SITA

2018

AIR TRANSPORT CYBERSECURITY INSIGHTS

AIR TRANSPORT CYBERSECURITY INSIGHTS

The 2018 Air Transport Cybersecurity Insights report is a worldwide study commissioned by SITA. It is the most comprehensive study investigating cybersecurity trends within the air transport industry.

The report discusses results from a survey conducted during May to July 2018, which drew responses from 59 senior decision makers at major airlines and airports globally, including CEOs, CIOs, CISOs, VPs and Directors of IT and security practices.

This aviation-specific research aims to determine the state of cybersecurity in the air transport industry. It explores trends and priorities for investments, current challenges faced by the industry, common initiatives and technology trends, as well as industry-specific risks and best practice.

The 2018 results provide clear insights into the air transport industry's strategic thinking and plans for cybersecurity in the years ahead.

CONTENT GUIDE

CYBER SPEND
& CHALLENGES

INVESTMENT
PRIORITIES

AREA OF FOCUS
& KEY THREATS

SECURITY OPERATIONS
CENTER (SOC)

HIGH AWARENESS OF THE IMPORTANCE OF CYBERSECURITY BUT EXISTING CHALLENGES ARE DELAYING PROGRESS

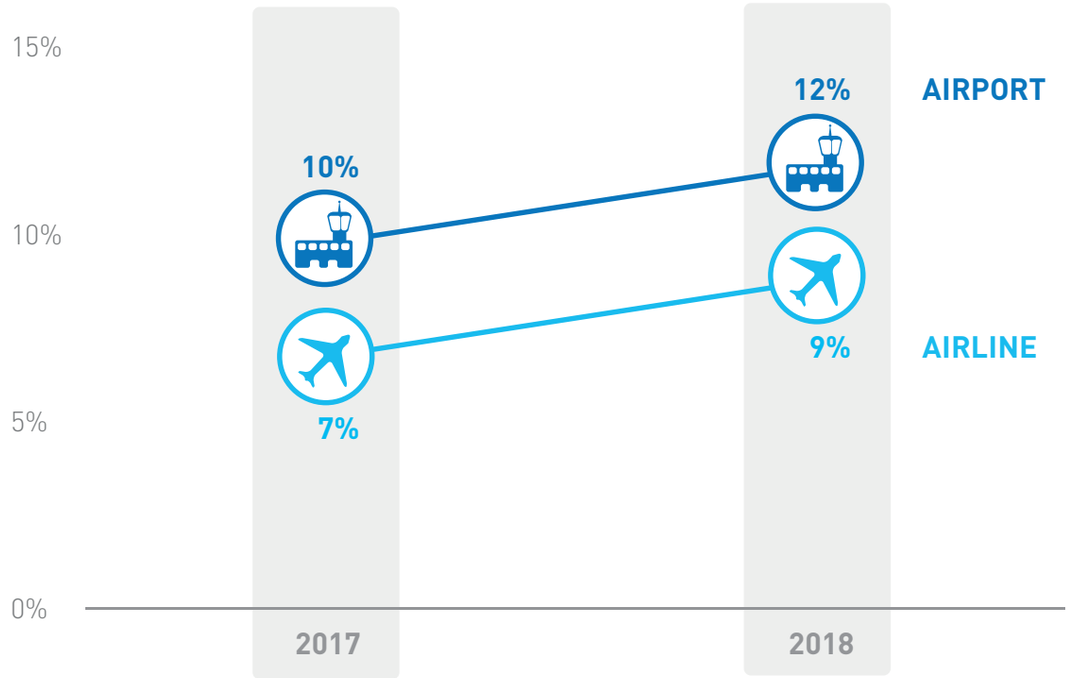
- Cybersecurity budgets are expected to grow and spending is shifting towards detection and prevention.
- Rising risk is well acknowledged, but Cybersecurity teams are still lacking empowerment and positioning at C-level.
- A lack of resources, budget and skills are the key barriers for advancing Cybersecurity protection.

SITA RECOMMENDATIONS

Air transport industry stakeholders must empower their Cybersecurity teams and provide necessary resources to initiate concrete and actionable projects.

CYBERSECURITY BUDGETS ARE GROWING AND SPENDING IS SHIFTING TOWARDS DETECTION AND PREVENTION

% of IT budget spent on Cybersecurity



ANALYSIS

Spend on Cybersecurity is increasing in the air transport industry and is set to be higher in 2018 compared to 2017.

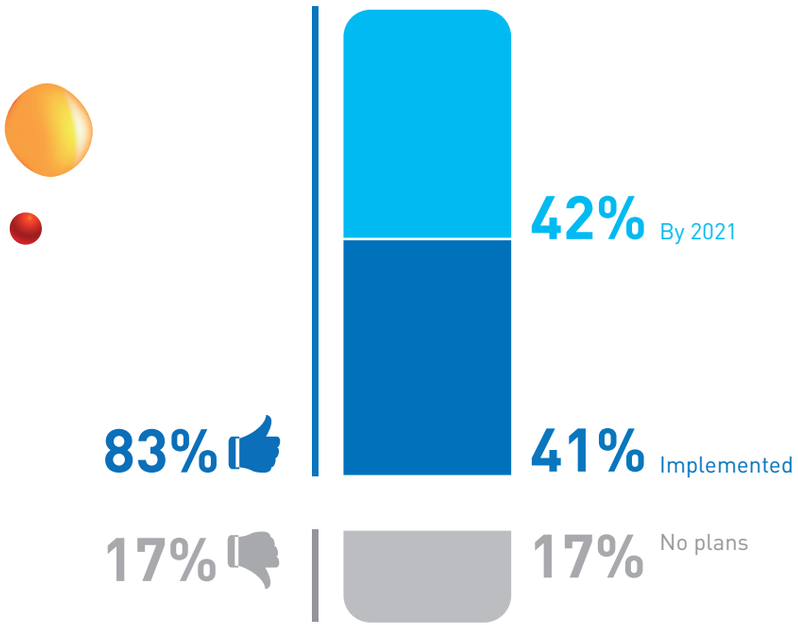
The level of spend on Cybersecurity in the air transport industry and is set to other industries. Airlines spend an average of 7% of their overall IT budget on Cybersecurity, compared to a higher airport investment at 10%.

