AVIATION ISAC

Annual Cyber Risk Survey

of

Aviation Cybersecurity Leaders

2021 edition

TLP WHITE

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Executive Summary

Our industry had its most challenging year ever in 2020. The pandemic drove a global slowdown in air travel yet there was no decrease in the level of attacks against networks, operational technologies, and products. Similarly, the Aviation ISAC noted an increase in engagement with security researchers which positively contributed to cyber risk reduction.

For the fourth year in a row, the Aviation ISAC conducted its annual Cyber Risk Survey of member company Chief Information Security Officers (CISOs) and Product Security Executives (PSEs) to identify their most pressing cybersecurity risks and challenges. The 2021 Cyber Risk Survey reflects the thought leadership of our community. The survey revealed CISO and PSE current priorities are in line with the changing threat landscape and financial challenges that emerged in 2020. Conducted via phone interviews and email by the Aviation ISAC, the survey took place in December 2020, just prior to the public announcement of the Solar Winds breach. This sophisticated and complex supply chain attack has necessitated a pivot to address risks within the software supply chain that is not reflected in this report.

Several changes were made to the survey process this year. In years past, the survey was conducted solely via personal interviews. This year, the Aviation ISAC collected responses by personal interview and email. This year, we expanded the survey to include Product Security Executives (PSEs) based on the importance of product security in last year's survey. Responses from PSEs were analyzed separately from CISO responses. Thirty-seven respondents representing thirty-six member companies participated in the survey. This represents 43 percent of the total Aviation ISAC membership. The fourth annual survey results are distinctly different from previous years. In 2020, survey participants identified Product Security as their second-highest cybersecurity priority. For two years, Aviation ISAC member companies have been addressing the many product security issues through the A-ISAC Product Security Working Group. Accordingly, this year's survey separated Product Security as a separate risk management function. Back-to-Basics was eliminated as a category; projects identified as such were allocated to more specific categories such as asset management, security awareness, vulnerability management, and so forth. Two new

categories of concern emerged this year: financial management and securing the industry. Additionally, five respondents identified ransomware as a significant concern driving their setting of priorities.

Top Five Priorities for Aviation ISAC Member Company CISOs in 2021

1. Security Operations Center
2. Identity & Access Management
3. Culture & Organizational Security Shift
4. Network Transformation
5. Asset/Vulnerability Management

Projects in these areas accounted for 55 percent of total responses and were ranked as Tier One priorities. Additional priorities were ranked into second and third tiers.

As mentioned, the 2021 survey is the first to include PSEs. As a result, PSE engagement was low, with just five member company PSEs responding to the survey. The two areas of concern most frequently mentioned by these respondents are: (1) Maturing VDP programs and engaging with Security Researchers and Increasing airlines ability to test at manufacturer labs. The other responses are identified further in this report. We anticipate that PSE participation will increase in future surveys.

The purpose of this report is to increase aviation industry CISO and PSE cybersecurity awareness and provide the ability to benchmark their 2021 priorities against their peers. The Aviation ISAC will use the results of this survey to guide the initiatives of its roundtables, working groups, and analyst communities. We sincerely appreciate the participants who shared their industry views and their priorities for the coming year.

Top Five CISO Priorities

Thirty-six A-ISAC member company CISOs responded to the survey. This represents approximately 38 percent of the Aviation ISAC membership. Thirty-one CISOs were interviewed, and an additional four provided email responses. Survey participants represented the industry as follows:

Airports: 9 Airlines: 14 Manufacturers and service providers: 13

A total of 127 priorities were identified for 2021, for an average of 4.1 priorities identified per CISO. Seventy-two priorities (57 percent) make up the top five categories:

Security Operations Center (17)

Identity and Access Management (16)

Cultural and Organizational Shift (15)

Network Transformation (13)

Asset and Vulnerability Management (11)

Security Operations Center

Seven sub-topics were identified in the SOC category. The most prevalent priority is to improve incident response, including the automation of elements of the incident response function. The next priority areas are equally ranked: centralize cyber security functions across the company; build new SIEM to work with detection tools; implement metrics using the MITRE ATT&CK framework; and improve SOC team skills. It was noted during the survey that two member companies which had outsourced their SOCs over the past few years reversed course and brought their SOCs back in-house.

