2024

CISO SURVEY RESULTS

CONTENTS

EXECUTIVE SUMMARY

Welcome to the 2024 edition of the Aviation ISAC Cyber Risk Survey. This is the seventh consecutive year the Aviation ISAC has published this survey. This year we added a new section, the Aviation Sector Threat Landscape. This new section highlights many of the concerns which drive the risk management strategies of the sector.

The Aviation industry is quite healthy, making a strong comeback following the pandemic. IATA predicts the aviation industry's total revenues in 2024 to grow 7.6% year on year to a record $964 billion, with around 4.7 billion people expected to travel in 2024, a figure exceeding the pre-pandemic level of 4.5 billion seen in 2019. [1] The 2024 air cargo demand outlook is muddied by factors including questions about the strength of the global economy and the impact of geopolitical tensions. However, industry experts expect upticks in air cargo in late 2024. [2]

In 2023, we saw extensive growth in the addition of new technologies to support the aviation industry. These technologies include the advancement of electric take-off and landing vehicles, drones, security and monitoring technologies, artificial intelligence, and more. These additional technologies underscore the importance of a strong cyber security program in all segments of the sector: air framers, airlines, airports, air navigation service providers, communications providers, supply chains, and more.

As the Aviation ISAC kicks off its 10th Anniversary, we celebrate the Chief Information Security Officers (CISO's), Chief Product Security Officers, Cyber Threat Intelligence Analysts, Network Security Architects, Network defenders and Incident Responders, Compliance Specialists and the many others who secure the networks and operating technologies of our industry. Our members are committed to safety and cyber security in the global aviation eco-system.

The purpose of the survey is to provide a tool for industry CISOs to benchmark their strategies, program maturity, and management of resources. The Aviation ISAC staff also utilizes this information to direct our efforts into the areas of emphasis for our members.

How do we get the data? Each year we survey CISOs in our community to understand their strategies for cyber risk reduction heading into the new year. The survey poses just one question, "What are the three to five things you committed to getting done in 2024 to reduce cyber risk?"

How do we analyze the data? The responses are catalogued using the National Institute of Standards and Technology's Cyber Security Framework (NIST CSF). We aggregate the responses and summarize where cyber security efforts are focused. We present the results along with highlights from the CISO narratives.

What did we learn? Identity Management, Authentication and Access Control, continues to be the most significant area of concern for the aviation cyber security community. Many initiatives are underway, and more details can be found in the body of this report. Supply Chain Risk Management was the second category of most concern. This aligns with the many supply chain-based attacks we saw impacting the industry in 2023. Governance was the third highest rated area of concern.

{1} https://www.cnbc.com/2023/12/06/airlines-signs-are-pointing-to-a-bumper-travel-year-in-2024.html#:~:text=Total%20revenues%20in%202024%20are,4.5%20billion%20seen%20in%202019.

[2] https://www.flightglobal.com/airlines/air-cargo-leaders-look-deep-into-2024-for-demand-uptick/155715.article

As regulators continue to add more requirements and the threats of fines and lawsuits loom larger, there is a growing need to deeply embed cybersecurity into the culture, policies, and processes across entire business enterprises. Rounding out the top 5 categories of risk reduction efforts were Information Protection Processes and Procedures and Risk Assessment.

Insights on other notable initiatives were also provided for the NIST CSF categories of Detection Processes, Awareness and Training, and Security Continuous monitoring. Finally, we present year-over-year analysis of the results by the overall industry and by industry segment.

Thank you for all you do to make aviation safe and secure.

THREAT LANDSCAPE

Over the past eight years, cyber threat actors have demonstrated an ability to disrupt 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. Certain companies have experienced significant operational disruption, loss of sensitive data, and financial losses. This assessment of the cyber threat landscape addresses the capabilities and intent of cyber threat actors, the increased vulnerabilities of the sector as more business functions become digital, and the impact attacks can have on global commercial aviation.

