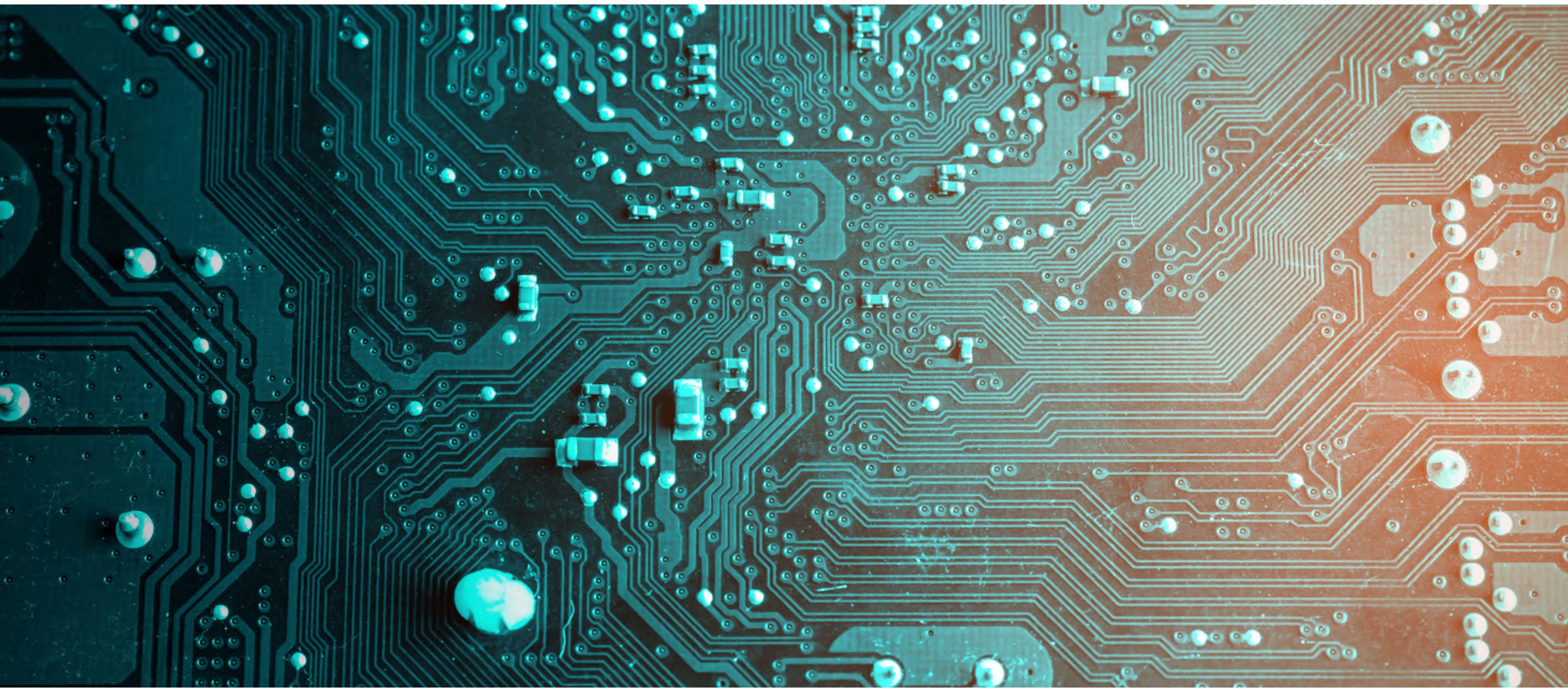
Kempegowda
INTERNATIONAL
AIRPORT
BENGALURU

THE COLLABORATION OF AIRPORT STAKEHOLDERS IN PROMOTING CYBER SECURITY CULTURE

MANOJ KUMAR A
BUSINESS ASSISTANT - CHIEF OPERATING OFFICER
BANGALORE INTERNATIONAL AIRPORT LIMITED

DECEMBER 2023 | AN ACI YEA 2024 REPORT

CONTENTS



EXECUTIVE SUMMARY

BY MANOJ KUMAR A

It's imperative for the aviation industry to prioritize the enhancement of cyber resilience through collaborative efforts on a global scale, involving multiple stakeholders.

The airport industry, with its ultra-sensitive nature, is attracting increasing attention from cybercriminals. The repercussions of a compromised fleet, coupled with the economic implications of reduced airport operations, and the potential for passenger data theft, all emphasize the criticality of cybersecurity in this sector.

The pandemic has adversely impacted revenues and cyber budgets, while cyber-attacks continue to persist.

The abrupt shift in our work culture, coupled with the pandemic's urgency and uncertainty, has provided a favorable ground for cybercriminals.

As a result, the industry must prepare for these attacks with greater diligence.