Identity and Access Management

In the 2020 Survey, one member company highlighted Identity and Access Management (IAM) as "the new perimeter." In this year's survey, thirteen member companies identified IAM as a top priority. All aspects of IAM, including active directory rebuilds and consolidation and multi-factor authentication rollouts were identified as priority projects. It should be noted that five survey respondents stated ransomware attacks are motivating their project prioritizations. Concurrently, the Aviation ISAC has frequently seen ransomware groups using active directory attacks as an element to facilitate lateral movement by ransomware groups.

Cultural and Organizational Shift

Cultural and Organizational Shift was the topic of great discussions in the February 2020 A-ISAC CISO roundtables and was identified as a top-five priority in this year's survey. Respondent CISOs are partnering more with business units to promote an organization-wide culture of security. Everyone's job is security. Clearly the CISOs in our industry are embracing their role as the company evangelists for Cyber Security across the entire business enterprise. The high prioritization of changing culture within our member companies aligns well with the International Civil Aviation Organization's initiative that declared 2020 and 2021 "The Year of Security Culture."

Initiatives aligned to this priority are to increase awareness, drive ownership, and enable the business to engage in better security practices. As CISOs provide more information about vulnerabilities to business units, they are leading product and application development teams, along with the infrastructure owners, to embed security in the development of products/applications and system builds.

Network Transformation

Migration to the cloud continues for many A-ISAC member companies. Respondents identified the challenge of creating the right suite of security tools to monitor the cloud and legacy networks. This increase in required tools creates cost pressure and requires additional skills and/or training for security teams. In addition, network segmentation is growing as a strategic play to minimize the impact of breaches and other unauthorized access attempts.

Asset and Vulnerability Management

Asset and Vulnerability Management (AVM) moved into the top five this year; in 2020 it was sixth. Respondents identified AVM as a core competency, an essential function, and a key component to their programs. In the past year, more than 25,000 Common Vulnerabilities and Exposures (CVE) were published. Bad actors look to build exploits for these vulnerabilities as swiftly as possible, with the intent to compromise entities that are slow to patch. The increase in CVEs is attributed to an increase in researchers and products being tested. Vulnerability management metrics, to include number of days a known critical vulnerability has gone unpatched, are driving more attention to the performance of AVM teams at A-ISAC member companies.

Tier Two Priorities

Following after the Tier One Top Five priorities discussed, the following nine priorities (39 percent) were identified:

1. Personnel (9)
2. Data Security (7)
3. Financial Management (6)
4. Operations Technology (6)
5. Risk Management (6)
6. Joint Venture and Supplier Risk (5)
7. Endpoint Security (4)
8. Threat Intelligence (4)
9. Compliance (3)

Personnel

Retention, skills development, and alignment with roles took the number six spot this year, and is an area of great concern for many of the CISOs. Respondents noted the challenges of retention in a year of budget locks and staffing and salary reductions. Survey participants also noted that restrictions on training dollars will make it more difficult to increase some staff skillsets.

Data Security

Priorities centered on three areas. Implementation of Data Loss Prevention tools was the most frequently identified initiative, followed by reducing the number of systems holding sensitive data and implementing encryption at rest.

Financial Management

New this year, Financial Management emerged as a top priority due to the pandemic-fueled industry slowdown. In the best-case scenarios, budgets were frozen. Many member companies have had to reduce cyber staff, put personnel on reduced work weeks, eliminate contractors, and take other cost saving actions.

Operations Technology

Four initiatives are called out to counter cyber risk in Operations Technology (OT). Two member companies are building continuous monitoring capabilities in their OT environments, and two airline member companies are looking across their businesses to identify and harden all OT systems, including aircraft. Respondents are also looking to improve OT security design and harden OT endpoints.

Risk Management

Numerous CISOs talked about their desire to better identify and leverage Key Performance Indicators (KPIs) to drive improvement and demonstrate maturity in risk management programs. One member mentioned the mapping of all events to the MITRE ATT&CK framework. Another discussed leveraging KPI metrics to work with suppliers on reducing supply chain risk. In late 2020, the Aviation ISAC rolled out a strategy to map its threat landscape to a yet-to-be-determined framework for each working group. The goal of this effort is to better identify and manage success in closing collective gaps.

Joint Venture and Supplier Risk

As mentioned in the Executive Summary, the Solar Winds breach and software contamination occurred just after the survey interviews were completed. The impact of this event underscores the importance of continuously monitoring the threat landscape to ensure incident response teams can instantly pivot to address new attack vectors. Based on the Solar Winds incident, the A-ISAC posits that Joint Venture and Supplier Risk would have ranked much higher had the survey been conducted in January.