- Three types of cyberthreat actors are targeting the commercial aviation sector: nation-state Advanced Persistent Threat (APT) groups, organized cybercriminal groups, and hacktivists. The objectives of these groups are to obtain sensitive corporate data (including intellectual property), track dissidents, steal or extort money, to gain a geopolitical advantage, and/or support a cause.
- The large and growing digital infrastructure which supports the commercial aviation sector provides attackers with a broad and extensive cyber-attack surface. Furthermore, the growing reliance upon managed service providers (MSPs) and cloud service providers increases the risk of indirect data breaches, when these providers are targeted by malicious cyberthreat actors.
- Although cyberthreat actors continue to exploit known computer vulnerabilities in organizations that have not fully mitigated these flaws, they are also becoming increasingly adept at finding and exploiting zero-day vulnerabilities before they are made public. Cyber threat actors are also getting much better at avoiding traditional signatures-based intrusion detection systems and maintaining network persistence through living-of-the-land (LOTL) tactics.
- The Aviation ISAC assesses that some cyberthreat actors likely possess the ability to inflict serious disruption upon the global commercial aviation sector. A serious malicious cyber disruption would most likely occur via exploitation of a software/firmware vulnerability to either (a) breach corporate networks directly or (b) breach the networks of service providers or supply chain companies to indirectly impact their downstream customers. The disruption may be intended to either extort ransoms or to temporarily shut down normal operations.
- Escalating regional tensions in EMEA and APAC regions are likely to serve as driving forces behind increases in malicious cyber activities emanating from these areas. Cyber hacktivism is evolving into a form of proxy cyber warfare with fewer boundaries than traditional state-directed cyber campaigns.
- The Aviation ISAC assesses that due to their frequent use of zero-day exploits, sophisticated evasion techniques, and targeting of aviation-related data, China-based APT groups are likely to pose the highest cybersecurity risk to the global commercial aviation sector.

SURVEY RESULTS

This year, just over 36% of our members participated in our annual one question survey. The question is quite simple and direct, “What are the three to five things you’ve committed to getting done in 2024 to reduce cyber risk?” We tabulated and analyzed the results from several perspectives. We looked at overall responses by function (Identify, Protect, Detect, Respond, and Recover), category, and sub-category. As seen in prior years, some responses did not fit into the NIST CSF Framework, but were critical to the health of a good cyber security team. This year we had the fewest number of responses in the “Other” category, all of which pertained to staffing challenges.

For 2024, more projects were called out in the Identify Function, followed by Protect, Detect, Respond, Other and Recover. (See figure 1) However, Identity Management, a category within the Protect Function, continued to be the number one focus of the industry. As depicted in figure 2, two significant changes from prior years were noted. There was a marked shift into projects in the Identify function as opposed to an emphasis on the Protect function in 2023. This was primarily due to an increased emphasis by member companies on supply chain risk management, governance, and risk assessments. Secondly, there was a sharp increase in initiatives within the Detect function, as members highlighted projects to broaden and improve security continuous monitoring and upgrade detection processes.

