2026

AVIATION ISAC

CISO SURVEY RESULTS

CONTENTS

EXECUTIVE SUMMARY

The Aviation ISAC is proud to present the 9th edition of our Annual CISO Cyber Risk Survey.

The purpose of the survey is to provide a tool for industry Chief Information Security Officers (CISO's) and Chief Product Security Officers (CPSO's) to benchmark their strategies, program maturity, and management of resources against those of their industry peers.

Each year the results of the survey provide unique insights into how shifts in technology and the behaviors of attackers impact the strategies of network and product defenders. Clearly, the rapid rise in the use of artificial intelligence (AI) has strongly impacted the lives of CISO's and CPSO's. And as much as things change, the survey showed that in many instances, the priorities stay the same. For example, each year Identity Management, Authentication and Access Control (IAM) has been the number one focus. For 2026, we heard that Agentic AI was a significant challenge for security officers. So as IAM continued to be the number one area of focus, many of the new IAM initiatives were triggered by concerns which were born from the many ways AI has been integrated into applications, networks, and products.

Governance has continued to rise as a priority in the daily lives of security officers. Similar to IAM, most of the governance challenges noted for the coming year were directly tied to the increased integration of AI across aviation business operations.

In 2025, we saw how an attack on a key supplier to many companies in the industry can have a magnifying impact across the aviation ecosystem. Analysis of the survey results revealed these types of attacks were clear drivers for increased initiatives to address supply chain risk.

Also in 2025, we saw targeted attacks on aviation companies wherein the same techniques were used by attacker groups against many companies. Shortly after these campaigns were initiated our community rose to the challenge. The power of information sharing ensured the community was aware of the current methods and tools of the attackers. The information sharing was directly responsible for reducing the ability of the attackers to successfully use these techniques against other companies.

We sincerely thank all the CISO's and CPSO's who participated in this year's survey. Your willingness to lean forward and share your challenges and insights improves the awareness and capabilities of everyone who has a role in protecting aviation operations.

Thanks for all you do in keeping aviation safe and secure.

Jeffrey Troy
President, CEO
Aviation ISAC

THREAT LANDSCAPE

Over the past decade, cyber threat actors have demonstrated an ability to negatively impact the global commercial aviation system. Airline and airport operators, aircraft manufacturers, satellite companies, and the complex aviation supply chains that support them will continue to be targeted. This quarterly assessment by the Aviation ISAC provides an analysis of the risk posed by various types of malicious cyber incidents impacting the commercial aviation sector.

- In Q4 2025, there were a total of 26 cybersecurity incidents that may have impacted the global commercial aviation sector, of which at least 6 incidents affected an Aviation-ISAC Member Company (MC). Malicious cyber activity in Q4 2025 was less than the scale and impact of incidents observed in Q3 2025.
- Three types of cyberthreat actors are targeting the commercial aviation sector: organized cybercriminal groups, hacktivists and Advanced Persistent Threat (APT) groups.
- The Aviation ISAC assesses that due to their frequent use of zero-day exploits, sophisticated evasion techniques and targeting of global telecom providers, China-based APT groups are likely to pose the greatest long-term cybersecurity risk to the global commercial aviation sector and its associated software supply chains. However, on an average daily basis, cybercriminal groups represent the most pervasive cyberthreats.
- In terms of significant trends, cyber threat actors are continuing to improve their ability to avoid traditional signatures-based intrusion detection systems and maintaining network persistence through living-of-the-land (LOTL) tactics.
- Cybercriminal actors such as “Scattered Spider,” UNC6040 and others associated with “the Com” cybercriminal telegram channel have demonstrated strong reconnaissance skills, often targeting IT support teams and employees directly through phone calls and social engineering campaigns to gain initial access.
- High regional tensions in Eastern Europe, the Mideast and the Far East regions serve as driving forces behind increased malicious cyber activities emanating from these areas. In addition, regional conflicts have led to an increase in GPS jamming/spoofing and other hybrid-style operations have impacted commercial aviation flights.
- Despite 26 reported/claimed cyber incidents in Q4 2025, no Aviation ISAC MC suffered significant operational disruptions due to malicious cyber activity in this quarter.

SURVEY RESULTS

How do we collect the data?
Each year we survey CISO's and CPSO's in our community to understand their strategies for cyber risk reduction heading into the new year. The survey poses just one question, "What are 3-5 things you committed to getting done in 2026 to reduce cyber risk within your organization?"