Cybersecurity is not yet getting the investment it deserves, with spend expected to increase to 9% and 12% respectively in 2018. This reflects the rising importance of protecting data and systems from unauthorized access.

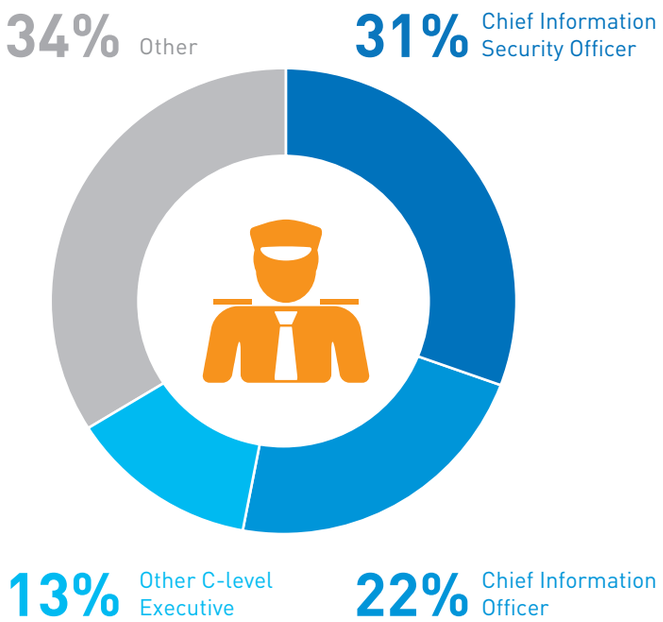
73% of respondents ranked regulatory compliance and data privacy regulation as being among the highest priorities. This has been considered an important driver for security investments during the past three years. Security spending is expected to shift towards detection and response in the coming years.

RISING RISK IS WELL ACKNOWLEDGED, BUT CYBERSECURITY TEAMS ARE STILL LACKING EMPOWERMENT AND POSITIONING AT C-LEVEL

% of organizations listing Cybersecurity in their global risk register to improve risk management



Position responsible for Information Security in the organization



ANALYSIS

Rising stakes in Cybersecurity are acknowledged among security leaders. Introducing a dedicated Chief Information Security Officer (CISO) is crucial to visibility and effective implementation.

For two thirds of the responding aviation organizations (66%), the overall responsibility for Information Security is assigned to a C-suite executive, reflecting the increasing importance of Cybersecurity to the industry.

Today 41% of respondents include Cybersecurity as part of a global risk register, while a further 42% of respondents planning to include cyber risk in their registers by 2021. This gives a further indication of the rising stakes in Cybersecurity across the air transport industry.

Yet only 31% of the responding organizations have a dedicated CISO. A dedicated CISO can be of pivotal importance for the empowerment and positioning of security teams at C-level.

A LACK OF RESOURCES, BUDGET AND SKILLS ARE THE KEY BARRIERS FOR ADVANCING CYBERSECURITY PROTECTION

Challenges when implementing Cybersecurity in the organization

78%
Limited resources

70%
Limited budget

56%
Staff training

51%
Visibility of network and IT assets

49%
Data protection

47%
Staff recruitment and retention

46%
Cloud usage (sanctioned/unsanctioned)

38%
Securing operational technologies (ICS, SCADA)

34%
Sponsorship at senior management level

28%
Securing outstations

ANALYSIS

When tackling Cybersecurity, the air transport industry faces similar challenges to other industries: a lack of resources, budget and skills.

The industry has moved beyond awareness, and has put in place the foundations necessary to protect against cyber threats. Yet, executives are also aware that bigger strides need to be made to advance to a proactive Cybersecurity maturity level.

Aviation companies face significant headwind when trying to improve their Cybersecurity protection. The biggest barrier is a lack of resources affecting 78% of organizations. This is compounded by the lack of sufficient Cybersecurity budgets - a problem for 70% of organizations. A significant challenge some executives face is the retention and recruitment of specialized skilled staff (47%) and the capacity for staff training (56%). The industry needs to complement internal resources with external expertise.

A MAJORITY OF AIRLINES AND AIRPORTS HAVE PUT CORE SAFEGUARDS IN PLACE AND ARE READY TO ADVANCE TO THE NEXT LEVEL

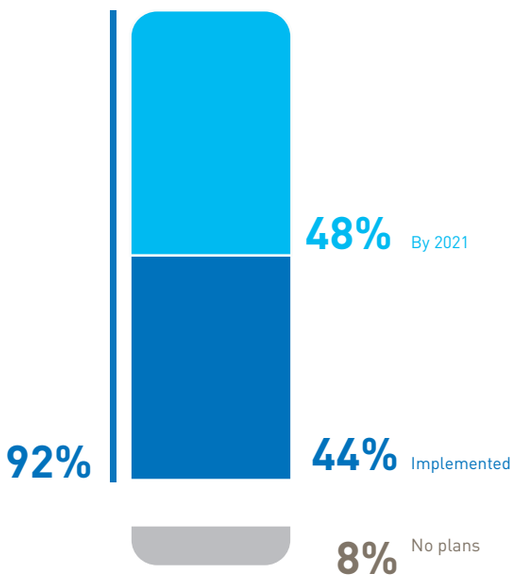
- Security foundations are being put in place with an objective of continuous improvement.
- Employee awareness is considered the most important component in the defence against cyber risk.
- Building a good foundation is top priority in all areas of Cybersecurity.