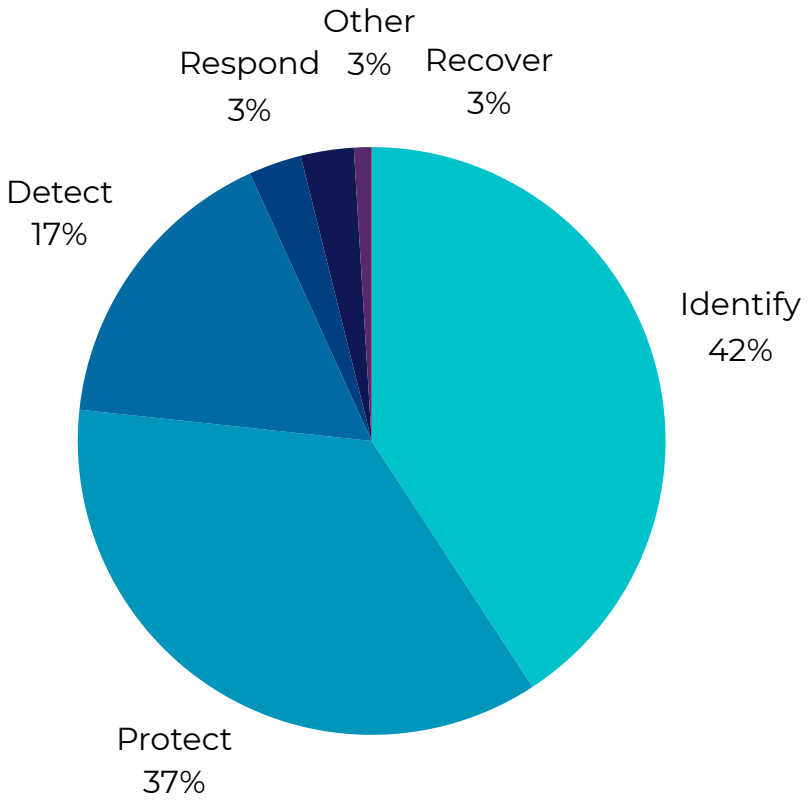


Figure 1
2024 Responses by Function, All Segments

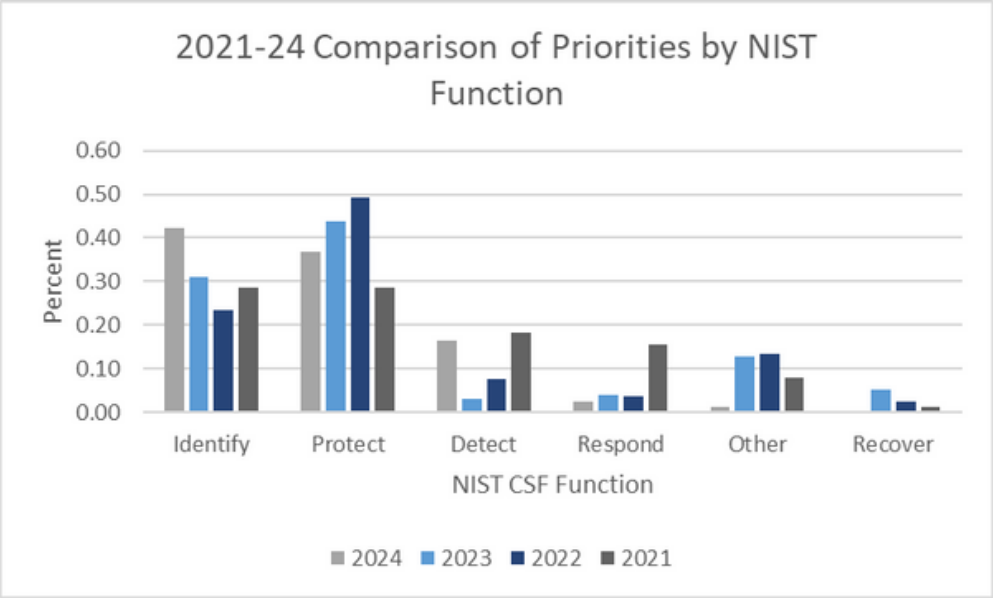


Figure 2
Comparison of survey results by NIST CSF function, 2021-24

A deeper dive into the categories, sub-categories and specific projects mentioned by the respondents are provided below. The NIST CSF has significantly less categories and sub-categories in the respond and recover functions, thus it is expected that we would see less initiatives in these areas.

WORD CLOUD

Our word cloud depiction (Figure 3) is derived from the cumulative narratives of the CISO and Chief Product Security Officer interviews. Identity and access management is most prominently mentioned which aligns with the prioritization of risk reduction efforts. Many efforts around overall risk management were also identified which led to such emphasis on “management” in the word cloud. We saw an uptick in conversations concerning the cyber security of the plane. CISOs discussed many projects to further implement MFA, building of new capabilities, and enhancing older tools with next-generation upgrades. There were many initiatives to increase monitoring capabilities across the IT and OT environments. Let’s jump into the details!

