AVIATION ISAC

CISO SURVEY RESULTS

2023

CONTENTS

EXECUTIVE SUMMARY

The aviation sector is deemed critical infrastructure in many countries around the world. Each year, billions of people and hundreds of billions in cargo revenue are transported safely, enabling economic growth, and bringing the world together. There is a growing digital footprint as e-enablement creates more and more efficiencies in the global aviation sector. Daily, our sector comes under attack from threat actors who, for political, financial, or other reasons, seek to disrupt or degrade the aviation industry.

Welcome to the sixth anniversary edition of the Aviation Information Sharing and Analysis Center, Inc.'s Cyber Risk Survey. The Aviation ISAC (A-ISAC) is a global, nonprofit community of airlines, airports, original equipment manufacturers, and service providers. Our members are committed to safety and cybersecurity in the global aviation ecosystem. 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 focus for our members.

How do we receive the data? Each year we survey Chief Information Security Officers (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 2023 to reduce cyber risk?"

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

What did we learn? This year the cyber risk reduction efforts across the global aviation industry, as represented by our participating members, are focused on the Protect and Identify functions. This is consistent with prior years, however, there is a significant growth in this emphasis from 2021, growing from 57% in 2021 to 75% heading into 2023. The focal categories for 2023 are Identity Management, Authentication, Access Control, Data Security, Asset Management, Awareness and Training, and Supply Chain Risk Management.

Insights on other notable initiatives were also provided for the CSF categories of Continuous Monitoring and Governance, along with efforts in the Respond and Recover functions. Finally, we present year-over- year analysis of the results by the overall industry and by industry segment.

What is the NIST Cybersecurity Framework? The NIST Cybersecurity Framework integrates industry standards and best practices to help organizations manage their cybersecurity risks. It provides a common language that allows staff at all levels within an organization—and at all points in a supply chain—to develop a shared understanding of their cybersecurity risks. NIST worked with private-sector and government experts to create the Framework, which was released in early 2014.

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

SURVEY RESULTS

This year, approximately 40% of Aviation ISAC members participated in the annual, one question survey. The question is quite simple and direct, “What are the three to five things you committed to getting done in 2023 to reduce cyber risk?” We tabulate and analyze the results from several perspectives. We look at overall responses by function (Identify, Protect, Detect, Respond, and Recover), category and sub-category. Each year, some responses do not fit into the NIST Framework, but are critical to the creation and health of a good cyber team. This year, Identity Management (IDM) was again the number one focus. During our survey interviews, some member companies noted that IDM work is of such importance that it is no longer considered a project to highlight, rather it is critical daily work. IDM gets more complex as networks expand to the cloud, networks become more segmented, and supply chain risk is addressed.

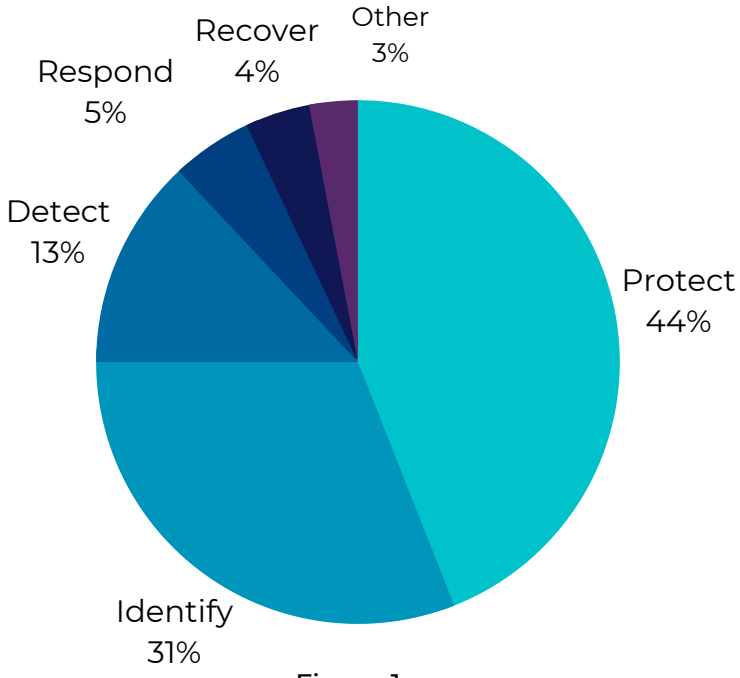


Figure 1

Figure 1 reveals the percentage of initiatives identified by NIST CSF Function. Protect was the most frequently mentioned function within which the CISOs are focusing their efforts. Protect was followed in descending order by Identify, Detect, Respond and Recover. The final category represents critical initiatives necessary to run a cybersecurity program, but not a part of the NIST CSF. This year those were diverse hiring initiatives and increasing the skillsets of the staff.