How do we analyze the data?
The responses are catalogued using the National Institute of Standards and Technology's Cybersecurity Framework (NIST CSF 2.0). A record 65 member companies participated in the annual survey. The question posed seeks to elicit the hurdles our members are addressing as they create a more secure environment for their networks - OT, IOT, and product development. We tabulated and analyzed the results from several perspectives. We looked at overall responses by function (Governance, Identify, Protect, Detect, Respond, and Recover), category, and sub-category.

What did we learn?
At the highest level, in comparing the survey results from 2025 to 2026, we learned some significant shifts in focus occurred as aviation cybersecurity teams headed into 2026. Comparing the data from 2025 & 2026 revealed a drop in the overall percentage of projects aligned under the Protect function heading into 2026. Importantly though, Protect remained the area of the most focus for CISO's. Although there was little change in the percentage of initiatives and resources dedicated to governance, many CISO's noted plans to improve governance over AI applications. Although there was a 7% decline in projects focused on Detect, many CISO's mentioned either upgrades to their Security Information and Event Management (SIEM) or a planned change in vendor. These projects were to take advantage of AI enhanced SIEM platforms.

The NIST CSF has significantly less categories and sub-categories in the respond and recover functions. As expected, we saw less initiatives in these areas in both 2025 and 2026.

CISO FOCUS BY NIST CSF FUNCTIONS

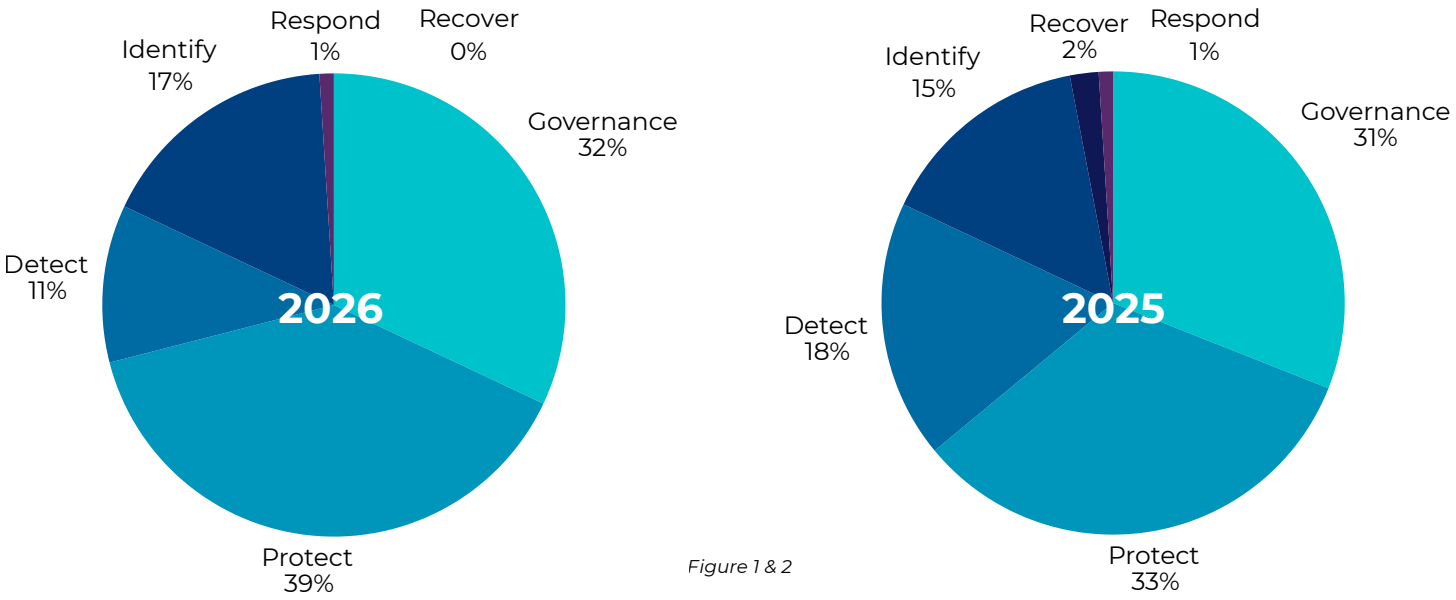

Figure 1 & 2

TOP 5 CATEGORIES OF RISK REDUCTION EFFORTS

1. Protect: (AA) Identity Management, Authentication, & Access Control
2. Governance: (OC) Organizational Context
3. Governace: (SC) Cybersecurity Supply Chain Risk Management
4. Protect: (DS) Data Security
5. Protect: (IR) Technology Infrastructure Resilience

Identity Management, Authentication, & Access Control, under the Protect function, is the year over year number one category of focus. Many larger organizations, particularly those dealing with legacy systems, acquisitions, social engineering hacks, and agentic AI are in search of simplification and security.