Figure 3
Word Cloud

TOP 5 CATEGORIES OF RISK REDUCTION EFFORTS

01 Protect: Identity Management, Authentication, & Access Control

02 Identify: Supply Chain Risk Management

03 Identify: Governance

04 Protect: Information Protection Processes & Procedures

05 Identify: Risk Assessment

Of those participating in the survey, 37 of the respondents identified initiatives in IDM, followed by 35 in Supply Chain Risk Management, 27 in Governance, 19 in Information Protections Processes and Procedures, and rounding out the top five, 17 initiatives in Risk Assessment.

01 Protect: Identity Management, Authentication, & Access Control

Identity Management, Authentication and Access Control (IDM) has been the forever challenge for CISO's across all industries. Survey respondents noted several multi-year projects to implement multifactor authentication (MFA) across their networks and operating technologies (OT), Zero Trust (ZT), and leveraging more IDM tools for analytics. Aviation companies are most focused on four IDM subcategories: PR.AC-1 credential management, PR.AC-5 network integrity, PR.AC-4 Access permission management, and PR.AC-7, Authentication and MFA.

PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	32%
PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	30%
PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	24%
PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	14%

PR.AC-1: A variety of challenges are to be addressed through initiatives mentioned by the respondents. Many of these issues are multi-year challenges. Many initiatives were started in 2023, or earlier, and others are still in the strategic planning phase. CISOs mentioned a broadening of the deployment of IAM tools, such as to customer accounts, and implementation of MFA for both privileged accounts and customers. CISOs mentioned extensive cleanup projects in IAM as well. CISOs noted that IAM tools now have more add-ons and analytic capabilities, such as privileged access monitoring, which they plan to leverage in 2024.

PR-AC-5: Many member companies have been engaged in multi-year segmentation projects. This year was the focus. Members mentioned the segmentation of OT from the network, and, in one case, segmenting business operational units. CISOs mentioned micro segmentation initiatives to include segmentation of applications and data. We also saw an overlap of ZT initiatives and Identity Management as members mentioned role-based access controls as part of their ZT initiatives.

PR.AC-4: CISO's described initiatives to identify, as one CISO called it, "toxic or over-privileged" accounts, to include administrative accounts. The initiatives were around strengthening the processes around system access management. Examples included understanding the business needs for network access of each role and improving automated validation checks ahead of authorization. The project scoping included access provided to vendors.

PR.AC-7: CISOs mentioned projects to increase the use of MFA across their organizations. Some members were leveraging recent regulatory requirements to drive adoption. Others mentioned the implementation of network access controls (NAC) and getting rid of VPN access in lieu of a private access solution. These solutions would also check for security tools on devices prior to authorizing their network access. Several members also noted MFA implementation was part of their ZT strategy.

02 Identify: Supply Chain Risk Management

Supply Chain Risk Management (SCRM) has been a top 5 category since 2021. SCRM concerns align with the threat landscape. Over the past several years we have continued to see the supply chain as a successful attack vector in aviation and other critical infrastructure sectors.

ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	31%
ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	29%
ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	23%
ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	17%

ID.SC-2, SC-1, SC-3: Many respondents noted that their companies would be establishing or rethinking their SCRM programs. Many felt their current programs were not reducing or eliminating the SC risk. As a result, they will adjust their strategies and create policies to drive better SCRM. This included leveraging contractual processes and regulatory requirements to require better cyber hygiene in their supply chains. Several airlines noted they would be reviewing the cyber risk to the aircraft. Other initiatives were mentioned such as reviewing the vetting process for vendors and as well as vendor access to networks.

ID.SC-4: Questionnaires are utilized by many respondents, however, as a part of the strategic re-thinking of their programs, many respondents expect to increase the validation efforts of their key suppliers to include audits.

