2022 Cyber Risk Survey

Aviation ISAC

AVIATION ISAC

TLP: WHITE

Contents

All information contained in this document is TLP: WHITE.

Introduction

Executive Summary

For the fifth consecutive year, the Aviation ISAC conducted its annual Cyber Risk Survey of member company Chief Information Security Officers (CISOs) and Chief Product Security Executives (CPSOs), or their equivalents, to identify their most pressing cybersecurity risks and challenges. This year's survey was a single question: "What are the three to five initiatives you will work on in 2022 to reduce cyber risk at your company?"

As we have seen each year, the survey results were enlightening. As in previous years, responses form a picture of the threat landscape and business needs combined with technical, legal, and contractual challenges and reflect the thought leadership of our community. The results identify the cybersecurity areas in which the aviation industry must continue to innovate.

The Pandemic

It is impossible to conduct any sort of industry assessment without including the effects of the global pandemic. For aviation, 2021 began on an optimistic note, with the hope that Covid-19 would quickly wane with widespread vaccine availability, resulting in the swift return of air travel. Passenger loads began increasing, at one point climbing over 80 percent of pre-pandemic levels on many routes. Unfortunately, third and fourth waves and the spread of the omicron variant significantly hampered the return to air travel. Moving into 2022, the pandemic's impact on aviation continues to significantly impact aviation operations, including cyber. The way we work, our ability to staff cyber programs, and fund cyber risk

EXECUTIVE SUMMARY

continued

reduction initiatives have all been affected. The survey highlighted that ransomware and the expansion of regulatory scope are two major factors driving initiatives in 2022. Regulators have directed mandatory breach reporting and are mandating controls on systems. It is very likely we will see an increase in mandates in 2022 and beyond.

This year's survey had fewer responses than in previous years, with just under one-third of member companies participating. Last year, we began mapping the results to the NIST cybersecurity framework (CSF) and have done the same this year. By doing so, we can obtain a more accurate year-over-year comparison of cyber initiatives and more effectively identify trends and patterns. This year we are benefiting from that work.

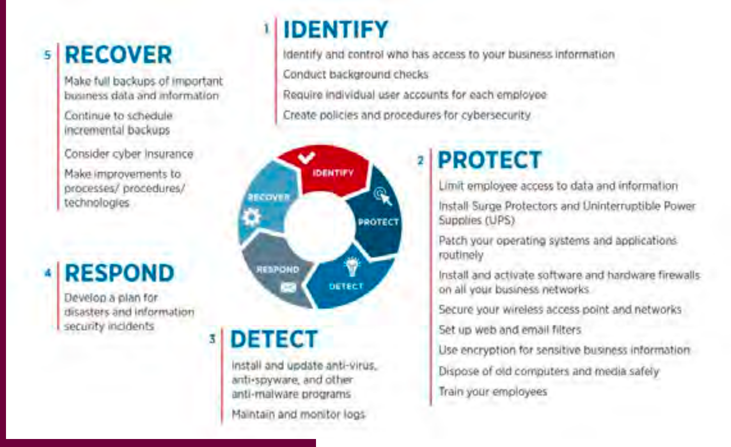
Survey results were grouped into three segments: airlines; airports; and original equipment manufacturers (OEMs)/service companies. The results include a consolidated view of the industry along with views reflecting the responses from each of the three segments.

For 2022, the top five cyber risk reduction initiative categories are: 1) Identity Management, (IDM), Authentication and Access Control; 2) Information Protection Processes and Procedures (IPPP); 3) Supply Chain Risk Management; 4) Data Security; and 5) Anomalies and Events. The report expands these priorities by subcategories and provides context about the most pressing of these initiatives. We also identify those initiatives we believe are likely to receive more focus by more industry members in the future.

As always, we offer our thanks to those member companies who took the time to participate in the survey. This data will guide the Aviation ISAC and industry stakeholders in best practices development and threat intelligence efforts. We are continually seeking feedback on our survey. Contact information is provided at the end of the report. Be safe and resilient!

What is the NIST CSF Framework?

The NIST 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.