In line with the 2025 survey results, Organizational Context, under the Governance function, was the second most mentioned area of focus. This highlights the importance of cybersecurity as a discipline which must be embedded across all aspects of aviation companies, regardless of whether a company is an airline, airport, original equipment manufacturer (OEM) or service provider.

Supply Chain Risk Management was the second highest area of focus in 2024. In 2025, it dropped to the fourth highest priority and heading into 2026, it moved back up a notch to number three. This reflects the impact seen from cyber attacks against common, key suppliers in 2025.

Two additional categories under the Protect Function also made the top areas of focus. Coming in at number four was Data Security. This is a clear reflection of the swift impact AI is having on aviation. AI's ability to aggregate data and crawl across networks is an emerging concern.

The fifth most mentioned area of focus was Technology Infrastructure Resilience. A diverse number of initiatives to include network segmentation, cloud resilience, and other defense in depth projects were mentioned.

As in prior years, we will conduct a deeper dive into the categories, sub-categories and specific projects mentioned by the respondents

Protect: Identity Management, Authentication, and Access Control

AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	40%
AA-01: Identities and credentials for authorized users, services, and hardware are managed by the organization	30%
AA-03: Users, services, and hardware are authenticated	20%
AA-04: Identity assertions are protected, conveyed, and verified	10%

Figure 4

As detailed in Figure 4, The respondents identified initiatives in four of the subcategories for IAM. The most heavily weighted in the subcategory 5. Some of the key drivers of the initiatives for IAM are best captured in quotes from some of the respondents:

- “We need to harmonize our identity infrastructure.“
- “We need to bring identity sprawl under control.“
- “We need to improve governance over access to data and networks.”
- “IDM now including the AI Agent identity.”
- “We intend to move [many] on-prem identity systems into one…”

This broad list of motivations drove members to create, or continue working on, IAM initiatives implementing new identity systems. Other members stated they were focused on better utilizing, or expanding the integration of their current identity management tools. Expansions included reviewing the Least Privileged Access principles for all employees and extending MFA and other identity verification tools to broader classes of employees as well as to joint venture partners and suppliers.

AI was brought up in many conversations on IAM. One dilemma was to resolve whether an AI agent gets the same permissions as the employee to whom the agent is attached, or is there a separate set of permissions?

Considering the fake IT worker schemes and social engineering attacks in 2025, CISO’s were also looking to improve processes and integrate tools to improve the assurance levels of human identity verification.

Other IAM initiatives included increased privileged access management, identity life cycle management (joiners, movers, and leavers), better management of the life cycle of certificates, expanding MFA integration, and doing credential audits.

02 Governance: Organizational Context

OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity - including privacy and civil liberties obligations - are understood and managed	60%
OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	40%

Figure 5

The initiatives to address gaps in Governance - organizational context, pointed to two significant challenges. As shown in Figure 5, 60% of the responses shared initiatives to ensure the business understands and manages legal and regulatory risk. The second most noted projects (40%) were designed to ensure all aspects of the business understand and consider cybersecurity risk management in their areas of responsibility/operations.

Two themes were woven across the responses: the challenges presented by the emergence of AI and those posed by ever-expanding government regulations. CISO's noted the need to get AI governance and controls in place swiftly. The business units, IT, and the cyber operations are leveraging AI tools but strategies on how to govern and manage the risk are not in place. Concerns run across all aspects of IT, applications, and safety. Many CISO's are concerned about agentic AI. They are looking to ensure guardrails are in place as they seek to better understand the breadth and depth of AI's penetration into their business operations and data repositories.