03 Identify: Governance

For the first time in the seven years we have been conducting this survey, Governance hit the top five focus areas. Interestingly, the next iteration of the NIST CSF, 2.0, has elevated governance from a category to a function. During our survey discussions, CISOs noted that more and more cyber regulations are driving the need for cyber security to be embedded in policies across the entire company. For years CISOs have been working to improve the cyber hygiene of business units and with recent changes in the Security Exchange Commission's cyber requirements, more of the C-Suite is feeling the need to increase the effectiveness of cyber security governance. One of the key drivers to increase the governance of cyber security is the rapidly expanding regulatory requirements. CISOs noted challenges in staying on top of these rapidly changing rulesets. CISOs noted they would be hiring staff to work in this area.

ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	44%
ID.GV-1: Organizational cybersecurity policy is established and communicated	26%
ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	22%
ID.GV-4: Governance and risk management processes address cybersecurity risks	7%

IID.GV-3, GV-4: The regulatory burden on CISOs and Chief Product Security Officers continues to grow. Respondents mentioned they would be hiring additional staff to address compliance matters. Depending on the maturity of the cyber programs at different companies, CISOs mentioned the pursuit of certifications in PCI-DSS, SOC2, and ISO. Many respondents noted their customers are seeking to have them be SOC2 compliant. Respondents are also expecting more contractually bound cyber security requirements in the coming year. European companies have an eye on NIS2 as individual countries roll out their regulations. Respondents also noted they expect more audits of their self-attestations. For those companies which also supply the US Department of Defense, there are initiatives to prepare for CMMC audits. To effectively measure that these risks are managed, respondents noted the creation of metrics to monitor the progress and effectiveness of meeting the legal and regulatory requirements.

ID.GV-1: There was a wide range of policy issues identified in the survey. Newer members to the Aviation ISAC were looking to identify frameworks and establish cybersecurity governance. Another respondent noted that the company expanded too quickly, and network expansions occurred without a unified strategy or reference architecture, and they were looking to remedy that problem in 2024. Another member highlighted a planned table-top exercise (TTX) in Q1 with a focus on policy improvement in the cyber program and when addressing a major incident, such as ransomware. Finally, another member noted the need for better governance over applications as they would address cybersecurity requirements in the acquisition and development of applications.

ID.GV-2: Respondents highlighted initiatives to make cyber security simpler, more understandable, and transparent for company employees. One member is building out the roles and responsibilities for conducting cyber security on the aircraft to include what logs to collect and analyze. Another member noted they are putting together cyber training materials for pilots dealing with Global Positioning System outages.

04 Protect: Awareness and Training

Either Data Security or Information Protection has been in the top five focus areas for the past two years. Process improvement, PR.IP-7, led the subcategories among the responses received. Many respondents highlighted refresh projects and plans to review their programs and identify opportunities to be more efficient. There were many responses in this category, we are highlighting only those sub-categories with multiple responses.

PR.IP-7: Protection processes are improved	26%
PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	16%
PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	11%
PR.IP-12: A vulnerability management plan is developed and implemented	11%
PR.IP-4: Backups of information are conducted, maintained, and tested	11%
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	11%

PR.IP-7: Data protection is another area where members are seeing increased regulation. Many efforts, highlighted earlier, contribute toward information protection, however, some CISOs called out specific data protection initiatives. These included: implementation of container security, establishing a mobile security program to include hiring of mobile security subject matter experts, increasing staffing to address acquisition security, and moving to next generation segmentation and next-gen firewalls.

PR.IP-5: The growing number of regulatory requirements for cyber are extending into operating technologies. CISOs noted the challenges of integrating cyber and safety cultures.

PR.IP-1: Several CISOs highlighted ongoing initiatives to remove ICS connections to their business networks.

PR.IP-12: CISOs are continuing to improve their vulnerability management processes and expedite priority patching.