Endpoint Security

Three projects were identified to harden endpoint security: (1) identifying and implementing Endpoint Detection and Response (EDR) capability on Linux systems; (2) pivoting to a new anti-virus solution; and (3) implementing virtual desktops as a component of an end-user computing strategy in a zero-trust environment.

Threat Intelligence

Initiatives in this category focus mainly on automation. One member company respondent is focused on increased intelligence in anticipation of the 2021 Olympics. Over the past year, nineteen member companies leveraged the automated indicator sharing capabilities of the A-ISAC secure portal. The A-ISAC encourages its members to continue swiftly sharing key threat intelligence within the community.

Compliance

While mentioned just three times by survey respondents, Compliance received a high ranking due to the upward trend in compliance requirements. One respondent highlighted how compliance requirements are starting to require a disproportionate amount of staff time. The Aviation ISAC Compliance Working Group continues to identify emerging compliance requirements directly impacting aviation.

Tier Three Priorities

The remaining priority project categories identified by respondents are: Automation, Securing the Industry, and Continuity of Operations Planning (COOP). For the purposes of this survey, Security Automation was described as "automating delivery of security capabilities to the business units along with system upgrades." Securing the Industry included initiatives to reduce cyber risk in the global aviation network. Many of these initiatives involve partner organizations such as ICAO, Airlines Industry Association, Aerospace Industries and Defense, International Coordinating Council of Airline Industry Associations, IATA, and others. This category aligns with the PSE top priorities. Finally, COOP planning was noted as another initiative borne of concern over the spike in ransomware attacks.

Mapping Survey Results to NIST Framework

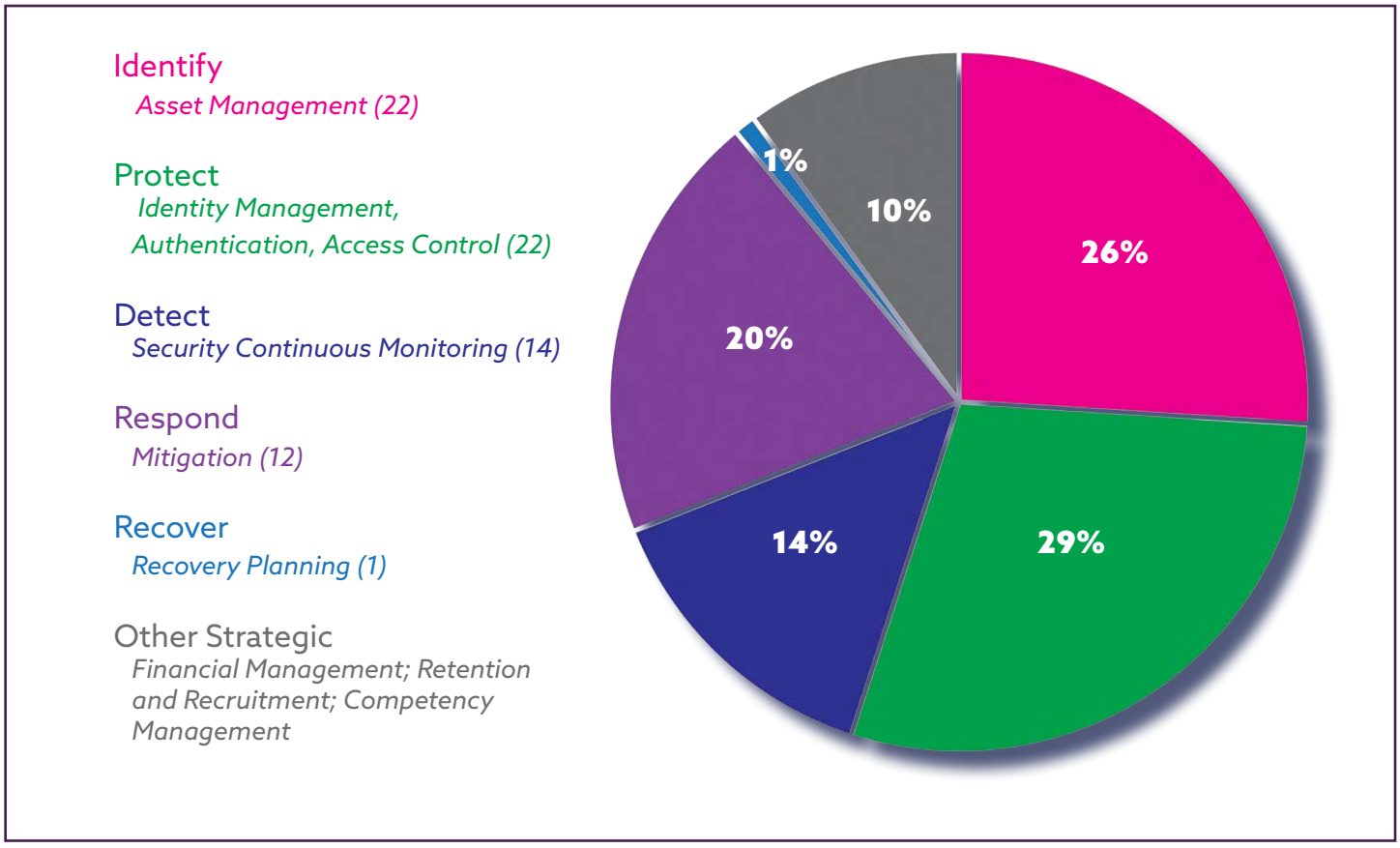
In the fourth quarter of 2020, the Aviation ISAC began a conversation about frameworks across its working groups and intelligence analyst community. Many members are using a variety of frameworks as strategic guides for risk reduction initiatives. As the A-ISAC community adopts the language and structure of frameworks, it will accelerate the delivery on initiatives and identify gaps in efforts.