SITA RECOMMENDATIONS

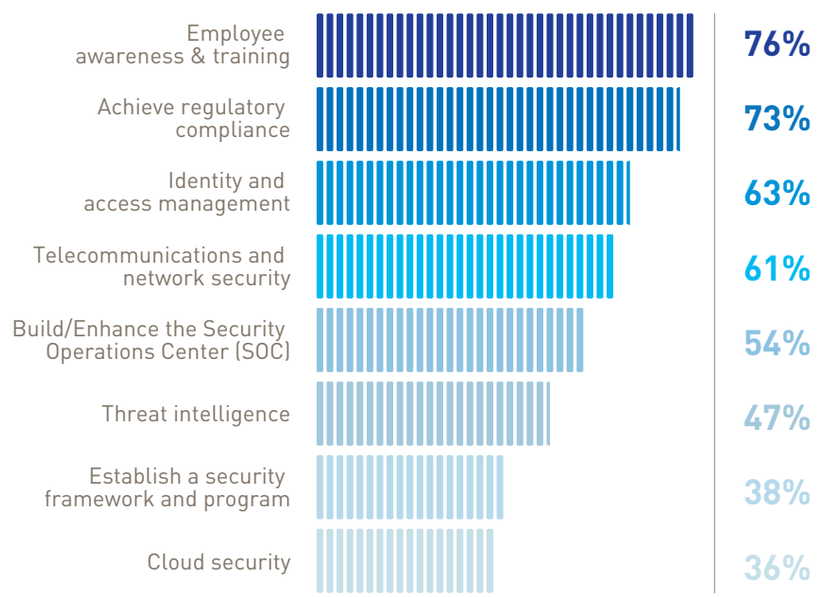
To advance an organization's Cybersecurity maturity, it is critical to have a clear long-term Cybersecurity strategy aligned with the organization's business objectives and IT environment.

SECURITY FOUNDATIONS ARE BEING PUT IN PLACE WITH AN OBJECTIVE OF CONTINUOUS IMPROVEMENT

% of organizations with a formal Information Security Strategy



Priorities investing in Cybersecurity initiatives



ANALYSIS

Industry leaders are starting to introduce core building blocks needed in the defence against cyber attacks.

Today, almost half (44%) of respondents have a formal Information Security Strategy in place. By 2021, almost all of the surveyed organizations will have a formal cyber strategy.

The most common spending priorities today are: 'employee awareness and training' (76%), 'achieving regulatory compliance' (73%) and 'identity & access management' (63%).

Regulatory compliance and data privacy regulations have stimulated spending on security during the past three years. A recent example is GDPR coming into effect in Europe during 2018. These regulations translated into increased spending, particularly in data security tools such as identity & access management technology.

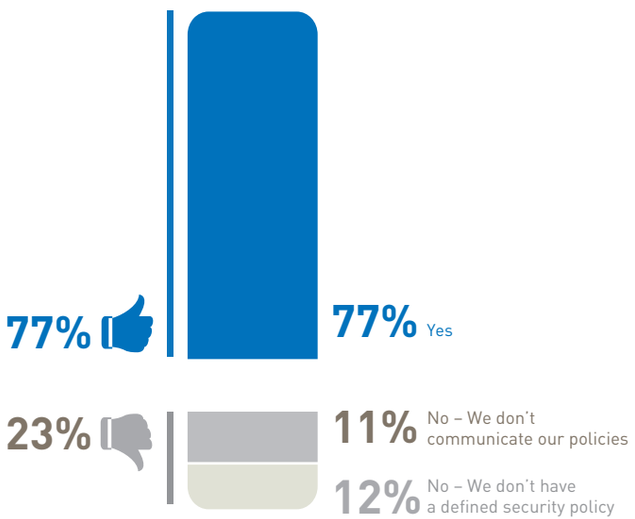
EMPLOYEE AWARENESS IS CONSIDERED THE MOST IMPORTANT COMPONENT IN THE DEFENCE AGAINST CYBER RISK

No. 1 investment priority

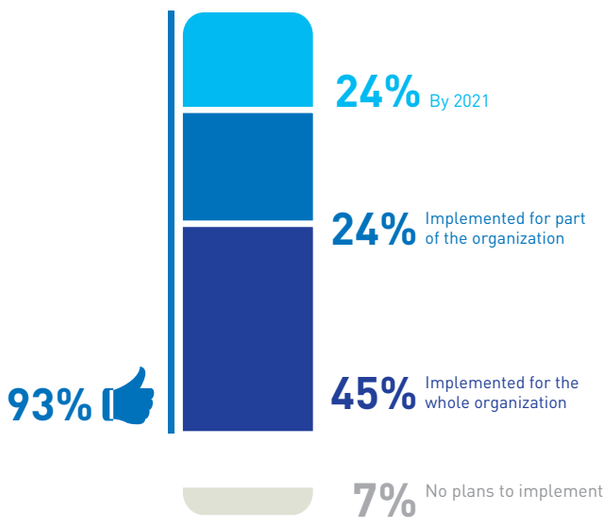
Employee awareness & training

76%

% of respondents who communicate their Security Policies to employees



% of respondents with a formal Cybersecurity training program for employees



ANALYSIS

Employees are the weakest link in the fight against cyber attacks, and the very first topic to address. Air transport industry security experts accept that employees need to be part of their core security arsenal in the defence against risk.