PR.IP-4: CISOs indicated they were replacing current back-up solutions to solutions which offer increased reliability and are more likely to provide the capability to retrieve a known, good back up.

PR.IP-9: CISOs continue to develop and refine IRPs.

05 Identify: Risk Assessment

Risk assessment is a newcomer to the top five in 2024. Risk assessment is a critical component to strategic planning and the prioritization and allocation of limited staff and budgets. As in the previous category, we are highlighting only those sub-categories of Risk Assessment with multiple responses.

ID.RA-1: Asset vulnerabilities are identified and documented	35%
ID.RA-4: Potential business impacts and likelihoods are identified	24%
ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	18%
ID.RA-6: Risk responses are identified and prioritized	12%

ID.RA-1: CISOs must manage vulnerabilities across the network, products, OT, ICS and more. Although many CISOs highlighted vulnerability management initiatives, the initiatives themselves were varied. One CISO noted efforts to push accountability for vulnerabilities back into the business units. Several mentioned pen testing initiatives on their own products as well as on OT systems. One CISO is looking into Vulnerability Management as a service. This would include identification and patching of external facing assets and internal servers.

ID.RA-4, RA-6: CISOs are concerned about their own companies leveraging or integrating artificial intelligence into their business processes and products. They will also be using their risk assessments to better secure OT and IT, as well as legacy interfaces.

ID.RA-2: The rise in geopolitical tensions has CISOs looking for additional intel on the tools, techniques, and behaviors of nation-state actors and those groups affiliated with the causes of nation states. CISOs are also looking for early warning indicators of attacks. All this goes toward promoting more and faster exchange of threat intel from both the public and private sectors.

Other Notable Responses from the Survey

A significant number of important initiatives were not included in the top five categories. Those notables are highlighted below:

DE.DP-5 Detect: Detection Processes: Detection Processes are continuously improved. Over 26% of those surveyed advised they were looking into next gen SIEMs and SOARs. One requirement was for the new products to be enhanced with artificial intelligence. Some CISOs intend to explore all the options and capabilities within currently within their SIEMs, but not being utilized. The intent is to leverage the SIEM to improve both their asset management and insider threat programs. Other members were in the process of putting together playbooks for incident response (IR) as the first phase of moving toward IR automation.

PR.AT-1 Protect: Awareness and Training: All users are informed and trained. Approximately 24% of the respondents noted they would be conducting cyber security awareness campaigns. The campaigns were much bigger than simply phishing and included more awareness of the threats, development of materials to help business process owners and employees understand the threat, as well as their roles in cybersecurity. Many of the CISOs described their program goals as two-pronged, first to increase awareness and second, to drive culture change.

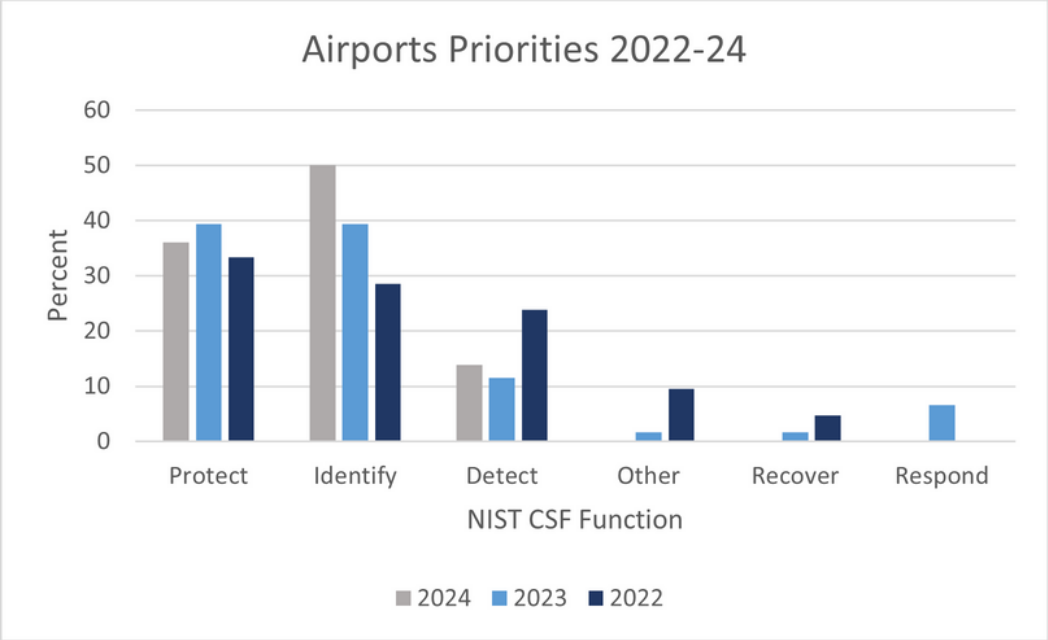
DE.CM-1 Detect: Security Continuous monitoring. The network is monitored to detect potential cybersecurity events.