In line with this organizational shift, the results of this year's survey were mapped to the NIST Cyber Security Framework. The mapping provided a different perspective on the results of the survey. the rank order of priority initiatives by frequency is:

- IDM
- Asset Management
- Mitigation
- Security Continuous Monitoring
- Recovery Planning

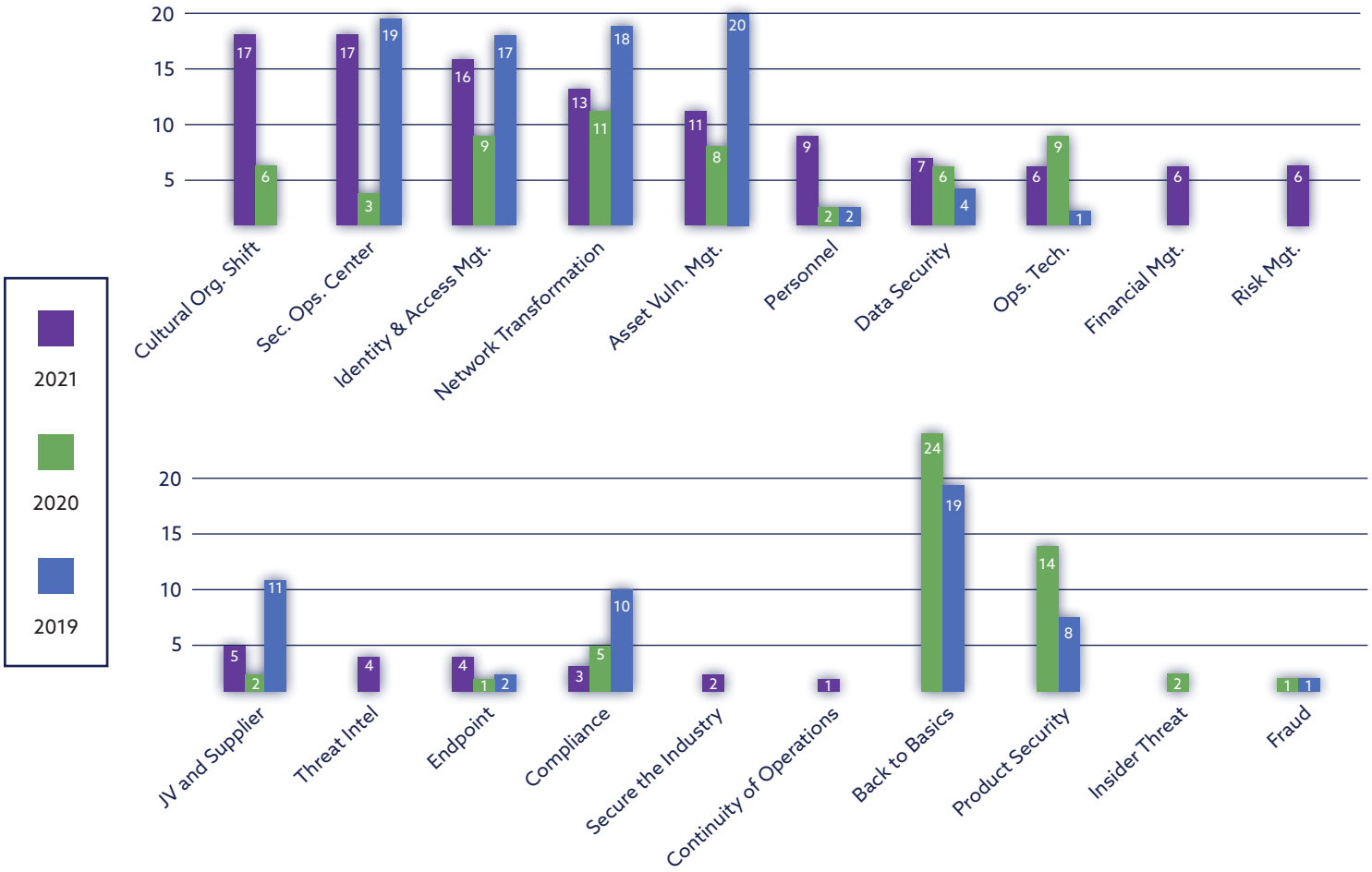
Ten percent of the priorities do not map directly to the framework and constitute priorities in personnel and financial management.