CISO's see AI as both a threat and a tool. Adversaries are using AI to identify network and application vulnerabilities. They are using AI to create new zero days and advanced malware. AI's rapid adoption by business units is yet another wave of computing capability being leveraged well ahead of the cybersecurity profession being able to put the governance and controls in place in a timely fashion. Similarly, AI can be leveraged to improve detection, protection, and incident response.

The respondents also pointed to the expanded government regulatory requirements in aviation. The European Union Aviation Safety Agency (EASA) Part IS regulation was most frequently referred to as implementation deadlines have arrived or are getting closer. Other government regulations noted were the TSA's AOSSP and ASP requirements, EU's Network and Information Security Directive (NIS-2), The EU's Cyber Resilience Act, Canada's Bill C-8: the Critical Cyber Systems Protection Act, and Cybersecurity Maturity Model Certification (CMMC). Some CISO's are concerned about overlapping regulations as the NIS2 Directive is transposed in a different way by each European Member State. CISO's also noted concerns around having enough resources to ensure compliance and manage audits.

CISO's noted the need to integrate cyber risk management into their Safety Management Systems.

03 Governance: Cybersecurity Supply Chain Risk Management

SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship	40%
SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders	30%
SC-02: Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally	10%
SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties	10%
SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities	10%

Figure 6

Over the past several years, supply chain risk has been a concern for the aviation industry. In 2025, we continued to see how cyber breaches at a common supplier can have an exponential impact on the sector. Figure 6 shows 70% of the initiatives are in the areas of Supply Chain Risk management program strategy reviews and improved monitoring of suppliers. Some of the telling thoughts from CISO's were:

- "We are reviewing SAAS providers as production lines. If the production lines fails, what are the cascading effects?"
- "We are seeing …fourth party risk that must be assessed and governed."

Several CISO's spoke of the need for a common questionnaire for suppliers. The Aviation ISAC undertook this challenge a few years ago and landed on common tool. We encourage aviation industry companies to consider this platform.

With the rapid integration of AI into so many tools and processes, many CISO's noted initiatives to once again look at the cybersecurity clauses in supplier contracts to ensure AI cyber risk is addressed.

Joint Venture risk was another area of concern for some CISO's. Unlike supplier risk which can be pushed directly down to the supplier, some CISO's noted that the ownership of cyber risk had not been clearly defined in some joint ventures and they planned to address those gaps in 2026.

Several CISO's also mentioned the initiation of cybersecurity program audits of key suppliers would be kicking off this next year.

04 Protect: Data Security

DS-01,02,10: The confidentiality, integrity, and availability of data-at-rest, in-transit, and in use, are protected.	90%
DS-11: Backups of data are created, protected, maintained, and tested	10%

Figure 7

As shown in Figure 7, we combined each of the confidentiality, integrity, and availability (CIA) subcategories as the initiatives clearly were addressing concerns about data security at-rest, in-transit and in use.

Three data security themes emerged from the interviews. In order of frequency, improving the creation, securing and testing of backups was highest priority in this area. Improving visibility and understanding of where all critical data resides is also on this year's roadmap for many companies. Woven into the understanding of where all critical data resides was a review of what should be considered critical data. Last year, we heard members mention concerns over Quantum and those concerns are growing as it appears Quantum applications and tools are expected to be commercially available in the near future.

05 Protect: Technology Infrastructure Resilience

IR-01: Networks and environments are protected from unauthorized logical access and usage	60%
IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations (recovery planning)	30%
Other: Other subcategories combined	10%

Figure 8

Figure 8 reveals that initiatives were predominantly aligned to two infrastructure resilience subcategories, 01 and 03. Network segmentation projects were called out the most frequently. In tandem with the network segmentation or as separate initiatives, CISO's spoke of the continued or new work in line with Zero Trust Network Access (ZTNA) aligned projects.

At a high level, some CISO's are working with the business functions to determine how to ensure critical processes can be performed in the absence of the technology used to support those processes. Other projects included protecting and hardening endpoints, improving firewalls, improving resilience in the cloud and testing disaster recover plans.

Other Notable Responses from the Survey

Identify: Improvement

- Security Operations Center Enhancement projects will be extensive in 2026. CISO's are looking to leverage AI enhanced SIEM products and will be doing bake-offs of tools in the coming year. Similarly, CISO's are looking to use AI to further automate their Security Orchestration, Automation, and Response (SOAR) playbooks.
- Many CISO's will be using tabletop exercises (TTX's) to identify improvement opportunities.
- CISO's will be building dashboards to include business intelligence indicators which may provide early warning visibility.