1 IDENTIFY

Identify and control who has access to your business information

Conduct background checks

Require individual user accounts for each employee

Create policies and procedures for cybersecurity

2 PROTECT

Limit employee access to data and information

Install Surge Protectors and Uninterruptible Power Supplies (UPS)

Patch your operating systems and applications routinely

Install and activate software and hardware firewalls on all your business networks

Secure your wireless access point and networks

Set up web and email filters

Use encryption for sensitive business information

Dispose of old computers and media safely

Train your employees

3 DETECT

Install and update anti-virus, anti-spyware, and other anti-malware programs

Maintain and monitor logs

4 RESPOND

Develop a plan for disasters and information security incidents

5 RECOVER

Make full backups of important business data and information

Continue to schedule incremental backups

Consider cyber insurance

Make improvements to processes/ procedures/ technologies

Survey Results

DATA
ACCESS
SECURITY
CLOUD
APPS
TOOLS
TRAINING
INSURANCE
ACCOUNTS
NEW
SERVICES
PROCESS
TEAM
RANSOMWARE
MAINTENANCE
PROTECTION
LEGACY
FOCUSED
CHALLENGE
AIRCRAFT
CISO
SHARED
NETWORK
SERVICE
YEARS
PEOPLE
SANS
SIEM
CYBER
WORK
RISK
CAN
GROUP
GOOD
LOOKING
MOVING
SYSTEMS
STRATEGY
GOING
USED
BEST
OT
TTX
USE
NEED
TOOL
BUILD

Each year, we begin the presentation of the survey results by highlighting the top five focus areas of our respondents. This year we generated a word cloud from the survey results. As mapped, the word cloud and the survey results align to the NIST CSF quite well.

Access and access management, data security, apps and tools, cloud, insurance, and training are some the most frequently captured words in our CISO conversations.

People, team, training, and the phrase "work from home" (WFH), when grouped, reflect a strong focus on the cyber work force.

Continuing the process we began last year, the top five focus areas to reduce cyber risk in aviation are presented in the NIST CSF. As shown at left, the NIST CSF has five functional areas, with a range of categories detailing more specific work to address risk in the functional area. The most significant initiatives for 2022 (Table 1) target cyber risk in the ***protect*** and ***identify*** functions.

Table 1. Top Five

Protect	Identity management, Authentication, Access control
Protect	Information protection, processes, and procedures
Identify	Supply chain risk management
Protect	Data security
Protect	Anomalies and events

1. Identity Management, Authentication, and Access Control

Identity Management (IDM), Authentication and Access Control were highlighted as either the highest or second-highest priority for respondents, a result we have seen consistently in each previous year's survey. Challenges persist in IDM in several areas. Two years ago, few companies were talking about segmentation; even fewer were discussing micro-segmentation. This year, segmentation strategy has become a priority, with many segmentation projects in progress or preparing to launch. As part of their IDM challenges, many companies are still working on initiatives to better manage privileged, technical, and shared accounts. Some respondents called out IDM work as a core function that must receive significant attention and support every year.

In years past, IDM challenges focused mainly on the implementation of multifactor authentication (MFA). Some companies continue to have MFA challenges, however, we are seeing a trend of addressing IDM cyber risk through network segmentation and applications access management.

Inclusive of PR.AC-5, Table 2 provides the six subcategories of IDM were referred to as the members described their initiatives.

Table 2. IDM, Authentication, and Access Control, Subcategories

PR.AC-5	Network integrity is protected (e.g., network segregation and/or segmentation)	33%
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-1	Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes	20%
PR.AC-4	Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	14%
PR.AC-2	Physical access to assets is managed and protected	5%
PR.AC-3	Remote access is managed	5%

HIGHLIGHTS

PR.AC-5 *One third of respondents are working on network segmentation projects. This includes cloud projects, software-based segmentation, and an airline's creation of a separate network for its e-enabled planes.*

PR.AC-7 *The initiatives included instituting SSO, MFA, and increased Privileged Access Management.*

PR.AC-4 *Restricting access to applications.*

> IAM is now a [business-as-usual] activity.”
>
> — Airline

2. Information Protection, Processes, and Procedures

Information Protection Processes and Procedures (IPPP) is the second most-identified category of initiatives for 2022 (see Table 3). The subcategories for IPPP overlap with some other categories; for example, PR.IP-9 overlaps with the Recovery Function, and PR.IP-7 overlaps with many initiatives, including segmentation as a protection process. Nonetheless, several excellent initiatives were called out in this category.