SITA's Air Transport Cybersecurity Insights survey shows that 'Employee awareness & training' is the number one priority for Cyber-security (76%).

With Ransomware and Phishing at the top of the risk agenda, it is good to see such a high proportion of organizations placing employees at the top of Cybersecurity best practice. Over three quarters (77%) of aviation organizations communicate their security policies to their employees, while 69% have a formal training program in place.

BUILDING A GOOD FOUNDATION IS TOP PRIORITY IN ALL AREAS OF CYBERSECURITY

ASSESS

% maintaining inventory of critical business processes

100%

60%

40%

% maintaining Inventory of critical infrastructure/applications

27% By 2021

73% Implemented

DETECT

% who have a Security Operations Center (SOC)

79%

46% By 2021

33% Implemented

21% No plans

RESPOND

% with a defined Cybersecurity incident process

91%

30% By 2021

61% Implemented

9% No plans

ANALYSIS

Securing your organization means being able to assess, detect and appropriately respond to risk and breaches.

It is encouraging that the vast majority of the responding organizations are conducting a formal risk assessment today (93%). 33% have a Security Operations Center to monitor their IT environment, with another 46% planning to do so by 2021. Almost two thirds have a defined incident process should a breach occur.

Yet, while 73% maintain an inventory of critical infrastructure today, only 40% do the same for critical business processes. This indicates that today the link between business processes and IT systems is missing for many organizations. Linking business process and IT systems enables organizations to manage Cybersecurity based on their potential financial or operational impact.

A LEADING CYBERSECURITY DRIVER IS SHIFTING FROM COMPLIANCE TO PROACTIVE PROTECTION WITH A FOCUS ON DETECTING EXTERNAL THREATS AND PREVENTING DISRUPTION

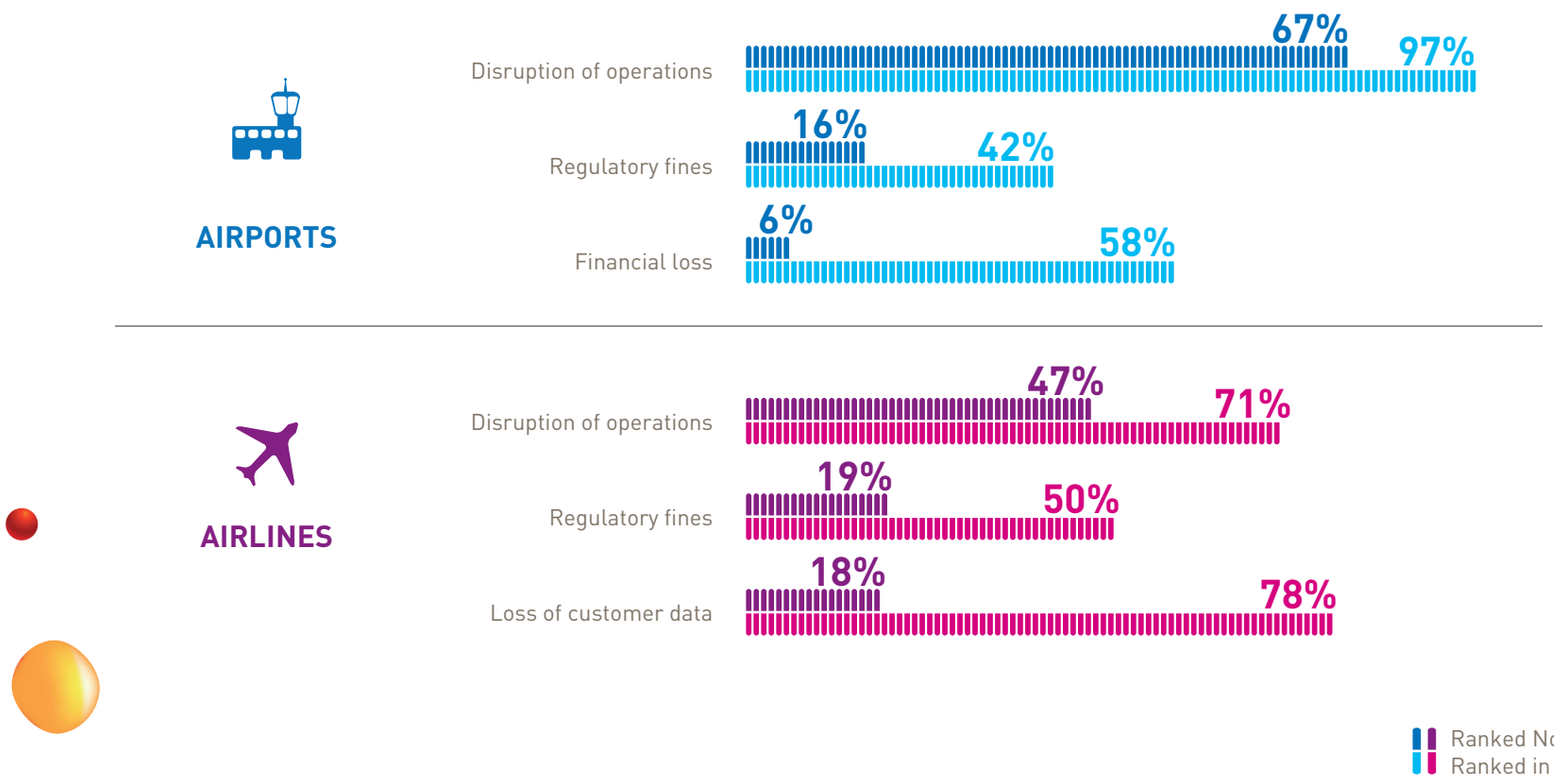
- A top priority for air transport industry - stakeholders: avoid operational disruptions, data loss and prevent regulatory fines.
- The air transport industry is targeted by the complete scope of cyber threats. External threats remain the main priority overall.
- Protection of the core network takes center stage today with securing the extended enterprise as the next step.