Identify: Asset Management

- CISO's are still trying to improve their visibility of OT assets and software as well as identifying "Shadow IT."
- Another prominent theme within responses in this category were initiatives to better protect or completely remove legacy technologies from the networks.

Detect: Continuous Monitoring

- Several recurring themes are driving initiatives in the continuous monitoring programs in aviation. CISO's will be enhancing, upgrading and expanding the scope of their SOCs to address OT cyber risk and Supply Chain Cyber risk. Some also mentioned monitoring customer cyber risk and working on ways to share intelligence with their customers.
- One measure which will be used to drive improvement is the Mean Time to Respond (MTTR).
- The use of AI to improve CM capabilities was also highlighted by many CISO's.

Protect: Platform Security

- Eliminating technical debt
- Increasing vulnerability management, with a particular emphasis on OT
- Integrating OT monitoring into the SOC
- Improving the security within the Software Development Life Cycle (SDLC).

Detect: Anomalies & Events

Many CISO's are replacing their SIEMs and deeply scrutinizing the value of the their managed service providers and the offerings of competitors as consider the AI implementations into these products. Members noted a consolidation occurring in the cybersecurity tool industry and how that might impact which tools they will select moving forward.

Two Points to Highlight

CISO's talked about the need to continue to support the development of talent in cybersecurity specialties, particularly in identity management. Most importantly, there is a significant daily workload which is compounded during significant incident response events. It is important for CISO's to be attentive to the mental health and work-life balance of their teams.

RESULTS BY INDUSTRY SEGMENT

Figures 9 - 11 depict the functional level changes in emphasis, by segment, from our CISO interviews ahead of calendar years 2025 versus 2026.

