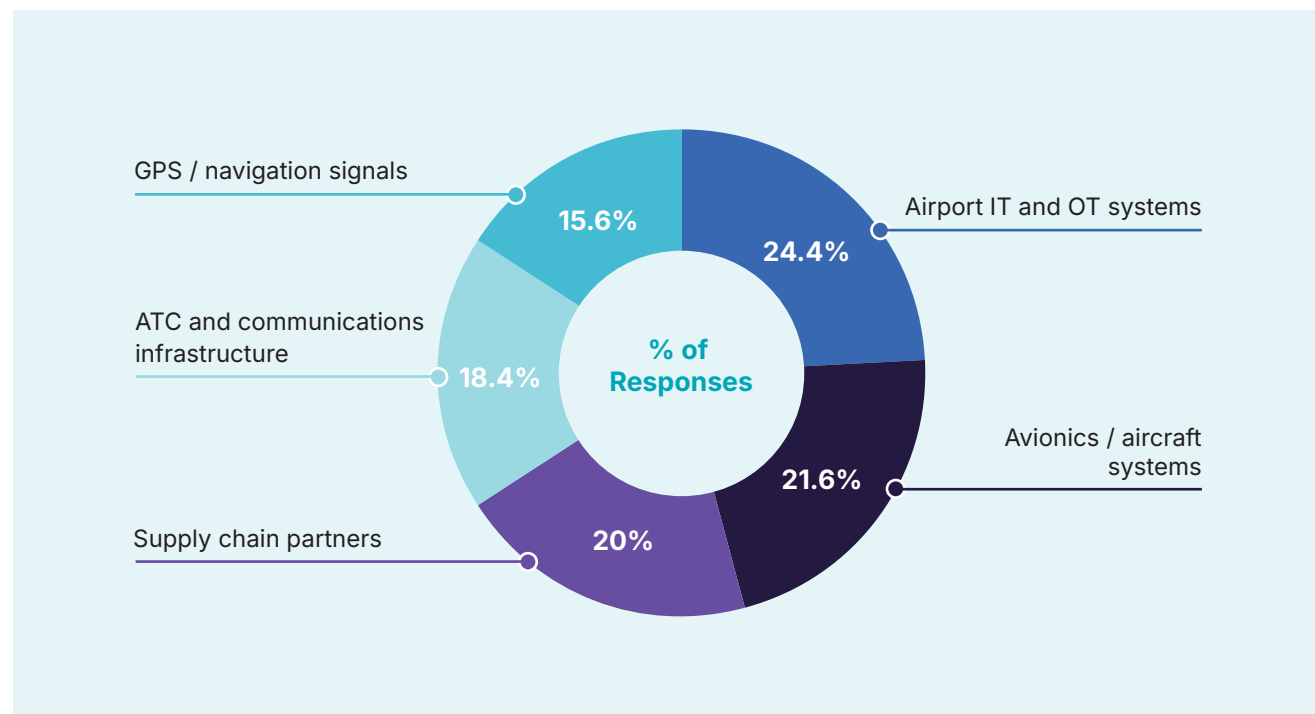
For aviation organizations, the attack surface is both broad and costly to defend, spanning corporate IT, operational technology, avionics, and passenger processing systems, as well as suppliers and handlers.

This also makes it difficult to deploy proactive fixes or patches without causing further disruption. So, understanding which systems represent the biggest threats becomes more important.

Respondents cited airport operational infrastructure and supply-chain partners as their greatest cybersecurity concerns, with 60% of respondents very or extremely concerned about cyber threats to each area.

Looking ahead to the next 24 months, airport IT and operational-technology systems rank as the highest perceived risk targets (24.4% of respondents). Avionics and aircraft systems ranked second (21.6%), ahead of supply-chain partners (20%).

Highest-Risk Aviation Asset (Next 24 Months)



Perception and Experience

Questioned on the aviation-specific cyber attacks their organization has faced over the past 12 months, respondents cited cyber interference with facilities or building-management systems as the most common (34.4%).

Almost a third of organizations (30.8%) reported attempted compromise of ground-support-equipment tracking or airside vehicle-management systems. Just over a quarter of organizations reported phishing or social engineering attacks targeting airport operations staff (27.6%) and interference with CCTV or video surveillance systems (26%) in the past 12 months.

