Aviation ISAC
Cyber Landscape

Nickelby Thane
Regional Information Security Manager
(nthane@a-isac.com)

Who Am I?

Nickelby (Nick) Thane has over 18 years of IT/information security experience (before the term cyber security was coined) ranging from roles such as a security engineer, penetration tester, consultant all the way to a CISO.

Nick joined the Aviation ISAC in February 2023 as the regional information security manager building communities in the APAC region and championing the importance of community sharing in a trusted manner.

Nick strongly believes that it is only through trust and continuous comradeship within the aviation community can then a resilient and extremely capable community can exist to battle against cyber threats effectively.

When not busy fighting cyber crime in his day job, Nick loves to spend time playing video games as well as spend quality bonding time with his family in Sydney– his wife Elisa, daughter Zelda, son Keanu and their 2 guinea pigs, Burrow and Coben.

Threat Landscape

Over the past 10 years, 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. Certain companies have experienced significant operational disruption, loss of sensitive data, and financial losses.

Three types of cyberthreat actors are targeting the commercial aviation sector: nation-state Advanced Persistent Threat (APT) groups, organized cybercriminal groups, and hacktivists.

Threat Landscape

The large and growing digital infrastructure which supports the commercial aviation sector provides attackers a broad and extensive cyber-attack surface. Furthermore, the increased 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.

Threat Landscape

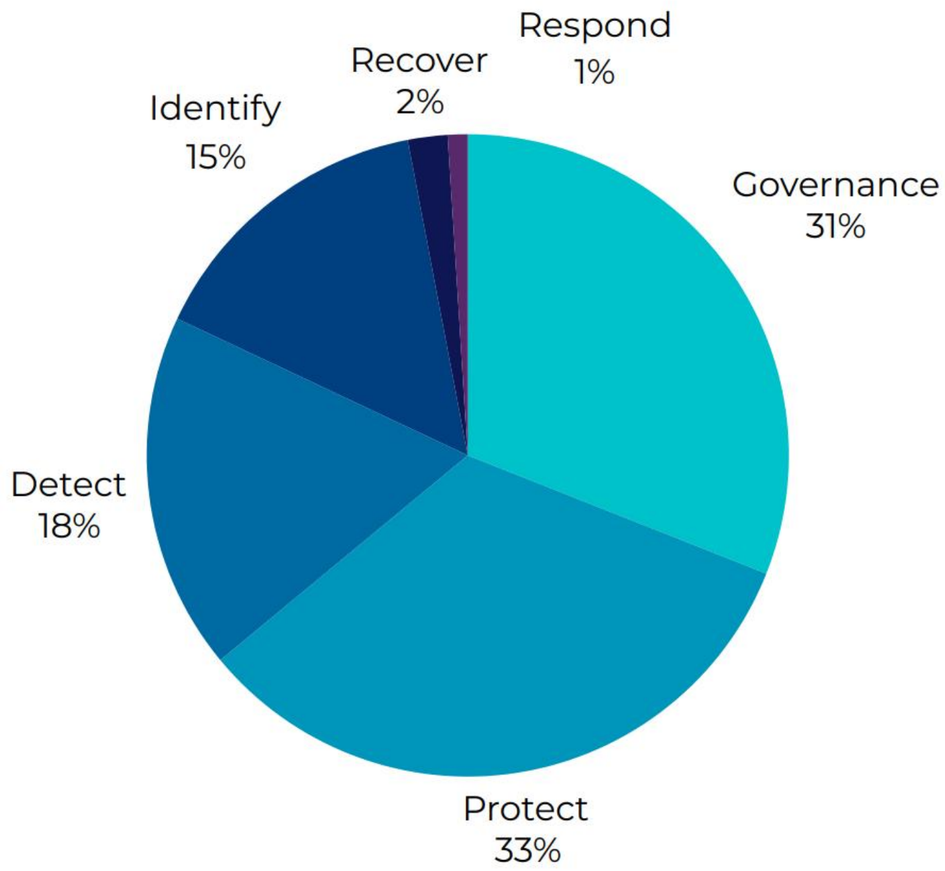
The Aviation ISAC assesses that some cyberthreat actors likely possess the ability to inflict serious, but localized, disruption upon the global commercial aviation sector.