SITA RECOMMENDATIONS

The key prerequisite for advancing Cybersecurity maturity is a clear understanding of the most business critical factors and their associated threat levels.

A TOP PRIORITY FOR AIR TRANSPORT INDUSTRY - STAKEHOLDERS: AVOID OPERATIONAL DISRUPTIONS, DATA LOSS & REGULATORY FINES

Respondents ranking cyber security risks in terms of their priority to prevent



ANALYSIS

Ensuring business continuity by protecting airport and airline operational processes takes priority in the air transport industry.

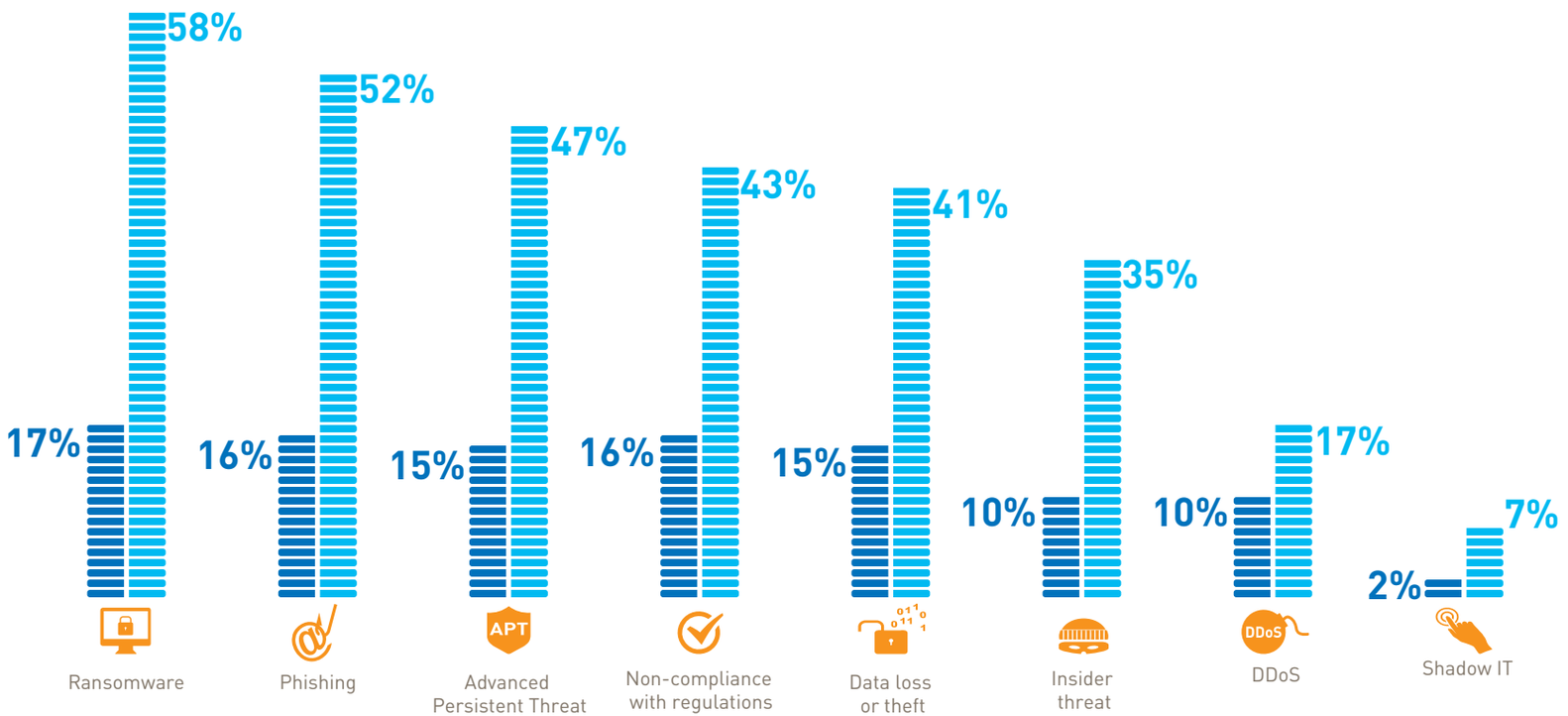
Industry executives at airlines and airports consider protecting operational systems and processes from cyber attacks to ensure business continuity as their biggest priority overall (Top 1: 57% of all respondents).

For airports, disruption is the clear number one concern. Airlines still rank disruption of operations highly (71%) but airline executives also give the protection of their passengers data (78%) and financial loss a similar priority level.

The risk of 'regulatory fines' is considered a priority for 50% and 42% of airlines and airports respectively. This is likely to increase as the regulatory eco-system globally matures.

THE AIR TRANSPORT INDUSTRY IS TARGETED BY THE COMPLETE SCOPE OF CYBERTHREATS. EXTERNAL THREATS REMAIN THE MAIN PRIORITY OVERALL

Security risks considered highest priority to address



ANALYSIS

There is a consensus that all cyber threats are equally pertinent in the air transport industry.