Details on the categories, subcategories and specific projects mentioned are provided further in this report. The NIST CSF has significantly less categories and subcategories in the respond and recover functions, thus it is expected that we would see less initiatives in these areas. Conversely, a significant increase in these categories demonstrates the importance of the work being done. There was a notable jump from 1% to 3% in projects in the Recover function. These efforts are called out in the “Other Notable Responses” section below.

WORD CLOUD

Our word cloud depiction is derived from the cumulative narratives of the CISO interviews. It emphasizes the growing challenges in management of cyber programs. “Managing to align with a framework” or “address compliancy matters” were frequently mentioned. We continue to see the trend of moving more and more of the network to the cloud and more challenges for companies with the dramatic increase of work attributed to compliance with regulation around network and operating technologies.

There was more discussion this year around strategic management of cyber programs. CISOs described a growing desire to be aligned to frameworks as a part of their strategic management efforts, as indicated by the word “Mapped.” Similarly, mapping was referred to as part of the growing burden of regulatory compliance.
Third-party risk and ransomware also continue to bubble up as concerns, driving much of the work in 2023.

TOP 5 CATEGORIES OF RISK REDUCTION EFFORTS

01 Protect: Identity Management, Authentication, & Access Control

02 Protect: Data Security

03 Identify: Asset Management

04 Protect: Awareness and Training

05 Identify: Supply Chain Risk Management

Details on the categories, subcategories and specific projects mentioned are provided further in this report. The NIST CSF has significantly less categories and subcategories in the respond and recover functions, thus it is expected that we would see less initiatives in these areas. Conversely, a significant increase in these categories demonstrates the importance of the work being done. There was a notable jump from 1% to 3% in projects in the Recover function. These efforts are called out in the "Other Notable Responses" section below.

01 Protect: Identity Management, Authentication, & Access Control

Your employees' corporate accounts are the doorways into your organization's data vault and your employees' credentials are the keys.[1] Consistent with prior years IDM remains the top priority for our members. Quite simply, IDM is complicated. Many companies have devised multi-year strategies to improve account management. These strategies are complex as CISOs attempt to manage on-prem, cloud and OT networks. There are also challenges in balancing segmentation projects and implementing least privilege with the business' drive to increase collaboration across functions.

Aviation companies are most focused on three IDM subcategories: PR.AC-1 credential management, PR.AC-5 network integrity, and PR.AC-4 authentication.

[1] https://expertinsights.com/insights/50-identity-and-access-security-stats-you-should-know/

PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	24%
PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	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)	24%
PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	15%
PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	9%
PR.AC-3: Remote access is managed	3%

PR.AC-1: CISOs are working on efforts to reduce the number of service and privileged accounts and increase security on those accounts. They are increasing the complexity of passwords, standardizing credentials across platforms, and improving security around portals accessible to customers. Companies mentioned that IDM security improvements are often multi-year efforts.

PR-AC-5: Many companies are continuing work on multi-year segmentation projects. These include segmenting the network to reduce the impact of a breach, such as ransomware events. Others noted continued efforts to remove OT controls from the legacy network. Companies are also working on micro-segmentation projects.

PR.AC-7: Projects which aligned to this subcategory were primarily multi-factor authentication (MFA) projects. One member advised they are looking into biometric characteristics as a form of MFA. CISOs also mentioned MFA on servers and continuation of efforts to increase security on legacy applications.

PR.AC-4: Several CISOs working on privileged access management (PAM) initiatives advised they are looking to upgrade or switch over to a new vendor for PAM.