High regional tensions in Eastern Europe, APAC, the Far East, and the Middle 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 that has impacted commercial aviation flights, as well as increased risk of accidental kinetic attacks. Ransomware attacks and the usual suspects including DDOS attacks and phishing attacks continue to be prevalent in all regions.

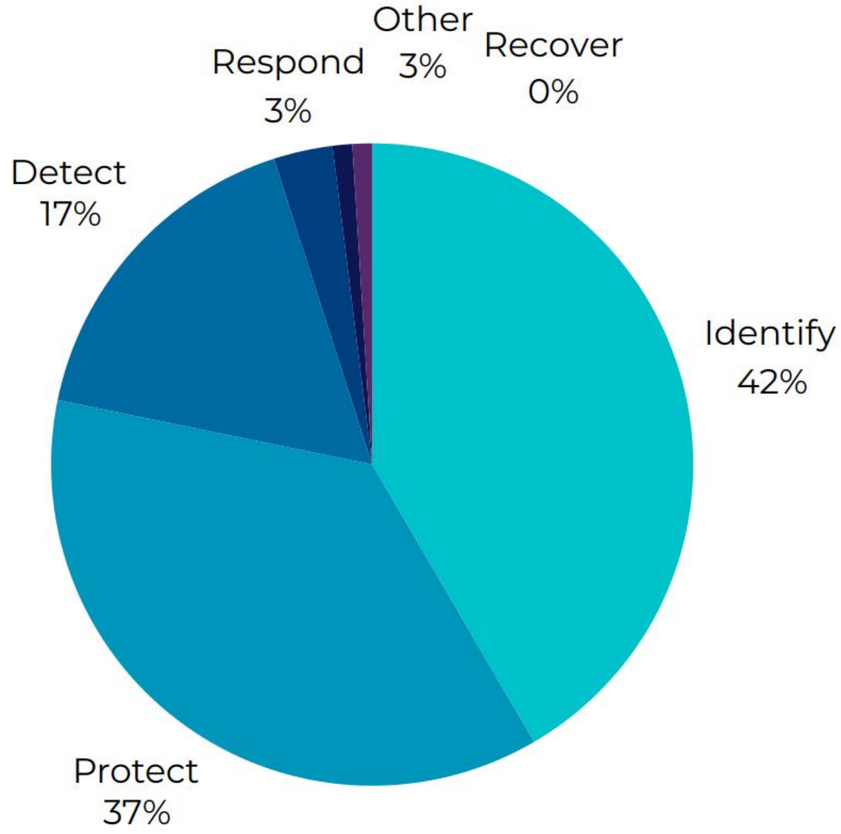
Cyber Risk Reduction Strategies

AVIATION ISAC

2025



2024



Cyber Risk Reduction Strategies

AVIATION ISAC

TOP 5 CATEGORIES OF RISK REDUCTION EFFORTS

1. Protect: (PR.AA) Identity Management, Authentication, & Access Control
2. Governance: (GV.OC) Organizational Context
3. Identify: (ID.AM) Asset Management
4. Governace: (GV.SC) Supply Chain Risk Management
5. Detect: (DE.CM) Continuous Monitoring

Cyber Risk Reduction Strategies

AVIATION ISAC

Protect: Identity Management, Authentication, and Access Control

Year after year, Identity Management, Authentication and Access Control (IDM) has been the number one ranked category of initiatives. Survey respondents continue to highlight multi-year projects to implement multifactor authentication (MFA) across their networks and operating technologies (OT). Identity management is a critical pillar in Zero Trust (ZT) strategies 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.

Cyber Risk Reduction Strategies

AVIATION ISAC

02 Governance: Organizational Context

Last year, Governance broke into the top 5 areas of action for CISOs in our survey. Governance, under NIST CSF 1.0 was a subcategory under Identify. This year governance is a function which took two of the 5 top slots.

Four of the six organizational context subcategories within the governance function aligned with projects identified by CISOs. Our global membership was reflected in the many different legal and regulatory schemes which our member companies must document their compliance through policy changes, process changes and audits.

Cyber Risk Reduction Strategies

AVIATION ISAC

03 Identify: Asset Management

Similar to the never-ending challenge of identity management, year over year asset management initiatives are a part of the cyber risk reduction strategies for CISOs in 2025.