A-ISAC Cyber Risk Survey Plotted to NIST Framework



Year-Over-Year: 2019–2021

The year-over-year comparison reveals how aviation CISOs are sharply increasing their strategic engagement at both the company and industry levels. This shift is reflected by the increased focus on risk management, leading efforts to shift organizational culture toward a security mindset and engaging with partners and regulators to better secure the industry. The global COVID-19 pandemic delayed the implementation of some compliance requirements; this was reflected in the survey as few CISOs highlighted compliance as a priority. As the pandemic comes under control, the A-ISAC expects that efforts to increase aviation security via regulation will increase. Similarly, the emergence of ever-more supply chain issues will likely bring about further contractual compliance requirements.

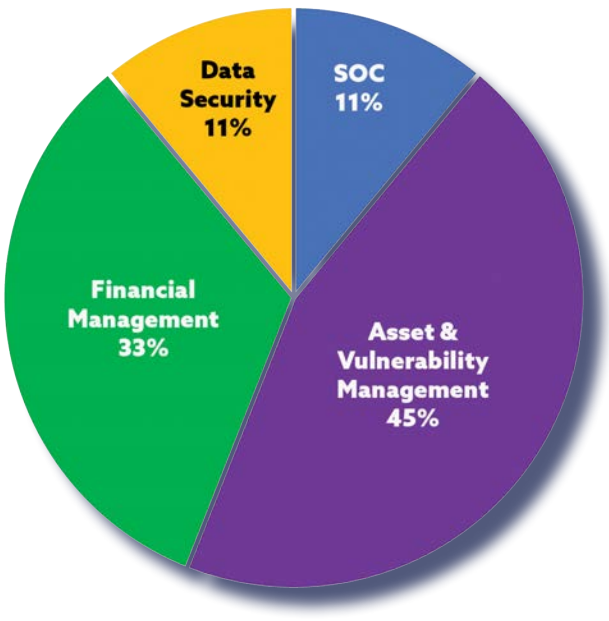


Priorities by Industry Segment

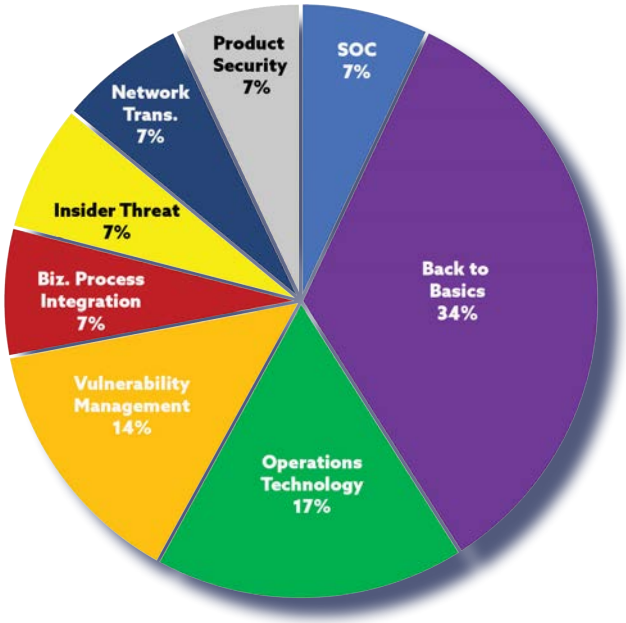
Airports

In 2021, eight airports responded to the survey, compared with ten in 2020. As previously noted, "Back to Basics" was broken out into more detailed areas this year which impacts year-over-year comparisons. The number of priority areas was much more uniform this year, as revealed by the fewer number of categories.

Asset and vulnerability management is the area most CISOs are focusing on in 2021. There was a significant reduction in Operations Technology as a 2021 topic, however, the AVM category includes identification and remediation of vulnerabilities in OT assets. The loss of revenue due to COVID-19 shutdowns impacted many airport cyber security staffs, resulting in the emergence of financial management as a Top Five priority. Building, expanding, and upgrading security operations centers is also a priority going into 2021.