02 Protect: Data Security

"Information is the oil of the 21st century," said Peter Sondergaard, Senior Vice President and Global Head of Research at Gartner, Inc. We are seeing dramatic growth in regulation on data privacy protection and breach reporting. We continue to see threat actors selling personal data on the dark web and use it for second stage ransoms. We also see a growing threat to intellectual property as geopolitical tensions drive countries to build their own aviation industries. Three data security sub-categories aligned with the highest priority efforts in Data Security: PR.DS-5 protecting against data leaks, PR.DS-2 protecting data in transit, and PR.DS-1 protecting data at rest.

PR.DS-5: Protections against data leaks are implemented	44%
PR.DS-2: Data-in-transit is protected	28%
PR.DS-1: Data-at-rest is protected	20%
PR.DS-4: Adequate capacity to ensure availability is maintained	4%
PR.DS-7: The development and testing environment(s) are separate from the production environment	4%

PR.DS-5: A broad range of projects were identified in this category. Companies continue to refine their insider threat programs. One member stated, “Can see [insider attacks] happen now, but want to prevent [them] from happening.” Others are formalizing their DLP programs and adding additional layers of protection.

PR.DS-2 and PR.DS-1: Projects discussed in these categories primarily related to cloud.

03 Identify: Asset Management

Socrates once said, “To know thyself is the beginning of wisdom.” Likewise, to know thy networks, and all digital functionality is core to thy business. These are foundational elements to the wisdom of every cybersecurity strategy. Asset management was the third most noted area of emphasis for 2023.

ID.AM-1: Physical devices and systems within the organization are inventoried	26%
ID.AM-2: Software platforms and applications within the organization are inventoried	26%
ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	17%
ID.AM-3: Organizational communication and data flows are mapped	13%
ID.AM-4: External information systems are catalogued	9%
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	9%

Respondents provided insight into projects across many of the subcategories within asset management. Shadow IT continues to keep CISOs up at night. Referring to a 2023 initiative, one CISO stated, “We will conduct embarrassing network sweeps.” Knowing what is on the network is foundational to protect, detect and vulnerability management.

In addition to employing tools to illuminate the network, CISOs mentioned efforts to map business practices and data flows to assets and applications.

The final category from the chart above, ID.AM-6, roles and responsibilities, ties in well with the fourth most prevalent category, Awareness and Training.

04 Protect: Awareness and Training

Cybersecurity is a team sport. The job of a CISO is to get everyone on the team to understand the big picture, understand their role, own it, and to communicate with the rest of the team. “What lies in our power to do, lies in our power not to do.” – Aristotle. CISOs overwhelmingly discussed initiatives to educate the business and key suppliers on what lies within their power to do, and not do, to reduce cyber security risk at their companies. There has been a growing movement to get every employee in the business to understand their role in the cybersecurity strategy.

PR.AT-1: All users are informed and trained	40%
PR.AT-2: Privileged users understand their roles and responsibilities	25%
PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	15%
PR.AT-4: Senior executives understand their roles and responsibilities	10%
PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities	10%

Initiatives to increase awareness identified during the interviews of CISO included:

- Enhanced social engineering and frequency of phishing tests
- Targeted training for privileged users
- Increased training on both physical and cyber risks to data protection
- Leveraging recent breaches in the industry to increase the conversations
- Updating Incident Response Plans through engagement with the business
- Conducting more tabletop exercises

05 Identify: Supply Chain Risk Management

Last year was the first year Supply Chain Risk Management (SCRM) made it into the top five areas of effort in our industry. In 2022, we observed an increase in supply chain attacks and we expect more of the same in 2023.

Of the four SCRM subcategories in the NIST CSF, two aligned well to the SCRM initiatives detailed by our members, IS.SC 1 and 2.

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	56%
ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	25%

The responses focused on two types of initiatives: leveraging third party vendor assessments and working on creating a shared assessment process. Outsourcing vendor assessments in whole or in part is a growing trend. Several vendors have well recognized programs. There is a growing acceptance toward the concept of shared assessments. One driver is the increased amount of regulation which will require companies to have a better handle on the cybersecurity posture of key vendors. Shared assessment programs present the opportunity for significant cost savings among companies that use common suppliers. Leveraging shared assessments, a company can achieve significant economies of scale and include more vendors in their assessment programs. These programs also reduce the cost and burden on the common supplier.