AIRPORT CISO FOCUS

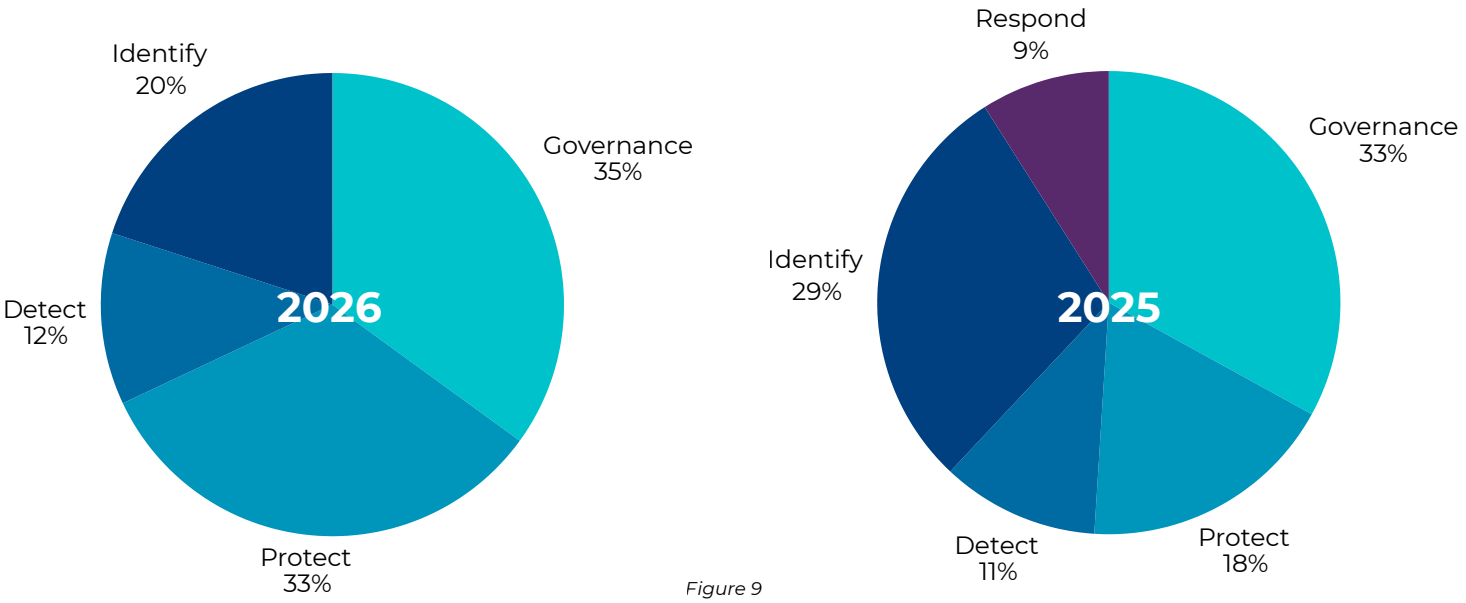

Figure 9

Governance remained the most noted area for initiatives going into 2026. The emphasis on Protect almost doubled, with the categories of focus being primarily IAM and platform security. Several CISO's noted the use of TTX's to help them better understand impact of events and to improve incident response.

OEM & SERVICE PROVIDER CISO FOCUS

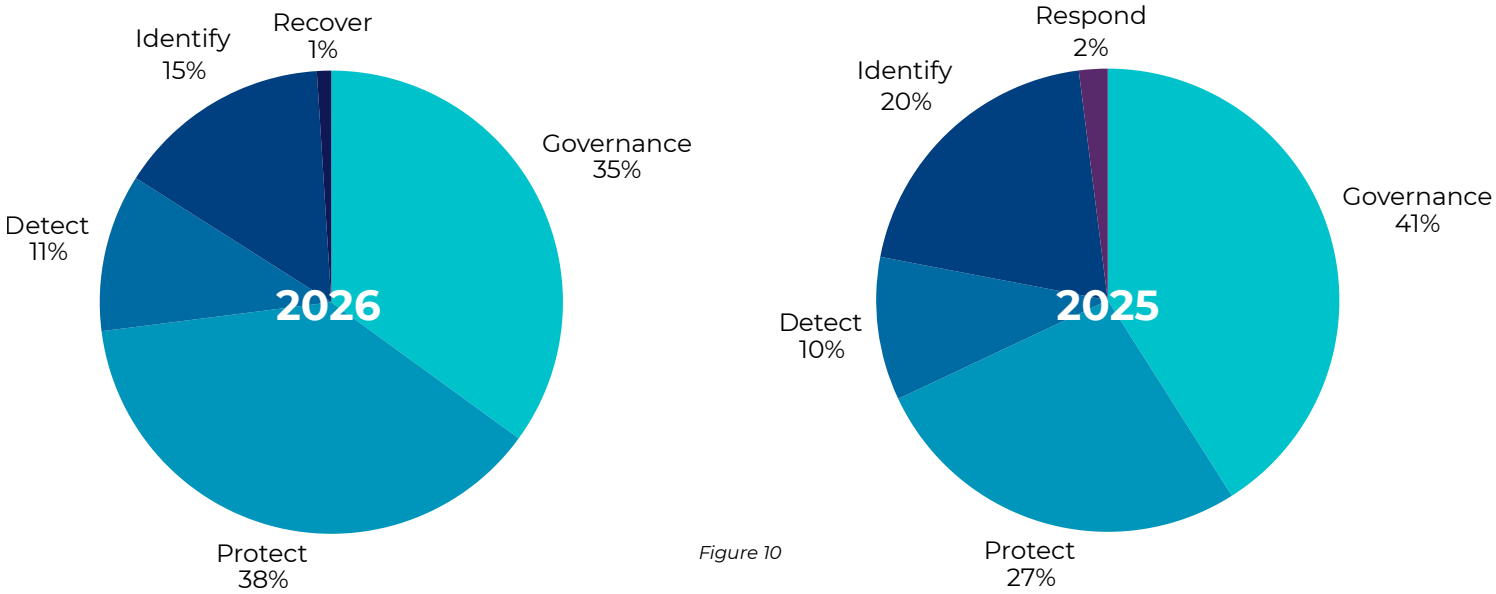

Figure 10

Protect was the most frequently mentioned functional focus in the OEM/Service provider's segment, just slightly ahead of Governance. In 2025, governance was 15% higher than Protect. Within the responses aligned with Protect, Identity and Access Management initiatives were most highly noted, followed closely by Data Security and Platform Security aligned projects.