A fifth of the respondents highlighted plans to extend or upgrade continuous monitoring capabilities. New detection capabilities were noted for OT environments. This included monitoring the health of the OT environments, installation of Endpoint Detection and Response (EDR) or Extended Detection and Response (XDR), along with monitoring for anomalies.

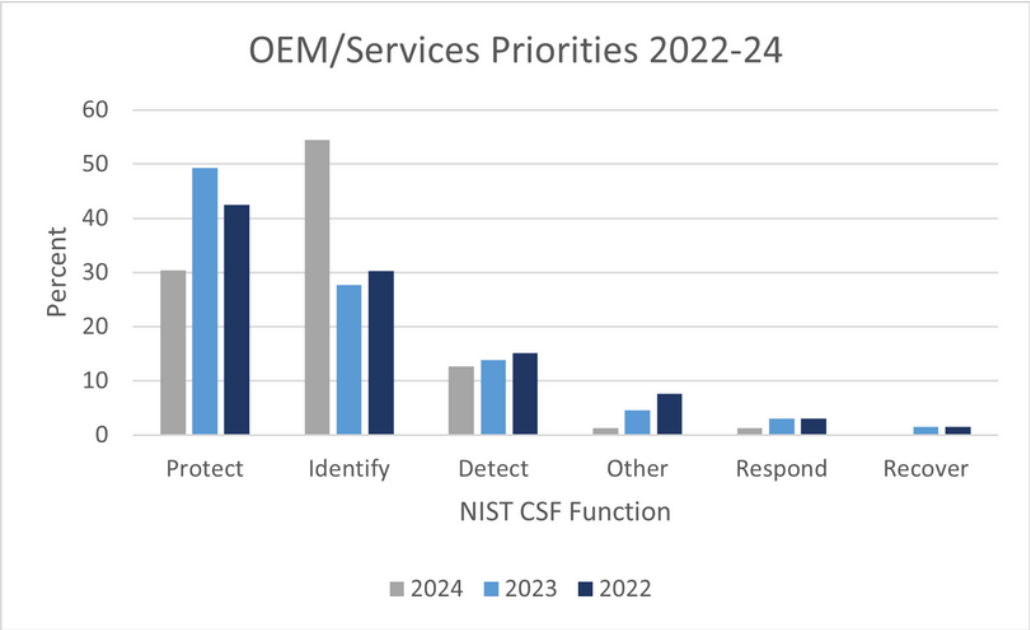
Other new detection capabilities included User Employee Behavioral Analytics (UEBA) to identify insider threats and improved detection of bot activity on the networks. Several members were looking to increase their cloud detection capabilities and one CISO noted they were putting their SOC MSSP contract out for bid.