Table 3. Information Protection Processes and Procedures, Subcategories

PR.IP-10	Response and recovery plans are tested	25%
PR.IP-9	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	25%
PR.IP-7	Protection processes are improved	21%
PR.IP-2	A system development life cycle to manage systems is implemented	12%
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)	4%
PR.IP-4	Remote access is managed	4%

HIGHLIGHTS

PR.IP-9 & 10 *Several member companies highlighted initiatives to enhance and test their recovery plans. This overlaps with the recovery function. This increased effort is attributed to the proliferation of ransomware attacks.*

PR.IP-7 *The move to the cloud continues for many members, as does the challenge for cyber security leaders to improve the security of the cloud environment.*

PR.IP-4 *OEM, service companies, and one airline with significant software development resources are improving their SDLC policies and procedures. One member is customizing an SDLC for each product.*

> We are working on ransomware incident response, including a fire drill.”
>
> —Services

3. Supply Chain Risk Management

Supply Chain Risk Management (SCRM) initiatives are the third most-frequently mentioned of cyber risk reduction efforts. This was exclusively called out by every original equipment manufacturer/service provider in the survey. Table 4 provides all the subcategories called out for SCRM.

Table 4. Supply Chain Risk Management, Subcategories

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	46%
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-1	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	15%
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.	15%

HIGHLIGHTS

PR.AC-5 *One third of respondents are working on network segmentation projects. This includes cloud projects, software-based segmentation, and an airline's creation of a separate network for its e-enabled planes.*

PR.AC-7 *The initiatives included instituting SSO, MFA, and increased Privileged Access Management.*

PR.AC-4 *Restricting access to applications.*

> IAM is now a [business-as-usual] activity."
>
> — Airline

4. Data Security

Data Security (Table 5) was the fourth most frequently identified category. Airlines and OEM/service providers were the two industry segments reporting data security initiatives. Table 5 shows the data security subcategories identified.

Table 5. Data Security, Subcategories

PR.DS-5	Protections against data leaks are implemented	40%
PR.DS-1	Data-at-rest is protected	30%
PR.DS-3	Assets are formally managed throughout removal, transfers, and disposition	20%
PR.DS-2	Data-in-transit is protected	10%

HIGHLIGHTS

Respondents identified initiatives to better protect data in the cloud. Companies are challenged with right-sizing security tool suites. Certain security tools security teams have used on legacy networks are not necessarily the best for the cloud environment. Companies are looking to hire or develop in-house staff who can assist in deployment, operations, and management of new data protection tools. As mentioned in the SCRM section above, DLP challenges persist within member companies as well.

5. Anomalies and Events

Anomalies and Events rounds out the top five categories identified for 2022. Respondents highlighted initiatives that addressed all five of the subcategories in Anomalies and Events. (see Table 6).

Table 6. Anomalies and Events, Subcategories

DE.AE-1	A baseline of network operations and expected data flows for users and systems	22%
DE.AE-2	Detected events are analyzed to understand attack targets and methods	22%
DE.AE-3	Event data are collected and correlated from multiple sources and sensors	22%
DE.AE-5	Incident alert thresholds are established	22%
DE.AE-4	Impact of events is determined	12%

HIGHLIGHTS

Three themes emerged in the Anomalies and Events discussion. There is significant effort on increasing resilience in the operating technologies (OT) environments by improving the ability to monitor OT environments and thus detect anomalous behaviors. Some aviation OT technologies are using older technologies not designed for continuous monitoring (CM). Second, many companies are challenged with CM in their cloud environments. Third, the process of continuous improvement in cyber security includes companies moving to new SOARs, SIEMs, and the like, and the automation of the alerting and disposition processes.

Each year, certain initiatives emerge that are essential to a strong cyber security program but either do not map well to the NIST CSF, or if integrated would not identify the specific nature of the initiative.

Staffing

Several respondents discussed initiatives to improve cyber talent staffing and retention. These efforts include recruiting from other IT functions within the company, broader recruiting efforts with an increased focus on diversity, and training employees to build cyber security skillsets that better align with the newer computing environments (most notably cloud and OT).

Increased Collaboration on OT and Aircraft Cybersecurity Assurance

This was mentioned by both OEMs and airlines.

Increased Engagement with the Cybersecurity Researcher Community

This engagement has been fruitful in building both culture and communications that foster collaborative vulnerability disclosures. It also creates a potential pipeline for new talent.

Financial Challenges

Some respondents expressed ongoing budget challenges due to pandemic-related revenue loss.

Honorable Mentions

Looking past the Top 5, *Governance* and *Awareness and Training* were the two most-mentioned CSF categories.