Other Notable Responses from the Survey

A significant number of important initiatives were identified across many of the CSF categories. Highlights from this next tier include many projects noted in the categories of Security and Continuous Monitoring; and Governance. Also, projects were noted in the categories of Improvements and Communications in both the Respond and Recover functions.

DE.CM Security and Continuous Monitoring

Many of the respondents explained they were working to upgrade their SIEMs - considering switching SIEM vendors and or adding functionality. Several spoke of increasing the number of sources which go into their SIEMs. Additional log sources included those from OT assets and even some third-party logs. Some members outsource their L1 and L2 event resolution and advised they were considering moves to new vendors for cost savings or better expertise.

Following on to their move to the cloud, members were also considering cloud monitoring tools native to the cloud vendor and a cloud security operations center. Members were increasing their red team testing as a part of their network monitoring programs. An increase in monitoring for insider threat was also mentioned by several members.

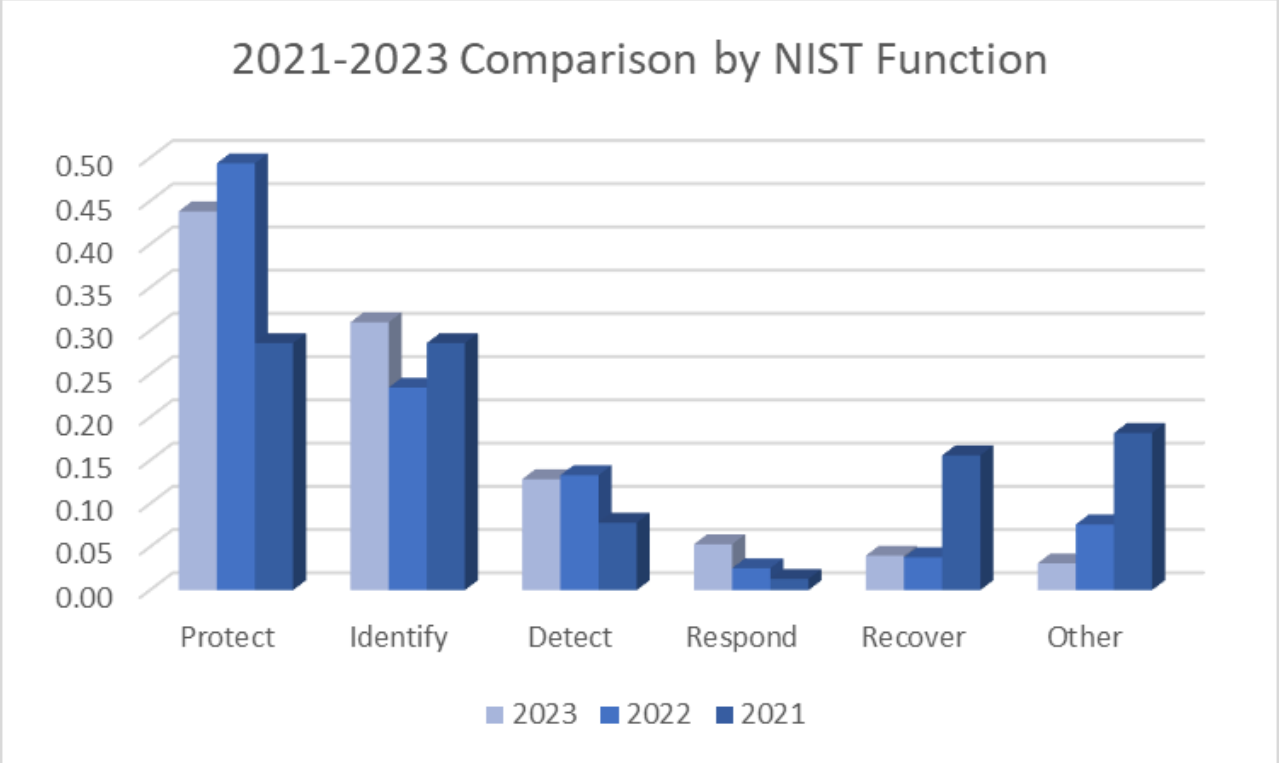
ID.GV Governance
Members discussed their strategies and initiatives to address the growing regulatory compliance burdens. Some members advised they would be engaging at the International Civil Aviation Organization level and/or with their governments as more regulations are drafted and acceptable means of compliance are defined.