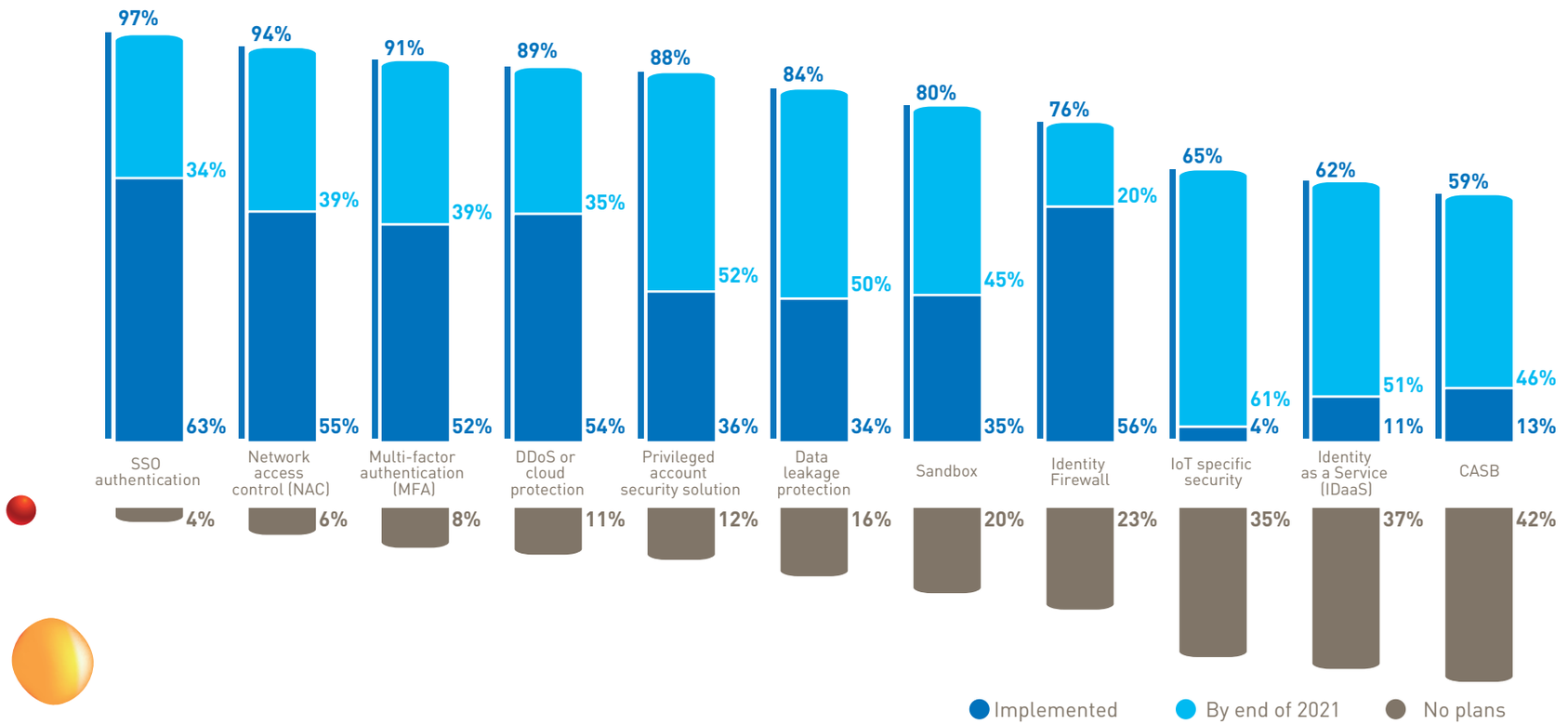
Consistent with other industries, ransomware (58%), phishing (52%) and advanced persistent threats (47%) are regular and frequent risks seen in the air transport industry.

Today, more attention is paid towards threats coming from external actors, with only 10% considering insider threats as a top priority today. This area will receive more attention in the future, as analysts report over a quarter of attacks involving insiders.

SITA expects that 'Shadow IT' - ranked lower in priority (7%) today - will need to be watched closer in the future. Shadow IT, in particular the adoption of 3rd party cloud solutions by employees, is a trend observed in other industries. It can bring productivity gains but also introduces additional vulnerabilities that need to be carefully managed.

PROTECTION OF THE CORE NETWORK TAKES CENTER STAGE TODAY WITH SECURING THE EXTENDED ENTERPRISE AS THE NEXT STEP

% of respondents with IT security technologies implemented or planning to implement



ANALYSIS

The most common technologies implemented by 2021 will be protecting the edges of the core network, while Internet of Things (IoT) Security, data leakage protection and Cloud access broker (CASB) will follow as the next technology deployment wave.

SSO Authentication (63%), Network access control (55%), and multi-factor authentication (52%) have been implemented by the majority of respondents, with most aviation companies set to have implemented all of these protection technologies by the end of 2021.

Deployment of technologies such as CASB, IoT Security and Identity-as-a-Service is limited today. These technologies will see a strong increase in deployment in the next three years as digital transformation progresses and security teams move towards securing the extended enterprise.