Unauthorized access to passenger data or departure-control systems was the least common aviation-specific incident reported (18.8%).

But perception and reality don't always align. Facilities and building-management systems top the list of incidents experienced, yet just 52% of respondents were very or extremely concerned about this risk. Fewer than 60% of respondents named airport operational infrastructure and supply-chain partners as their greatest concerns.

“ 34.4% of respondents named **cyber interference with facilities or building-management systems as the **most common aviation-specific cyberattack** in the past 12 months ”**

AI as a Threat

AI has arguably proved no more transformational anywhere than in cybersecurity, reshaping the fight on both sides. The same capabilities that empower cybersecurity professionals to spot anomalies at speed and automate responses can also enable attackers to widen the scope and scale of their attempts.

Cybersecurity professionals in aviation are alert to the scale and severity of AI-enabled threats. AI-generated phishing and social engineering topped the list of their fears, with 63% of respondents very or extremely concerned about this threat. AI-accelerated vulnerability discovery is also cause for concern among cybersecurity professionals with 61% reporting they are very or extremely concerned about this threat.

Deepfake audio or video used for fraud and impersonation ranked as the lowest concern, with almost a fifth (18%) of respondents saying they were not at all or only slightly concerned.

“ 63% of respondents reported that AI-generated phishing and social engineering are the most concerning AI-enabled threats ”



AI as a Line of Defense

Despite widespread concern over AI's potential to increase the scope and power of cyber attacks, professionals in the aviation industry are also seeing the opportunity to harness the technology for their benefit.

Over two-thirds of respondents (70.8%) revealed that their organization has adopted AI or machine learning for cyber defense in some capacity. This ranges from pilots to broad deployment. Over a quarter (28.4%) are evaluating the use of AI for cyber defense, while just 0.8% were not exploring it at all.

But it's not as simple as deploying AI to support or even replace existing efforts. Aviation technology often makes AI deployment more difficult than in other critical national infrastructure (CNI) sectors. This was echoed by respondents, who cited integration with legacy systems as the most common barrier to adoption (23.2%).

Interestingly, lack of trust in AI outputs was the least commonly cited barrier (8.4%), despite the fact that the same professionals confessed to fearing AI in the hands of malicious actors.