Members also mentioned initiatives to align their cyber programs to NIST, Mitre, and other, sometimes custom, frameworks.

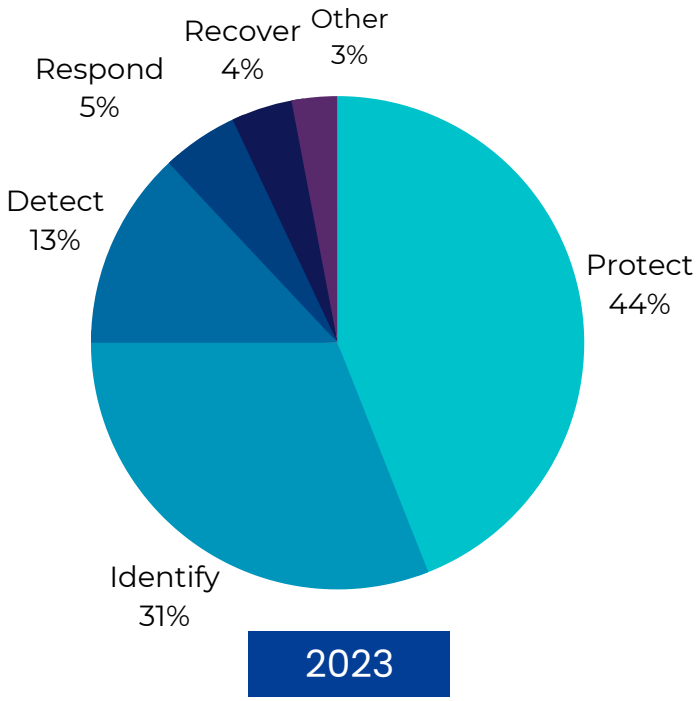
RS.CM/IM Respond Communications and Improvements
Members noted efforts to refine response plans in areas such as ensuring all employees understand their roles, improve communications with the board, and improve information sharing with the Aviation ISAC and other communities.

RC.CO/RC.IM Recover Communications/Improvements
Improving the quality of systems which back up the networks was most frequently mentioned. Members discussed looking at new solutions with an eye toward reducing the amount of time it takes to restore business functionality from the backups. One member noted that the government regulators were currently focusing on restoration capability of aviation critical national infrastructure.