ONE IN TWO ORGANIZATIONS WILL IMPLEMENT A 'SECURITY OPERATIONS CENTER' IN THE NEXT THREE YEARS TO RAMP UP PROTECTION

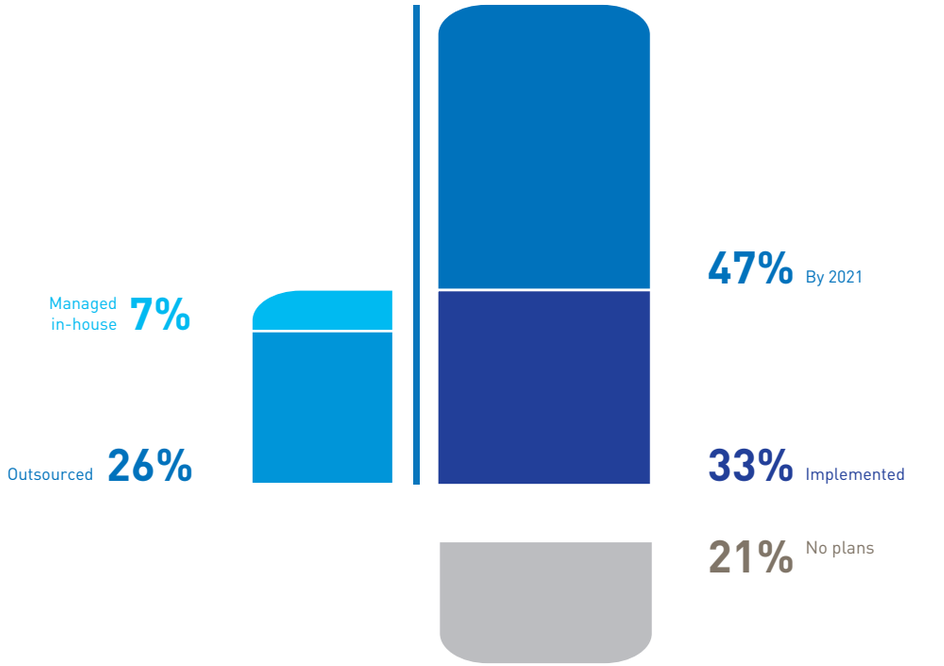
- The air transport industry's immediate objective: implementation of a 'Security Operations Center (SOC)'.
- SOC implementations put emphasis on the infrastructure layer before extending to the application layer.

SITA RECOMMENDATIONS

Security Operations Center Services are necessary but complex projects. To guarantee faster ROI, staged implementation is essential, beginning with what is business critical before extending into less critical areas.

THE AIR TRANSPORT INDUSTRY'S IMMEDIATE OBJECTIVE: IMPLEMENTATION OF A 'SECURITY OPERATIONS CENTER (SOC)'

% who have a Security Operations Center (SOC) implemented or plan to implement



ANALYSIS

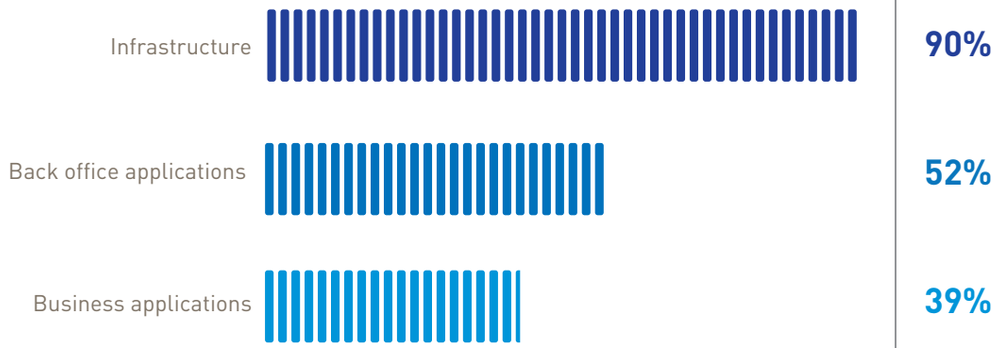
Proactive monitoring through a Security Operations Center (SOC) is a core topic for proactive Cybersecurity. It is encouraging to see that the majority of respondents have plans to quickly implement such services to enable fast detection of intrusions.

A SOC is often the first component security executives look at when building up their cyber defence capabilities. Only 33% of responding organizations have a SOC implemented today, but a further 47% of respondents plan for such investment by 2021.

The results also highlight a strong trend towards security outsourcing, with 8 out of 10 Security Operations Centers today run by external providers. Outsourcing SOC services addresses many of the key challenges, in particular, the lack of internal resources & skills which are cited as top challenges implementing Cybersecurity strategy.

SOC IMPLEMENTATIONS PUT EMPHASIS ON THE INFRASTRUCTURE LAYER BEFORE EXTENDING TO THE APPLICATION LAYER

Currently monitored through the Security Operations Center (SOC)



ANALYSIS

Most air transport industry organizations are monitoring their infrastructure through their Security Operations Center today, but have not yet advanced to the application layer due to the effort required.

9 out of 10 respondents monitor their network and infrastructure through a SOC, while only 52% monitor back office applications and 39% business applications.

Protecting the infrastructure is quicker to achieve as existing knowledge and best practice already exists. Assessing and monitoring critical applications, in particular bespoke business applications, is more complex than monitoring the infrastructure layer.

Monitoring business applications through a SOC requires a deep understanding of how the application behaves and what interactions need to be monitored to detect intrusions. It often needs a high level of effort involving those with in-depth knowledge of the application.

SURVEY FINDINGS SUMMARY

HIGH AWARENESS OF THE IMPORTANCE OF CYBERSECURITY BUT EXISTING CHALLENGES ARE DELAYING PROGRESS

The growing risk is well acknowledged, but still more must be done to raise the importance of Cybersecurity at board level or at senior management level. Spend on cybersecurity is increasing year on year and remains in line with other industries. Yet a lack of resources, tight budgets and missing skills remain the key barriers for advancing Cybersecurity protection in the air transport industry.

A MAJORITY OF AIRLINES AND AIRPORTS HAVE PUT CORE SAFEGUARDS IN PLACE AND ARE READY TO ADVANCE TO THE NEXT LEVEL

The most common spending priorities today are 'employee awareness and training', achieving 'regulatory compliance' and 'identity & access management'. Further security foundations are being put in place with an objective of continuous improvement. Creating a stronger link between business process and IT systems is key to move towards impact-based protection.