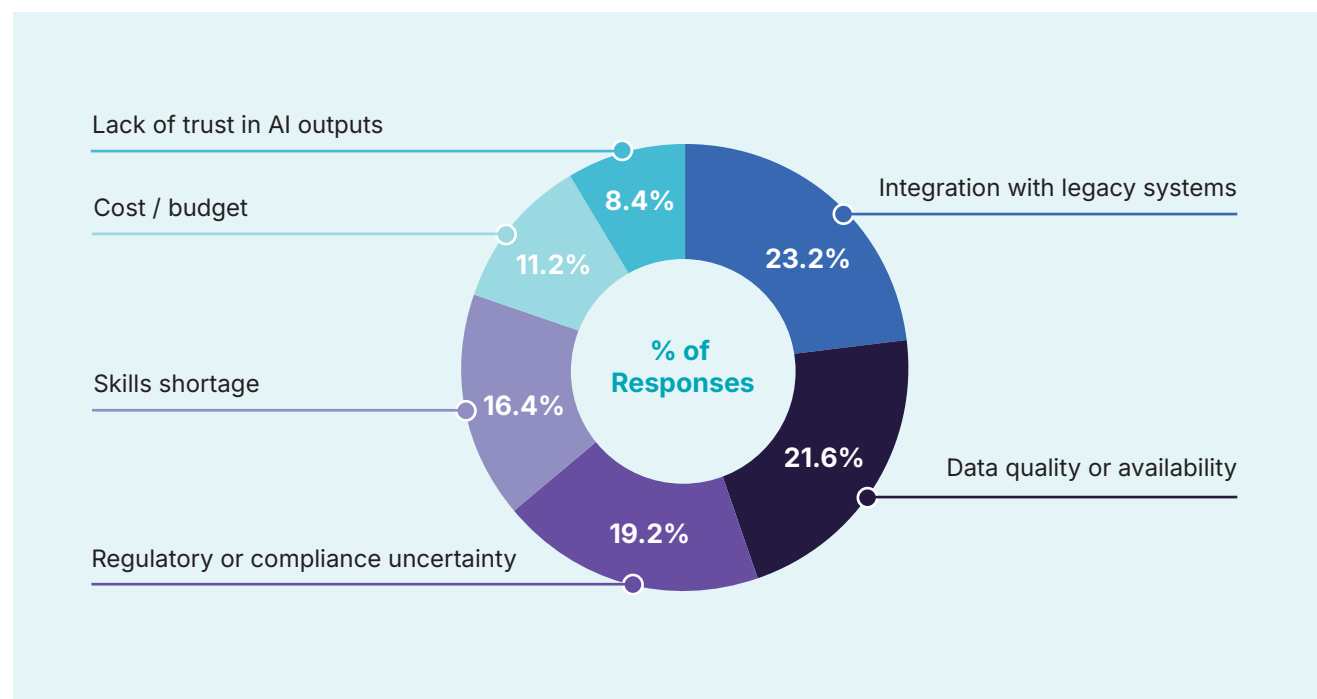
7.6%

Proportion of organizations that have widely deployed AI for cyber defense

23.2%

Proportion of organizations that cite integration with legacy systems as the biggest barrier to adoption

Biggest Barrier to AI Adoption for Cyber Defense



Rising Budgets, Scarce Skills

In an industry defined by thin margins, investment reveals a lot about the priorities of aviation businesses. And it's unsurprising that there is a trend towards increasing cybersecurity budgets.

Over three-quarters of respondents (77.6%) reported an increase in cybersecurity budgets during the current fiscal year. For 44.8% of respondents, their budget had increased by between 1–10% while 7.2% reported budget increases of over 25%. Just 10.8% said budgets had remained flat, while 11.6% reported a decrease.

It's one thing increasing budgets and another investing in the right skills and capabilities. Cybersecurity professionals noted difficulty in finding a range of skills. AI and machine-learning security was noted as the hardest skill to find (40.8%), followed by aviation-specific regulatory expertise (39.6%) and governance, risk and compliance skills (36.4%). Incident response and forensics (33.6%) and cloud security (32.4%) were close behind, with most respondents selecting several areas of expertise that are difficult to find.



Getting to Grips with Regulatory Compliance

Cybersecurity represents more than a box-ticking exercise in aviation. Few industries are as heavily regulated, and few risk such significant disruption and financial harm. Practices that were once voluntary are now regulatory requirements, and aviation organizations are moving to demonstrate compliance.

Two-thirds of respondents (67%) said their organization was substantially or fully compliant with the NIST Cybersecurity Framework, and a similar proportion (66%) reported substantial or full compliance with the CISA Cybersecurity Performance Goals.

However, participation in information-sharing initiatives is far lower. Just over a third (35.6%) of respondents are active members of the Aviation ISAC, while just 26% are involved in CISA programs.

And 18% had either not started preparing for, or were still planning how to meet, the requirements of the FAA Reauthorization Act.



Looking Forward

Cybersecurity in Aviation: 2026 shines a light on an industry under pressure, but one increasingly motivated to meet its responsibilities.

The volume and scope of cyber attacks on aviation organizations are increasing. And every organization surveyed suffered financial damage as a result of an attempted or successful breach. Cybersecurity threats are also causing significant disruption, and the long-term implications on consumer confidence and financial sustainability are yet to be seen.

But there is cause for optimism. Aviation cybersecurity teams understand where they're exposed, budgets are moving in the right direction, and the sector is demonstrating a willingness to embrace the defensive capabilities of AI.

Looking ahead, cybersecurity professionals in aviation must tackle the disparity between perceived risk and legitimate threat. This will likely require extensive testing based on logged threats rather than focusing resources on proactively preparing for perceived risks.

There may also be a shift in investment, with an increased focus on training and upskilling cybersecurity talent to plug the capability gaps noted by a significant proportion of respondents.

Organizations that are able to convert their investment into demonstrable operational resilience will be the ones least disrupted in the years to come.



Bridewell

Cybersecurity. *Where it Matters.*



+1 646 396 5603



hello@bridewell.com



bridewell.com/us