Governance

Three of the four Governance categories were mapped to respondents' initiatives. All three industry segments had initiatives addressing Governance (see Table 7).

Table 7. Governance, Subcategories

ID.GV-3	Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managedis established and managed	55%
ID.GV-4	Governance and risk management processes address cybersecurity risks	33%
ID.GV-1	Organizational cybersecurity policy is established and communicated	12%

HIGHLIGHTS

The elevation of Governance as a priority focus area in 2022 is a significant shift from prior years, though not a surprise. We have seen the International Civil Aviation Organization (ICAO), the European Aviation Safety Agency (EASA), the United States Transportation Security Administration (TSA), and many other CAA's undertaking efforts to develop and issue mandatory cyber security breach reporting and cyber security controls. The number of regulatory bodies issuing aviation cybersecurity requirements was highlighted as a concern. Respondents noted that it is incumbent upon the industry to work toward the global harmonization of these new requirements.

The external influence on governance is one of the two aspects of governance mentioned by respondents. Members also mentioned initiatives to improve internal application of cybersecurity policy across the business units of companies. Instituting or improving the software development life cycle (SDLC) was a frequently-mentioned governance initiative.

Awareness and Training

The ranking of Awareness and Training underscores the importance of creating a company-wide cybersecurity mindset. Phish continue to get past email scanning tools, configuration errors continue to occur, and application owners must embrace their cybersecurity functions. Several companies mentioned plans to execute more tabletop exercises as a part of training, awareness, and identification of areas for improvement.

Top 5 Year-Over-Year

Table 8 provides a two-year comparison of the most frequently identified functions. We list the most frequently named category(ies) within those functions. "Protect" was again the most frequently referenced, along with IDM, Authentication, and Access Control as the areas within that function receiving the most attention. In 2022, Information Protection Processes and Procedures was the second-most focused area for improvement. This was primarily driven by work on recovery processes and was a significant jump over recovery work in 2021. In 2022, SCRM, which was not in top 5 in 2021, was the third ranked priority area. Emphasis in these areas reflects work to specifically address ransomware. An increase in CISOs' focus on the security of data in 2022, reflects an increase in emphasis on layered security as well as challenges in securing data in the cloud. Finally, the top 5 in 2021 and 2022 included work on security monitoring. In both years, this included increasing visibility into OT networks and the cloud. For 2022, we have heard that more work is being done on creating behavior and baseline patterns in these networks.

Table 8. Year-Over-Year by Function, Category

FUNCTION	2022	FUNCTION	2021
PROTECT	ID Mgmt., Authentication, Access Control	PROTECT	ID Mgmt., Authentication, Access Control
PROTECT	Info. Protection, Processes, Procedures	IDENTIFY	Asset Management
IDENTIFY	Supply Chain Risk Management	DETECT	Security Continuous Monitoring
PROTECT	Data Security	RESPOND	Mitigation
PROTECT	Anomalies and Events	RECOVER	Recovery Planning

Although Protect and Identify remained numbers 1 and 2, respectively, as the functions with the most initiatives, Figures 1 and 2 highlights the signficant shift of resources across the industry to focus on IDM issues in 2022. In 2021, Asset Management initiatives were as prominent as the IDM initiatives.

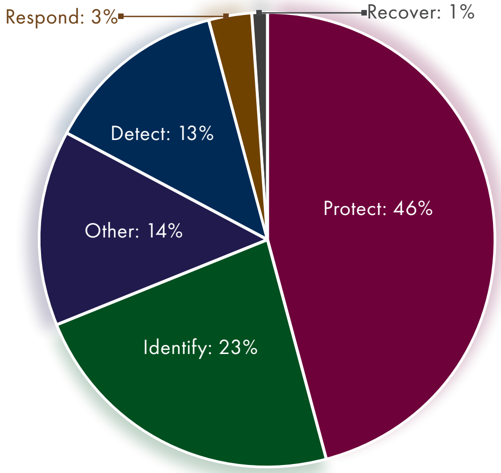


Figure 1. 2022, All Segments

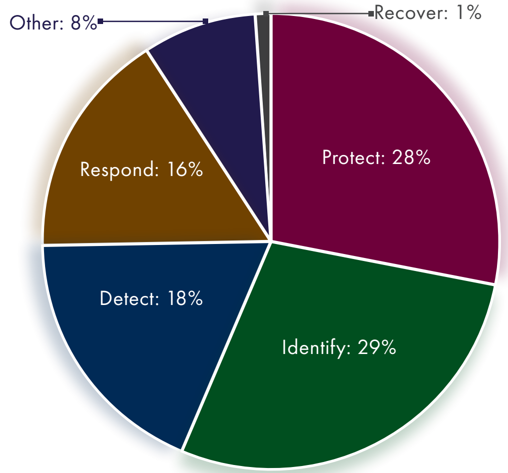


Figure 2. 2021, All Segments

What Will Trend?