AIRLINE CISO FOCUS

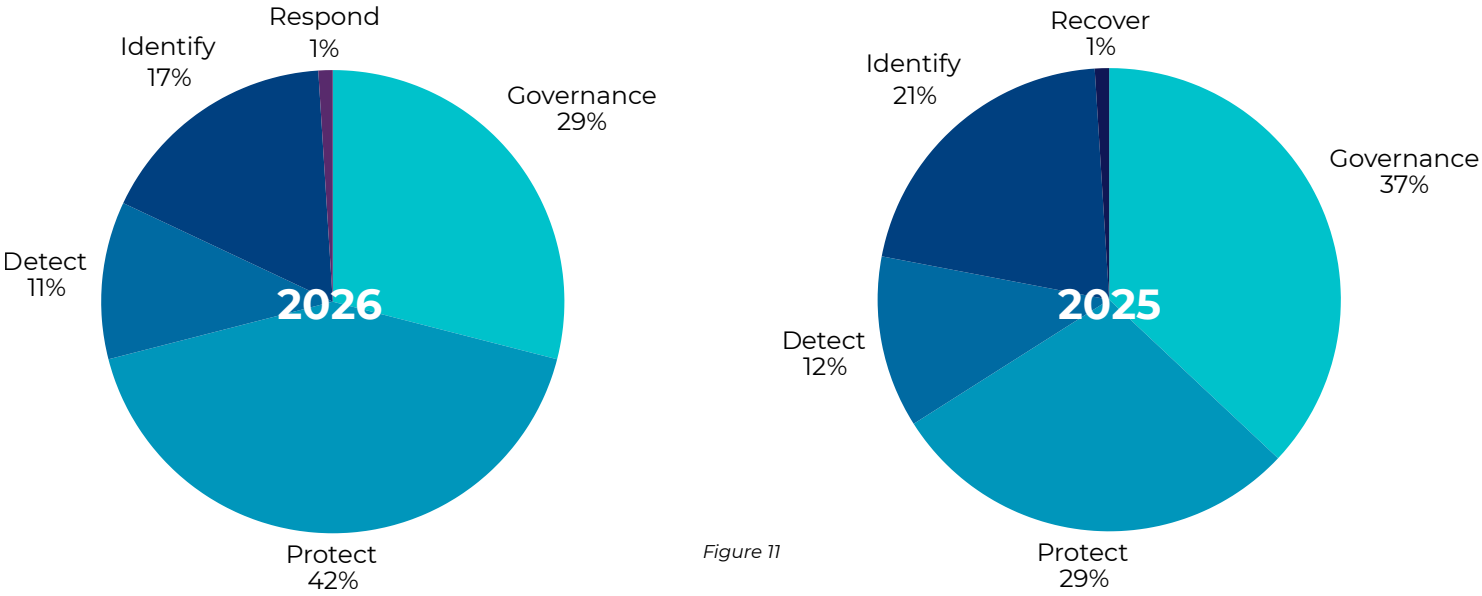

Figure 11

The most significant shifts in the airline sector were projects addressing the two most significant areas of concern, Governance and Protect. However, it was clear that the airlines, particularly those operating in Europe remain highly focused on regulatory compliance. The increase emphasis on protect was identity management, again driven most by AI concerns, and data security for the same reasons.

SUMMARY

This report presents an industry trend analysis of annual cybersecurity priorities identified by Chief Information Security Officers and Chief Product Security Officers across the aviation sector. It does not reflect the perspective or emphasis of any single organization. Rather, its value lies in providing a broad, peer-driven view that helps aviation CISOs and CPSOs benchmark their cybersecurity strategies, program maturity, and resource management against the collective insights of the industry.

We extend our sincere thanks to the many Aviation ISAC member CISOs and CPSOs who took the time to share their perspectives and priorities for 2026. Your willingness to contribute strengthens our community and helps advance cybersecurity resilience across aviation.

Cyber resilience in aviation is not something any organization can achieve alone. It requires collaboration and a shared commitment to protecting the industry we all support. The Aviation ISAC is a global community of dedicated professionals who care deeply about aviation safety, security. We provide a trusted environment where members can openly share threat intelligence, exchange lessons learned, and collaborate on best practices to better protect, detect, respond to, and recover from cyber threats.

If you are interested in joining the Aviation ISAC community, please contact membership@a-isac.com. For partnership or sponsorship opportunities, we welcome you to reach out to sponsorships@a-isac.com.

CONTACT

1997 Annapolis
Exchange Pkwy
Suite 300
Annapolis, MD 21401

membership@a-isac.com
www.a-isac.com