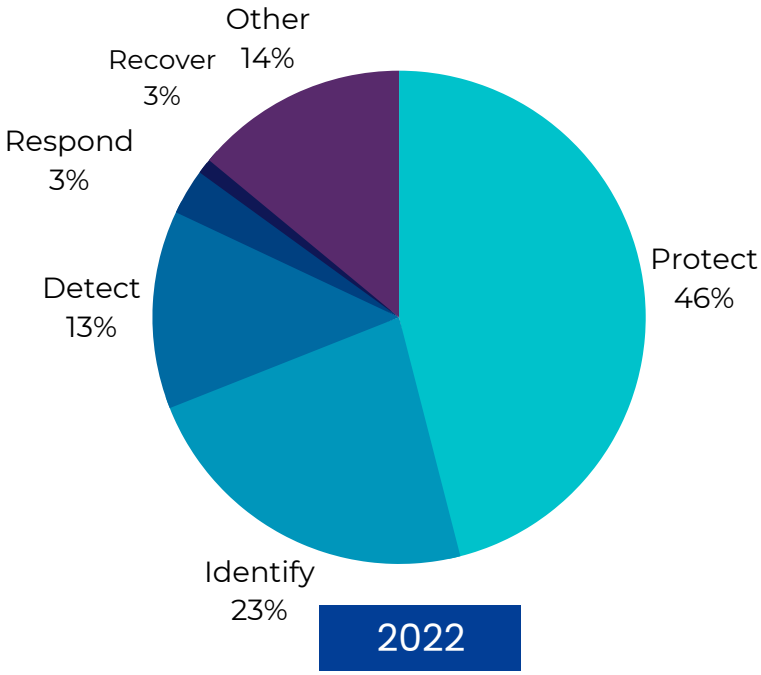
TOP 5 YEAR OVER YEAR



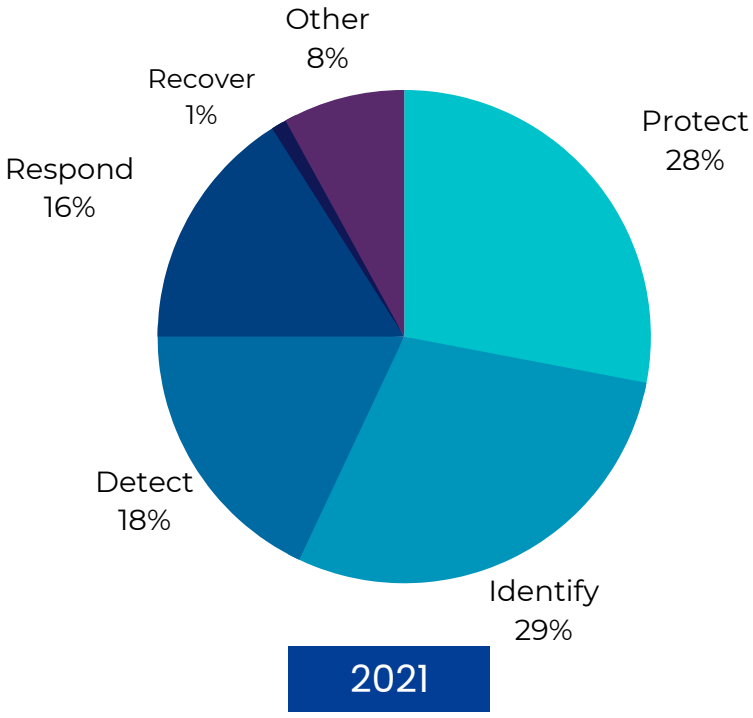
All Segments



2023



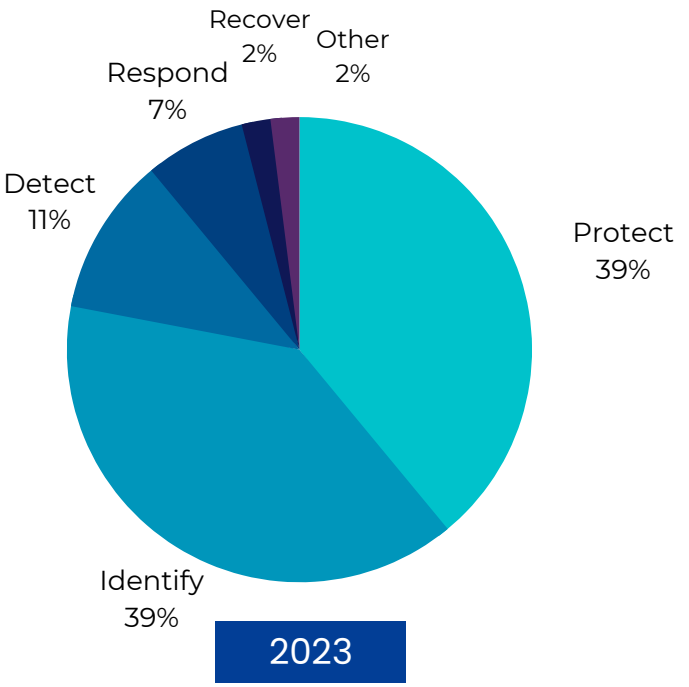
2022



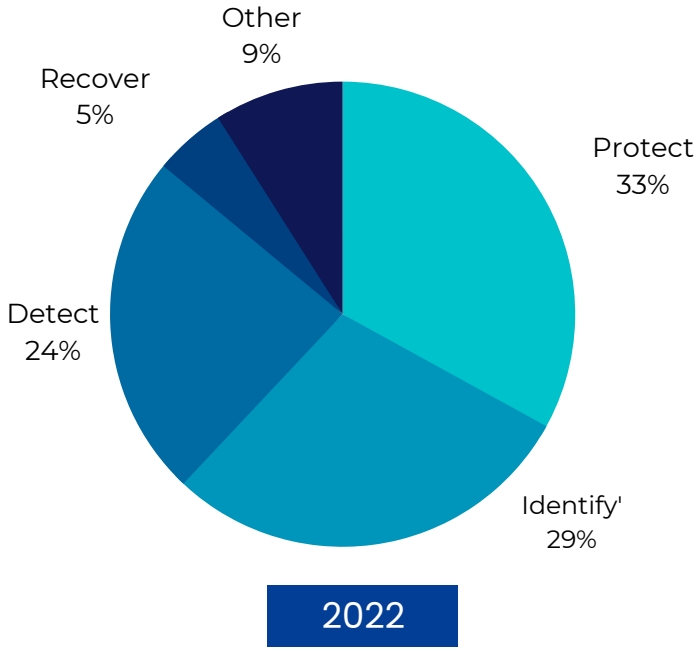
2021

In comparison to the past two years, efforts in the Protect and Identify functions are growing and increasingly dominate the attention of CISOs and their teams. The growth in the emphasis on projects in these areas has increased from 57% in 2021, to 75% in 2023. Efforts in the detect function seem to be constant at about 13%. Initiatives in the respond category rebounded