As the world navigates through the pandemic's aftermath, industries are at a heightened risk of uncertainty, majorly due to;

1. The rapid changes in the operational landscape.

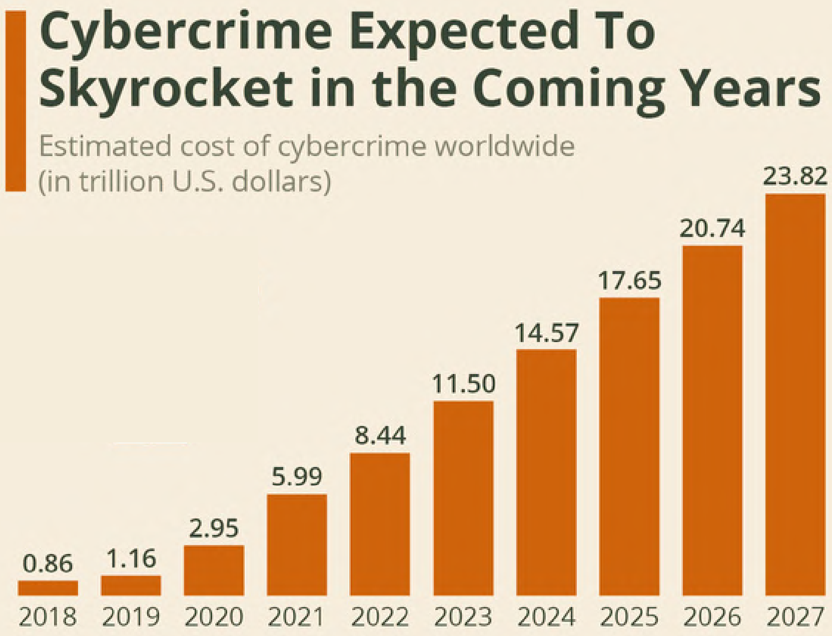
Work from home

Rapid Innovation

Fast rising attacks

Lean headcount

2. The consistent reprioritisation of the budget to align with business needs.



Graph showing the rise in cybercrime over the next few years.

SOURCE

Statista Technology Market Outlook, National Cyber Security Organisations, FBI, IMF.

As businesses continue to leverage deeper performance insights and embrace breakthrough technologies, the world is witnessing a shift towards faster, more flexible, and more efficient operations. This transformation is driving the convergence of physical and digital entities, connecting critical infrastructure assets, people, and data.

However, this growing interconnectivity also heightens the risks of security threats, necessitating a common understanding and approach to mitigate supply chain security risks and enable industry and government actors to implement appropriate countermeasures.

In addition to the traditional actors linked to the aviation industry, other industries are increasingly playing a vital role in the broader value and supply chains of the aviation ecosystem. Through acquisitions and partnerships, these non-traditional stakeholders are integral to the sector's success.

This report aims to address the challenges posed by the evolving aviation landscape.

Despite the industry's rapid technological innovation, its cyber security abilities have been slow to develop.

The aviation industry faces numerous challenges, including scale and complexity, interdependency, the nature of the challenge, and the vulnerability of management. To address these challenges, the industry must adopt a collaborative approach to counter the rapidly increasing threat of cyber security.

The following measures are recommended:

- Establishing a holistic framework to address cybersecurity risks and implementing it.
- Developing and implementing a third-party risk management strategy.
- Achieving clarity by identifying the roles and responsibilities of stakeholders.
- Strengthening the cybersecurity culture in the industry to enhance preparedness.
- Fostering transparency and trust in all industry operations to promote accountability and responsibility.
- Encouraging active communication and collaboration among stakeholders to promote information sharing.
- Developing effective workforce management strategies to ensure competent staffing.
- Establishing clear regulatory guidelines to ensure industry-wide compliance with cybersecurity standards.

INDUSTRY OVERVIEW

INDUSTRY OVERVIEW

The growth of aviation industry

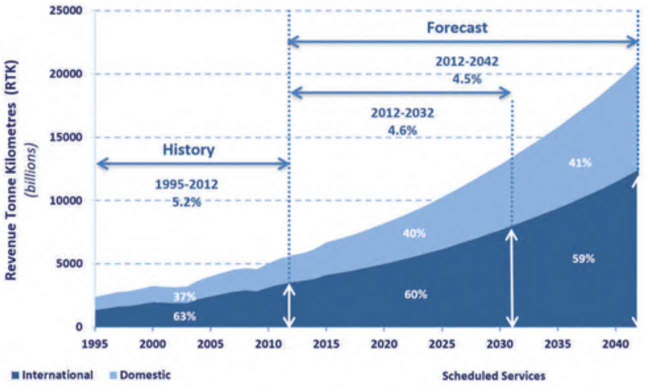
Over the past century, the aviation industry has made significant progress, advancing from the early stages of flight to achieving feats such as faster, longer, and heavier aircraft.