ANALYZING THE RESULTS BY INDUSTRY SEGMENT

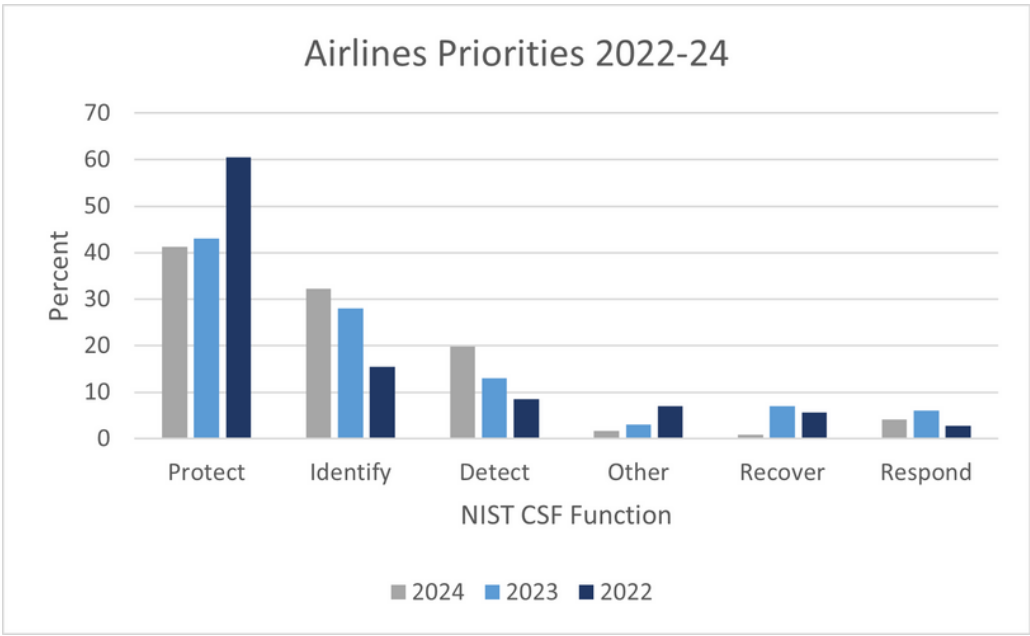
The charts below depict the percentage of initiatives by function for the years 2022-24 by each of the three segments used for this survey: Airports, OEM's/Service companies, and Airlines. Thus, the totals for each function tally to 100 Percent.



Airports: Year over year, Protect, Identify, and Detect initiatives remain the top 3 areas of emphasis for the majority or our airport member companies. For 2024 there was a significant shift in resources toward identify-based initiatives. The sub-categories of Supply Chain and Risk Assessment were the most frequently mentioned areas of emphasis.



Original Equipment Manufacturers (OEM)/Services (Svc): Year over year the emphasis on cyber risk reduction has remained constant in the OEM/Svc segment, with an overwhelming focus on Protect and Identify functions. In 2024, the emphasis on Identify-based initiatives also spiked. The sub-categories of focus were led by Supply Chain, followed closely by Governance and Asset Management.



Airlines: Like the Airports and OEM/Svc's segments, emphasis in the Airlines segment remained on Protect, Identify, and Detect from 2022-24. However, in 2024, the airlines surveyed were more focused on Protect-based initiatives, whereas Identify-based initiatives were the focus of the other two segments. Identity Management, Authentication, and Access Control initiatives far outnumbered the initiatives in all the other subcategories.

SUMMARY

This report is an industry trend analysis of annual cyber security priorities. It does not reflect the emphasis of any one company. The value of the report is in its ability to assist CISOs in Aviation to benchmark their cyber security strategies, program maturity, and management of resources with the industry as a whole.

We want to thank the many CISOs who took the time to share their thoughts and strategies for 2024.

ACKNOWLEDGEMENTS

The collective expertise and commitment within the Aviation ISAC community serve as a vital force in safeguarding the integrity and resilience of aviation systems against evolving cybersecurity challenges. Thank you to all who participated in collecting this vital information.

For more on how to become a part of our community please visit us at www.a-isac.com.

CONTACT

1997 Annapolis
Exchange Pkwy
Suite 300
Annapolis, MD 21401

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