As noted earlier, network segmentations were just beginning to be mentioned in our survey two years ago. This year, respondents discussed numerous segmentation and micro-segmentation initiatives. What will trend in the years ahead? One member company explained they were seeking out coders and data analysts to supplement their cybersecurity team. These skillsets are needed as the move to the cloud requires more custom cyber security coding to build get the data necessary for continuous monitoring. Similarly, looking within that data for patterns of anomalous behavior also necessitates the big data analytics skills.

Data by Industry Segment

For the first time in the Annual Aviation Cyber Risk Survey, we are transitioning the industry segment view into the NIST CSF.

Airports

Going into 2022, asset and vulnerability management processes appear to more stabilized. Awareness and training initiatives have been prioritized, along with Security Operations Center (SOC) initiatives to increase visibility of assets being continuously monitored and detecting anomalous events in the data collected for continuous monitoring. Figures 3–5 show the year-over-year shift, 2020-2022 in airport cyber security initiatives.

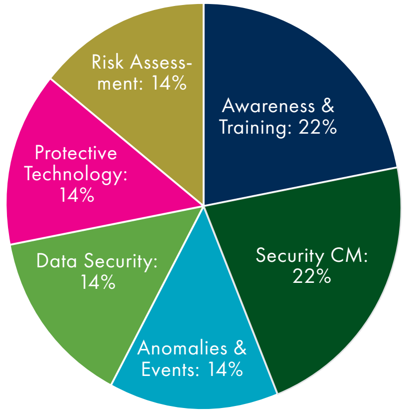


Figure 3: Airports, 2022

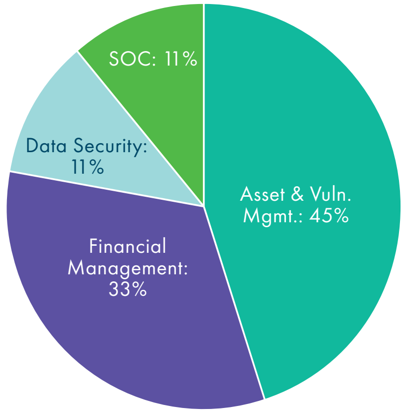


Figure 4: Airports, 2021

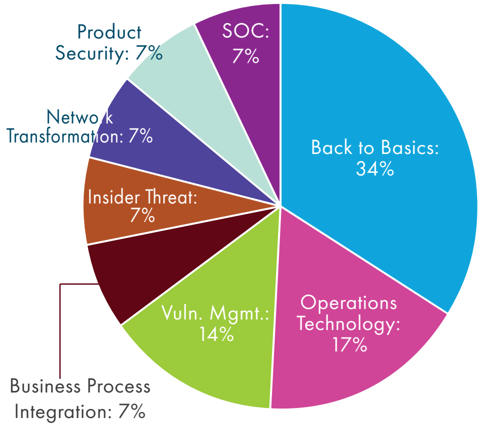


Figure 5: Airports, 2020

OEM/Services

Trends over the past three years in changing cyber security initiatives for the Original Equipment and Services segment are reflected in Figures 6–8. The charts reflect only the categories of the most frequently mentioned initiatives. Only two Chief Product Security Officers participated in this year's survey; as such, the results of those interviews are integrated into the other results. Information protection and SCRM are growing areas of focus. Both IDM and IAM have consistently been areas for improvement initiatives. The addition of governance reflects the increased coordination between the cyber security function and other business functions.