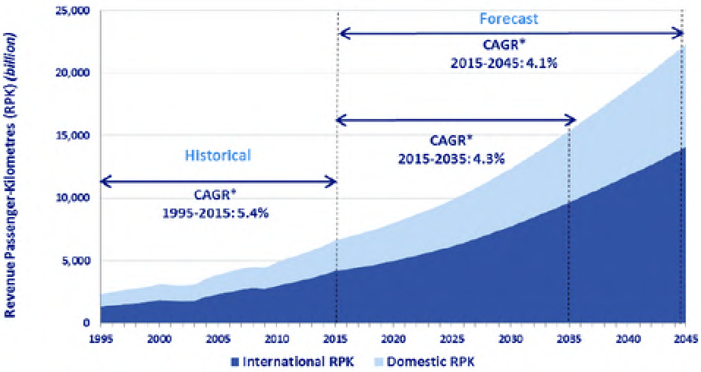
Today, there are over 100,000 commercial flights worldwide every day, making air travel one of the most reliable and secure modes of transportation.

The aviation industry continues to grow, and its future looks promising. In 2017, airlines transported approximately 4.1 billion passengers, and 56 million tonnes of freight, and operated 37 million commercial flights. Each day, airlines transport over 10 million passengers and goods worth around $18 billion.

This demonstrates the significant economic impact of aviation on the global economy, as the industry contributes 3.5% to the gross domestic product (GDP) worldwide, equivalent to $2.7 trillion. Moreover, aviation has created 65 million jobs across the globe.

According to recent estimates by ICAO, demand for air transport will continue to grow by an average of 4.3% per year over the next two decades, indicating a promising future for the aviation industry.





Source: ICAO, Meetings and Events, Future of Aviation.

If the air transport industry can maintain its projected growth path, it is anticipated that by 2036, the industry will generate 15.5 million direct jobs and contribute $1.5 trillion to the world economy in terms of GDP. When factoring in the impact of global tourism, these numbers could potentially increase to 97.8 million jobs and $5.7 trillion in GDP.

By the mid-2030s, the industry is expected to operate no fewer than 200,000 daily flights worldwide.

UNDERSTANDING THE SCOPE FOR CYBER ATTACKS

UNDERSTANDING THE SCOPE FOR CYBER ATTACKS

To reverse the downward trend in revenue, airports have had to embrace a technology-driven strategy. This approach involved revitalizing and accelerating digital transformation initiatives, adopting cloud-based digital infrastructure, leveraging new-age hyper-automation platforms, harnessing big data and digital business intelligence and analytics, and incorporating advanced technologies that require integration with third-party devices. While beneficial, this integration does increase the exposure to potential cybersecurity threats.

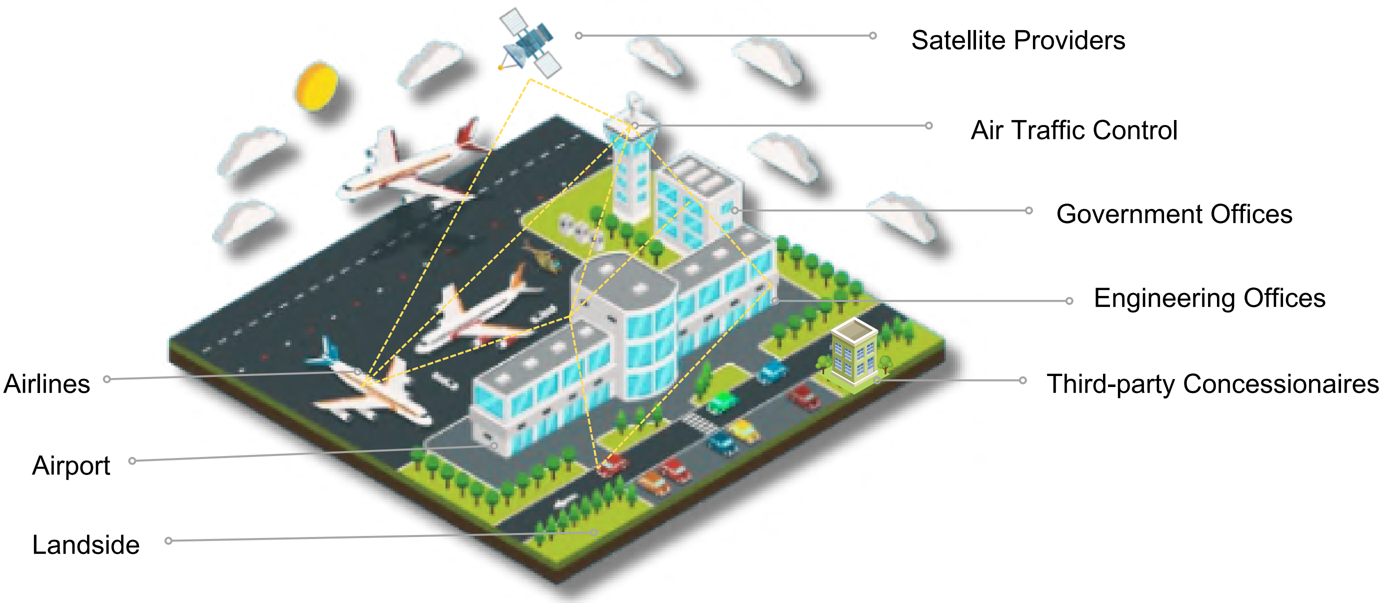


Figure 2 - Explaining the large attack surface of the aviation industry.