for 2023. Members noted that some of this work was driven by lessons learned from specific and industry impacting breaches in 2022.

Airports



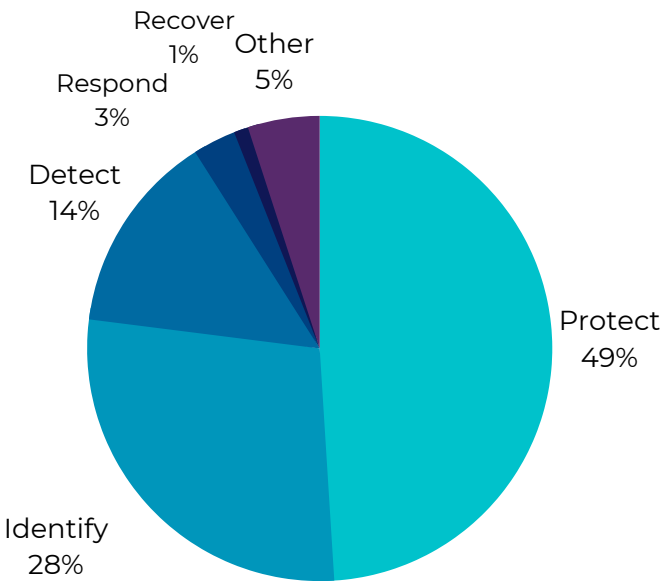
2023



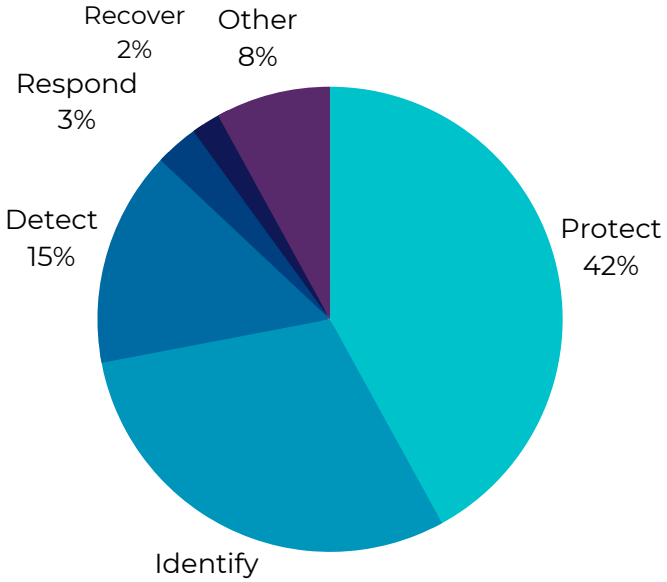
2022

Year over year, Protect, Identify, and Detect initiatives, in that order, remain the top 3 areas of emphasis for the majority or our airport member companies. Heading into 2023, there was a significant shift in efforts towards initiatives in the Identify function. Those Identify categories, by volume, were in Asset Management, Governance, and Risk Assessment.