Cyber Risk Reduction Strategies

AVIATION ISAC

04 Governance: Supply Chain Risk Management

There were numerous responses to the survey noting initiatives to reduce supply chain risk. Most of the subcategories in this function speak directly to CISOs engagement of their company's executives managing the business functions as well as ensuring cybersecurity is a part of the enterprises overall risk management plan.

Cyber Risk Reduction Strategies

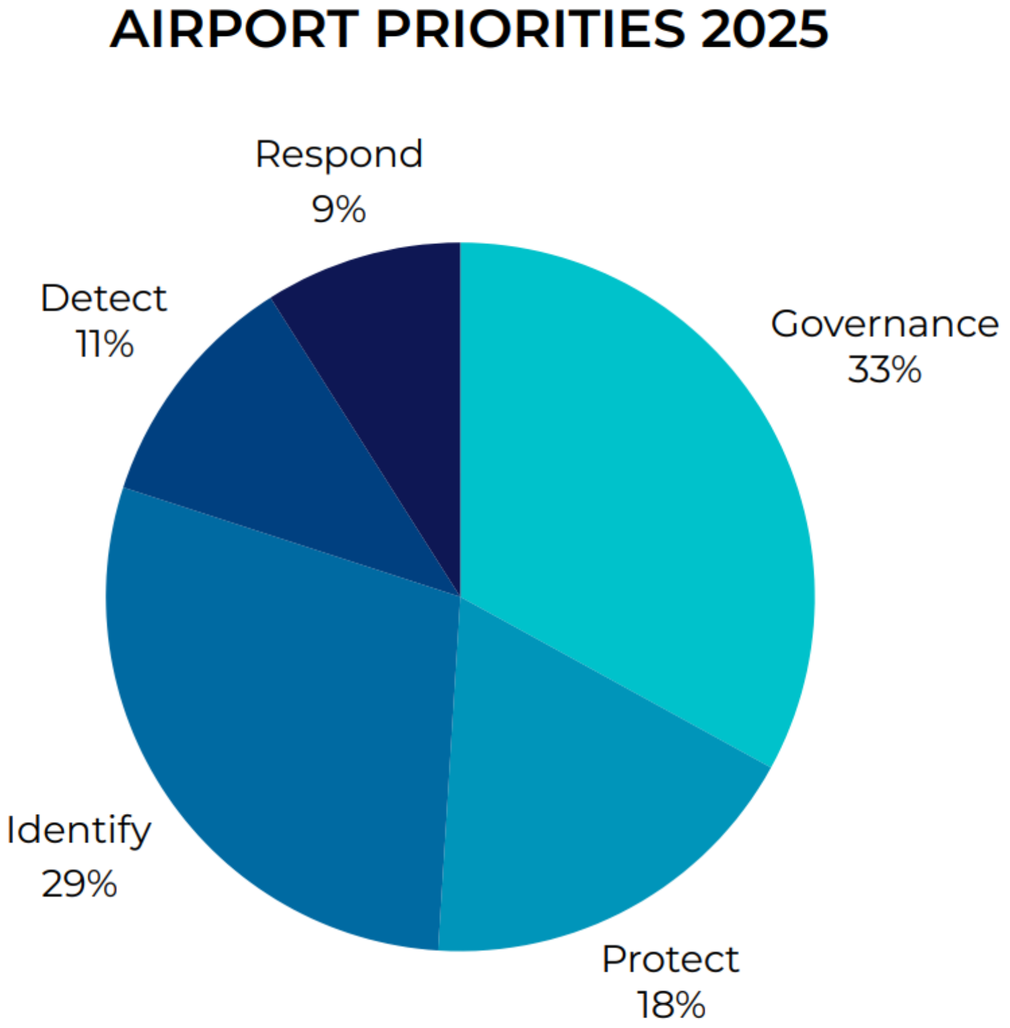
AVIATION ISAC

05 Detect: Continuous Monitoring

CISOs noted several environmental factors which are driving continuous monitoring initiatives. Many CISOs have had the same SIEM toolsets in place for five or more years and are open to looking at new vendors. The integration and/or planned integration of artificial intelligence into many security tools is also driving reviews into replacement of security operations center tooling and network monitoring tools.