Airports 2021



Airports 2020

Airlines

This year, fourteen airline member companies responded to the survey, compared to nine in 2021. While the elimination of "Back to Basics" has improved the clarity of survey results, it does impact the ability to provide a year-over-year comparison.

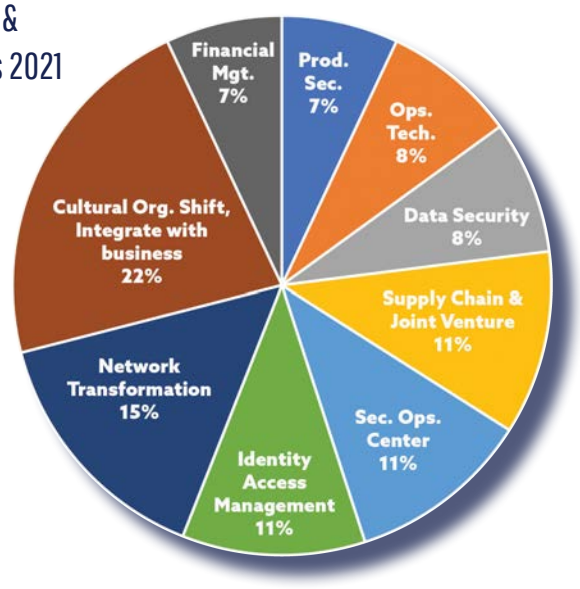
In 2021, IAM and SOC projects were most frequently highlighted by airline CISOs, followed closely by network transformation. This aligns with responses provided in the 2020 survey. Asset and vulnerability management and personnel concerns increased in priority across the airline segment.

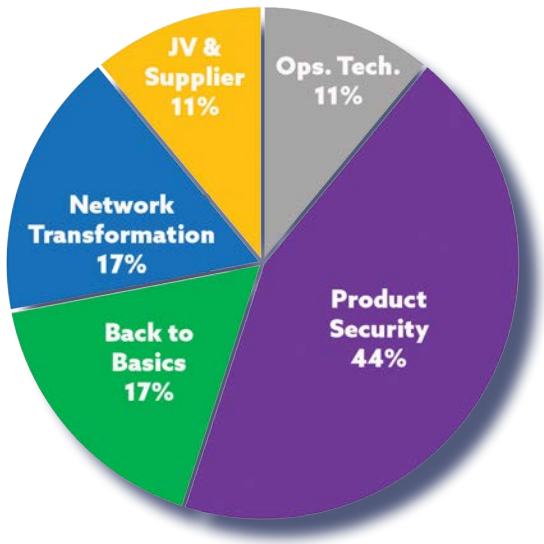
Original Equipment Manufacturers and Services

This year, eight original equipment manufacturer (OEM) and services CISOs responded to the survey, compared to seven in 2020. Product Security was ranked as the number one priority for this segment and was broken into its own category, discussed below. Back to Basics was eliminated as a category, and those projects were separated into their own respective areas. The analysis of this year's survey is filtered to address these changes.

Just as it was in 2020 for OEM and services member companies, network transformation remains the most frequently mentioned priority. The supply chain was also consistently identified as a high priority. In 2021, IAM and SOC projects ranked higher than previous years.