Original Equipment Manufacturers (OEM)/Services (Svc):



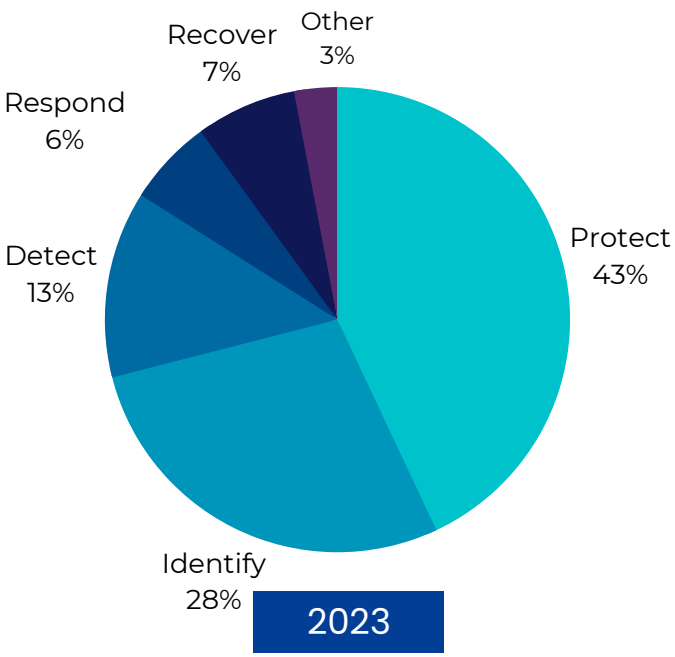
2023

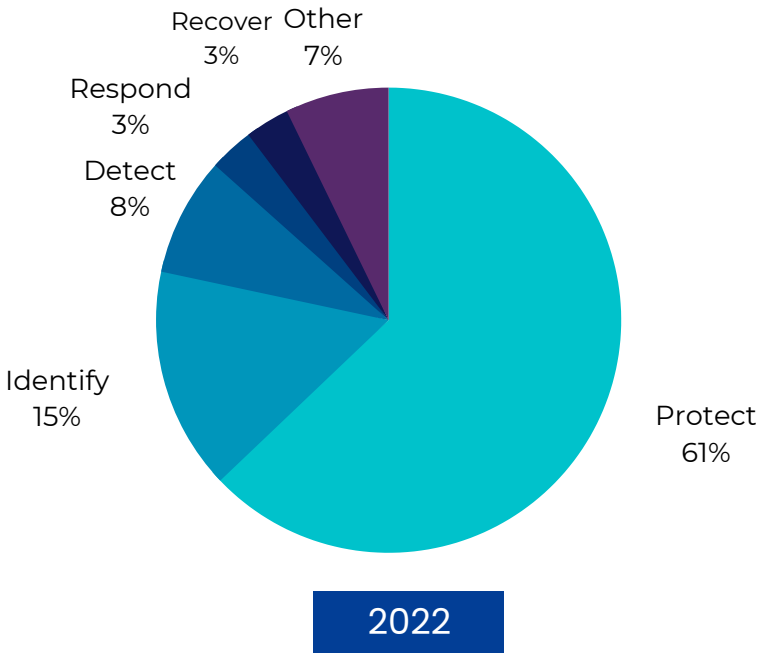


2022

Year over year the emphasis on cyber risk reduction has remained constant in the OEM/Svc segment, with an overwhelming focus on Protect and Identity functions.

Airlines





In 2023 the airline segment shifted significant efforts into the Identify function. The efforts were mostly in the Asset Management, Governance, and Risk Assessment subcategories. There was also an increase in initiatives in Detect. Members talked about increasing coverage with new tools. Some members were considering switching up their commercial tool line-up and/or their MSSP.

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 the Aviation industry in benchmarking their cyber security strategies, program maturity, and management of resources.

We want to thank the many CISOs who took the time to share their thoughts and strategies for 2023.

ACKNOWLEDGEMENTS

Cybersecurity is a team sport. The Aviation ISAC is a community of passionate people. Passionate about aviation. Passionate about ensuring there is a level playing field for companies to operate in the aviation industry unencumbered by the malicious acts of cyber attackers.

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