THE LEADING DRIVER FOR CYBERSECURITY INVESTMENT IS SHIFTING FROM COMPLIANCE TO PROACTIVE PROTECTION WITH FOCUS ON DETECTION OF EXTERNAL THREATS AND PREVENTION OF DISRUPTION

Top priority for air transport industry stakeholders is to avoid operational disruptions by protecting the core network from external threats. Technologies such as CASB, IoT Security and Identity-as-a-Service will see a strong increase in deployment in the next three years as the air transport industry's digital transformation progresses and protecting the extended network takes center stage.

ONE IN TWO ORGANIZATIONS WILL IMPLEMENT A 'SECURITY OPERATIONS CENTER' IN THE NEXT THREE YEARS TO RAMP UP PROTECTION

The air transport industry's immediate priority is the implementation of a 'Security Operations Center (SOC)'. A SOC is often the first component security executives look at when building up their cyber defence capabilities. Today, only 33% of responding organizations have a SOC implemented, but a further 47 % plan such investment by 2021. Most of today's implementations put emphasis on the infrastructure layer before extending to the application layer.

METHODOLOGY

SURVEY

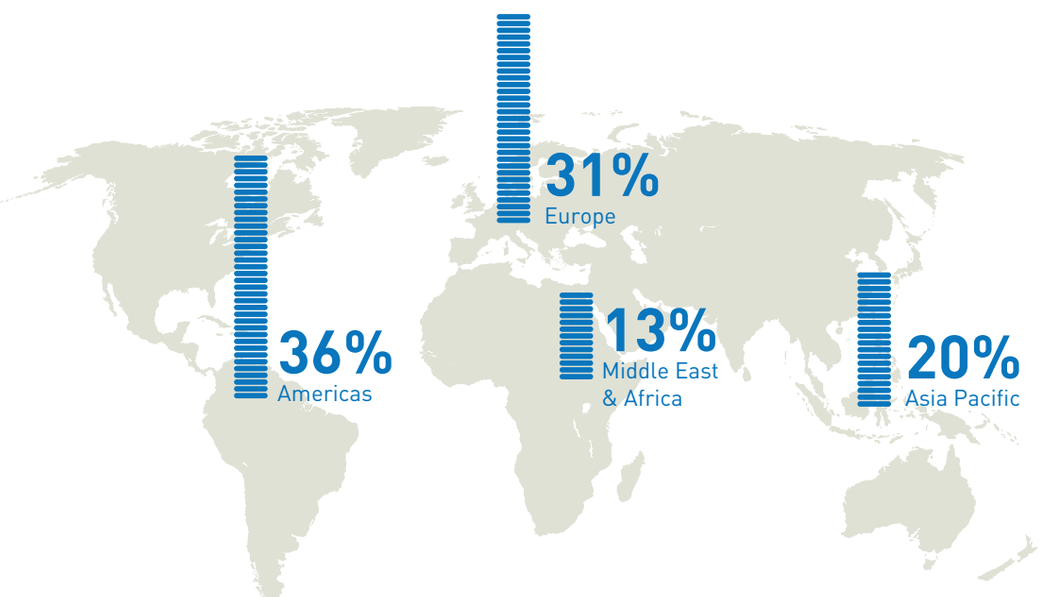
The SITA Cybersecurity Insights 2018 is a worldwide study commissioned by SITA. It is the most comprehensive study investigating Cybersecurity trends within the air transport industry and was conducted during May to July 2018. The results discussed in this report are based on responses of 59 senior decision makers at major airlines and airports globally, including CEOs, CIOs, CISOs, VPs and Directors of IT and security practices.

RESEARCH

Independent market research agency Circle Research was commissioned to undertake the study on behalf of SITA. The research was conducted in strict confidentiality and the results are presented in an aggregated form only. All source data remains confidential and the results of individual returns are not disclosed to the research stakeholders.

WEIGHTING

A weighting system is applied, based on the respondents' annual passenger traffic statistics, to ensure that the results are a representative sample in relation to global passenger traffic, and to compensate for annual fluctuations in the respondent group.



FOR A DEEPER DIVE INTO SITA CYBERSECURITY GO TO SITA.AERO/CYBERSECURITY

SITA AT A GLANCE

Easy air travel every step of the way.
Transforming air travel through technology for Airlines, at Airports, on Aircraft and at Borders.

- SITA's vision is: 'Easy air travel every step of the way'.
- Through information and communications technology, we help to make the end-to-end journey easier for passengers – from pre-travel, check-in and baggage processing, to boarding, border control and inflight connectivity.
- We work with about 400 air transport industry members and 2,800 customers in over 200 countries and territories. Almost every airline and airport in the world does business with SITA.
- Our customers include airlines, airports, GDSs and governments.
- Created and owned 100% by air transport, SITA is the community's dedicated partner for IT and communications, uniquely able to respond to community needs and issues.
- We innovate and develop collaboratively with our air transport customers, industry bodies and partners. Our portfolio and strategic direction are driven by the community, through the SITA Board and Council, comprising air transport industry members the world over.
- We provide services over the world's most extensive communications network. It's the vital asset that keeps the global air transport industry connected.
- With a customer service team of over 2,000 people around the world, we invest significantly in achieving best-in-class customer service, providing 24/7 integrated local and global support for our services.
- Our annual Air Transport and Passenger IT Trends Surveys for airlines, airports and passengers are industry-renowned, as is our Baggage Report.
- In 2017, we had consolidated revenues of US$ 1.6 billion.

For further information, please visit **www.sita.aero**

For further information, please contact SITA by telephone or e-mail:

Americas
+1 770 850 4500
info.amer@sita.aero

Asia Pacific
+65 6545 3711
info.apac@sita.aero

Europe
+41 22 747 6000
info.euro@sita.aero

Middle East, India & Africa
+961 1 637300
info.meia@sita.aero