Industry Segment Priorities

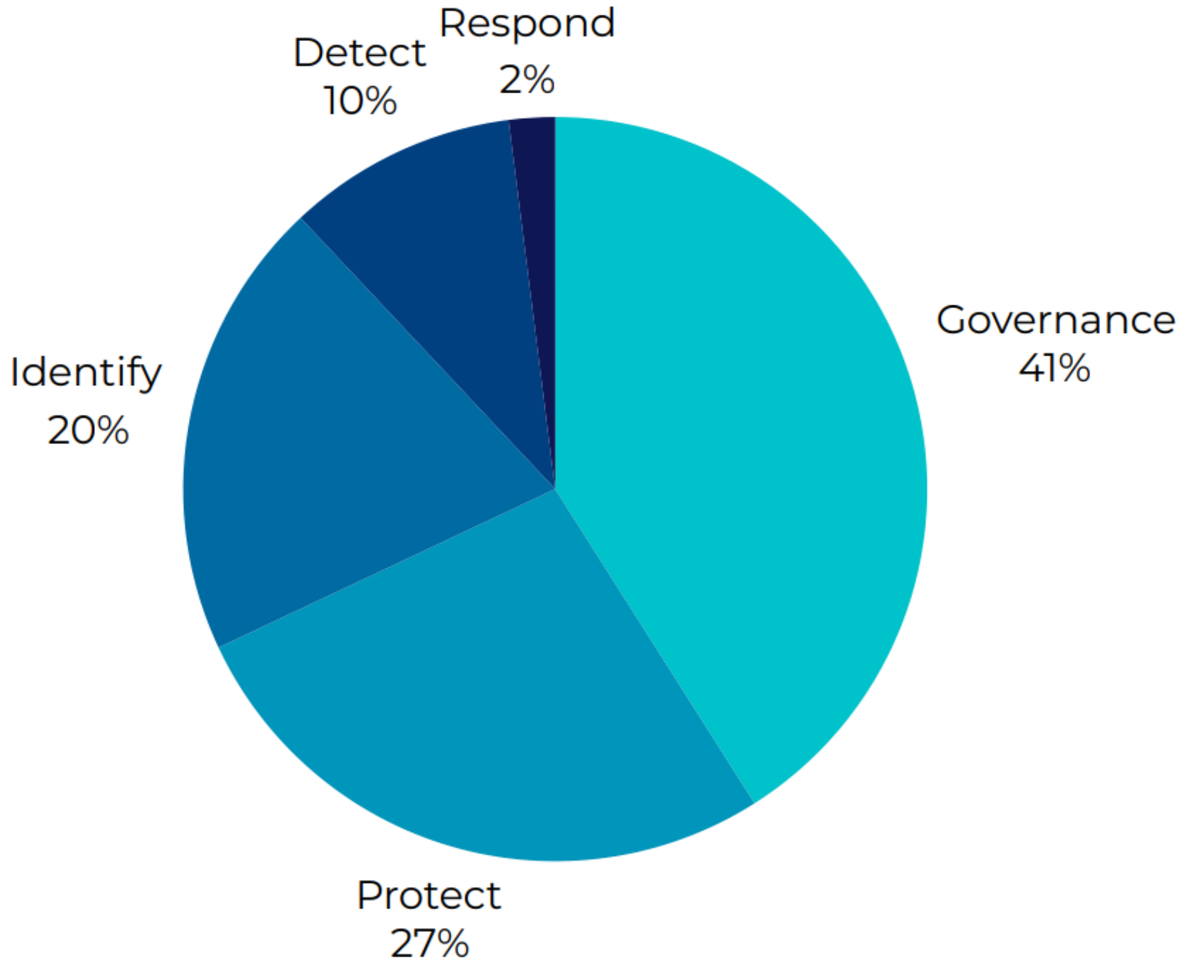
AVIATION ISAC



Industry Segment Priorities

AVIATION ISAC

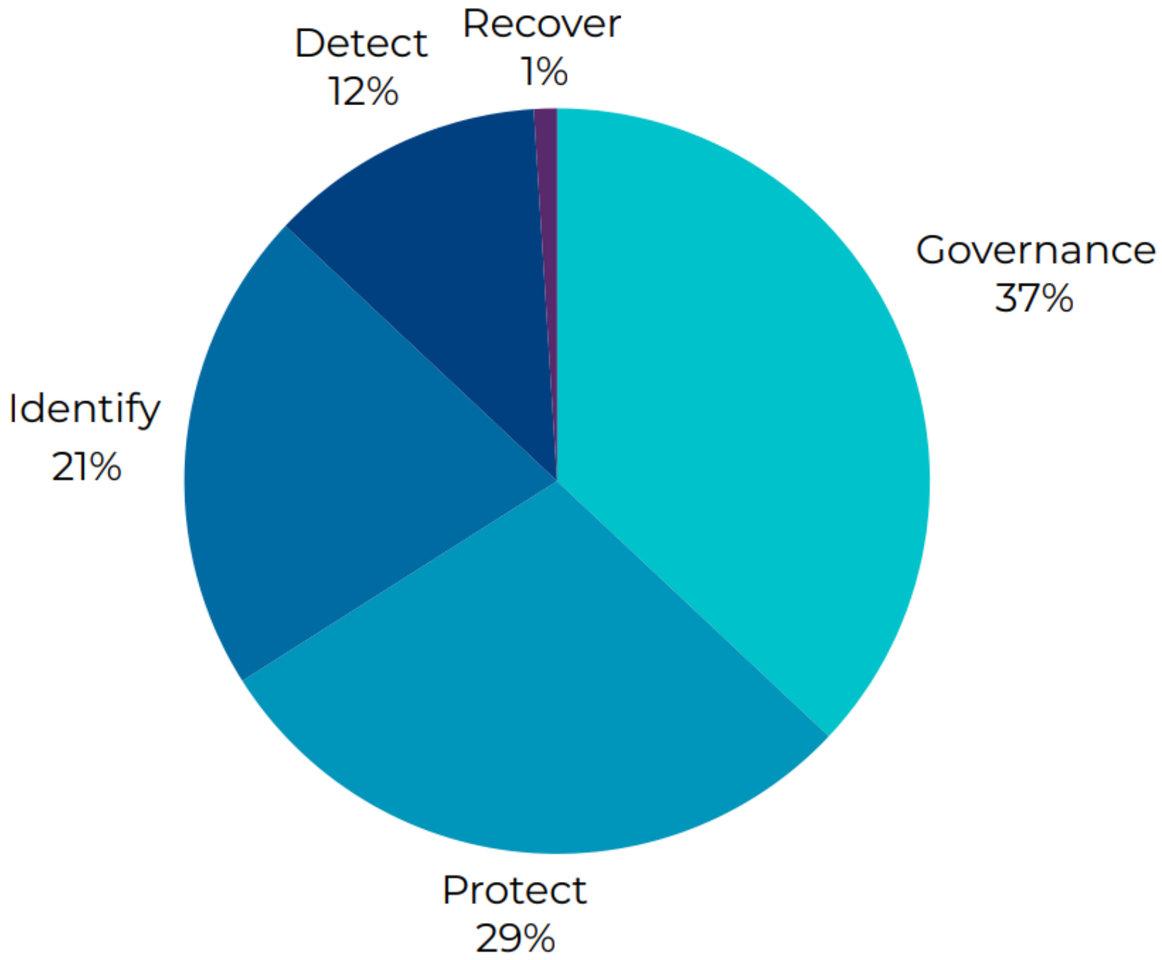
OEM/SERVICE PROVIDER PRIORITIES 2025



Industry Segment Priorities

AVIATION ISAC

AIRLINE PRIORITIES 2025



Summary

Cyber resilience in aviation demands a unified, community-wide commitment. At Aviation ISAC, we are a dedicated community driven by a shared passion for aviation and a commitment to safeguarding the industry. Our goal is to ensure a level playing field where companies can operate without the disruption of cyber threats.

We provide a safe and trusted platform for sharing cyber threat intelligence and developing best practices to protect, detect, respond to, and mitigate cyber-attacks. To learn more about joining our community, visit us at https://www.a-isac.com

Questions?

Contact Information

Aviation ISAC

https://www.a-isac.com

APAC Contact

Nickelby Thane

Regional Information Security Manager

nthane@a-isac.com / +61 468 458 897