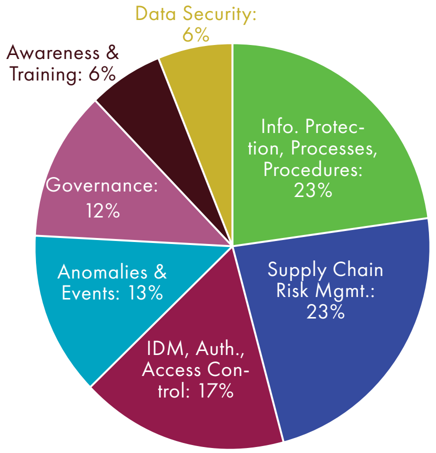


Figure 6: OEMs/Services, 2022

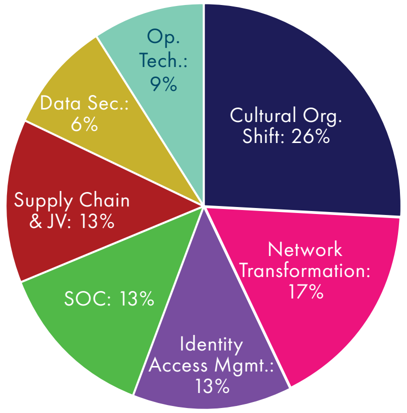


Figure 7: OEMs/Services, 2021

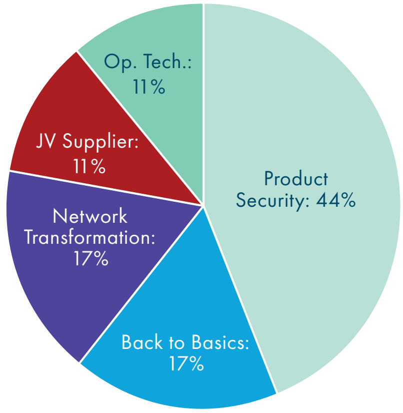


Figure 8: OEMs/Services, 2020

Due to a low sample size, the results from Chief Product Security Officers were integrated into the overall survey results.

Airlines

The IDM and IAM categories continue to be areas of emphasis for airlines. As noted in the airport segment year-over-year comparison, of vulnerability management appears to be functioning well as a foundational element of the airline cyber security programs. Information protection (including recovery efforts) and data security are two categories receiving significantly more resources to reduce cyber risk in the airline segment. Figures 9–10 shows the year-over-year comparison of cyber risk reduction initiatives in the Airline segment for 2021 and 2022. (Prior to and including 2020, the data did not map well to the shift to the NIST CSF format.)

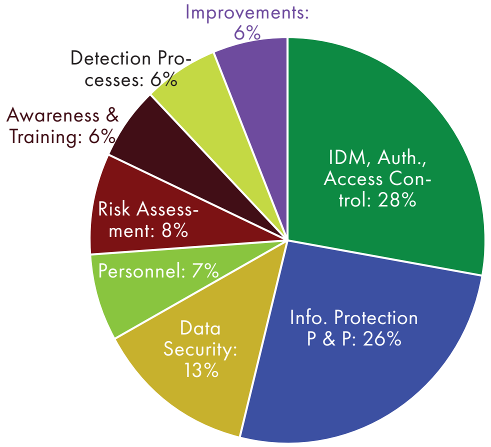


Figure 9: Airlines, 2022

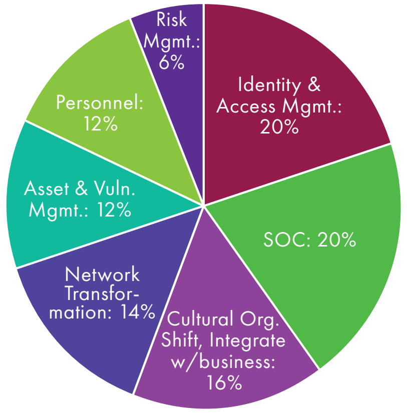


Figure 10: Airlines, 2021

Summary

The survey results revealed deliberate and consistent year-to-year focus on challenging areas, such as identity and access management. An increasing number of companies are employing segregation and segmentation to reduce the impact of a breach. The survey also revealed some important shifts 2022 toward recovery of business functions, data protection, and supply chain risk management.

The Aviation ISAC extends its thanks to the member companies that participated in our fifth Annual Aviation Cyber Security Risk Survey. We hope this survey is a valuable benchmarking tool for your company. Within the Aviation ISAC community, this data is used to guide our development of best practices, set threat intelligence requirements, and develop targeted cyber skills among our member companies.

We welcome your feedback. Please send any comments to: membership@a-isac.com. We look forward to another successful year of collaboration with our members and global partners as we work as a community to make aviation safer and more resilient.

AVIATION **ISAC**

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