OEM & Services 2021





OEM & Services 2020

Product Security Priorities

Product security collaboration within the Aviation ISAC has increased dramatically over the past two years. This year, in light of the unique challenges in product versus network security, the Aviation ISAC broke out product security priorities from network priorities. Because this is a new feature of the annual survey, participation was limited. We anticipate stronger engagement with PSEs in future surveys.

The top two priorities were almost equally rated at ~28 percent of the responses:

Improve security researcher outreach and vulnerability disclosure programs

Increase airlines' ability to test cybersecurity of products at manufacturer's labs

The remaining priorities were equally rated but much lower, at 9 percent each:

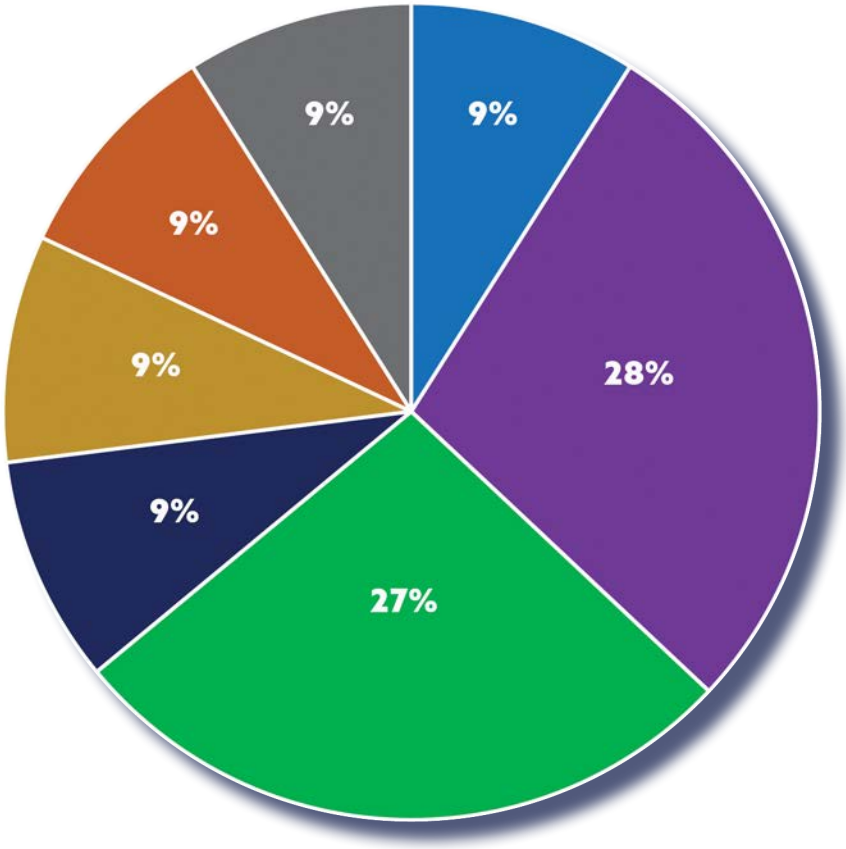
Create a best practices playbook

Influence regulators to create harmonized requirements

Secure the industry

Build a product certification program

Other



Summary

The aviation industry faced its most challenging year in 2020. Industry-wide financial constraints stressed cybersecurity staffing, programs, and initiatives, all while cyber attacks remained high. Ransomware attacks and their related impacts affected not only aviation, but all industries. Ransomware threats were mentioned numerous times by survey participants.

The Aviation ISAC extends its thanks to the member companies that participated in this year's survey and looks forward to leading efforts in 2021 that will address the identified priorities and challenges.

About the Aviation ISAC

Founded in 2014, we are a nonprofit membership association supporting the global air transport network.

We are the only global cyber-threat sharing organization that provides aviation-specific threat information to the airport community. With members headquartered on five continents, our reach spans the global aviation transport network.

We:

- Act as an extension of your IT team, focusing on airport- and aviation-specific threats, risks, and challenges. We connect your cyber risk management team to hundreds of aviation cybersecurity analysts around the globe.
- Provide clear and concise critical cyber threat information to the aviation community.
- Facilitate security communities for Aviation IT Managers, Chief Information Security Officers, Network Security Architects, Product Security Specialists, and Compliance Experts.
- Crowdsource membership expertise to deal with unique issues.

For more information, contact us: membership@a-isac.com; www.a-isac.com