With the modernisation of the aviation industry, the integration of digital technologies has brought about significant transformations and novel challenges to the industry.

Historically, airport security measures have concentrated on addressing physical threats such as terrorism and smuggling. However, the emergence of digital systems has introduced new adversaries with the potential to exploit vulnerabilities in airport security protocols.

Cyber-attacks may arise from various sources such as state-sponsored hackers, criminal organisations, and individuals with insider access to sensitive information. These attacks can manifest as phishing, malware, ransomware, or denial-of-service (DoS) attacks.

It is essential for airports to integrate measures that address these digital threats to ensure the safety of their systems and passengers.

OVERVIEW OF CYBERSECURITY LANDSCAPE AT AIRPORTS

The following threat radar illustrates both current and developing threats in the cyber landscape, which cybercriminals are utilizing to attack the airport sector's most critical assets.

THREAT ACTORS

Corporate Espionage

Foreign Governments

Organized Crime

Domestic Business Competitor

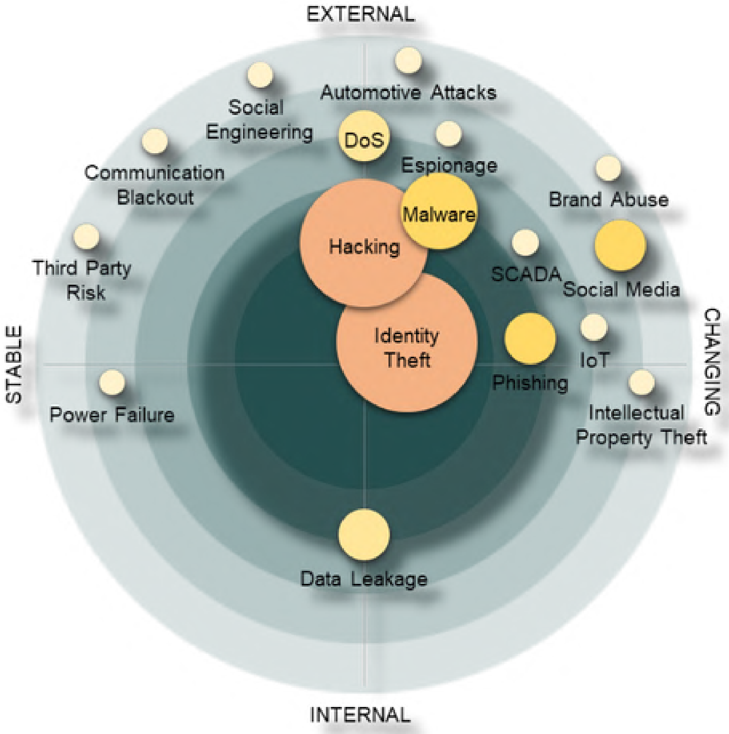
Criminally motivated individuals

Your own employees

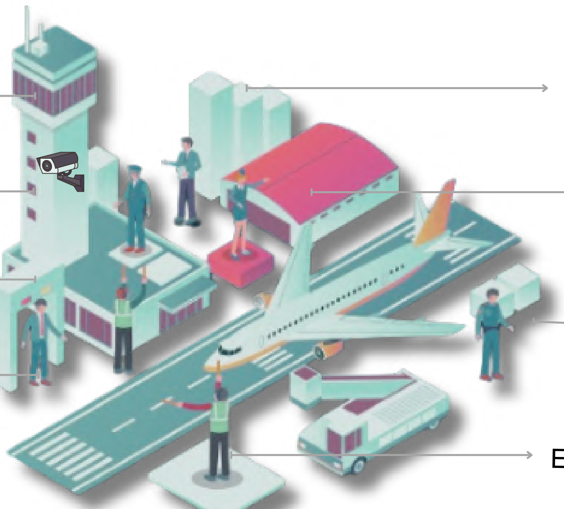
Foreign business competitor

Hacktivist/ Politically motivated

CYBER THREATS



CROWN JEWELS



Air-traffic Control Systems

Surveillance Cameras

Pax Processing Systems

Customer Information

Company Assets

Core Airport Systems

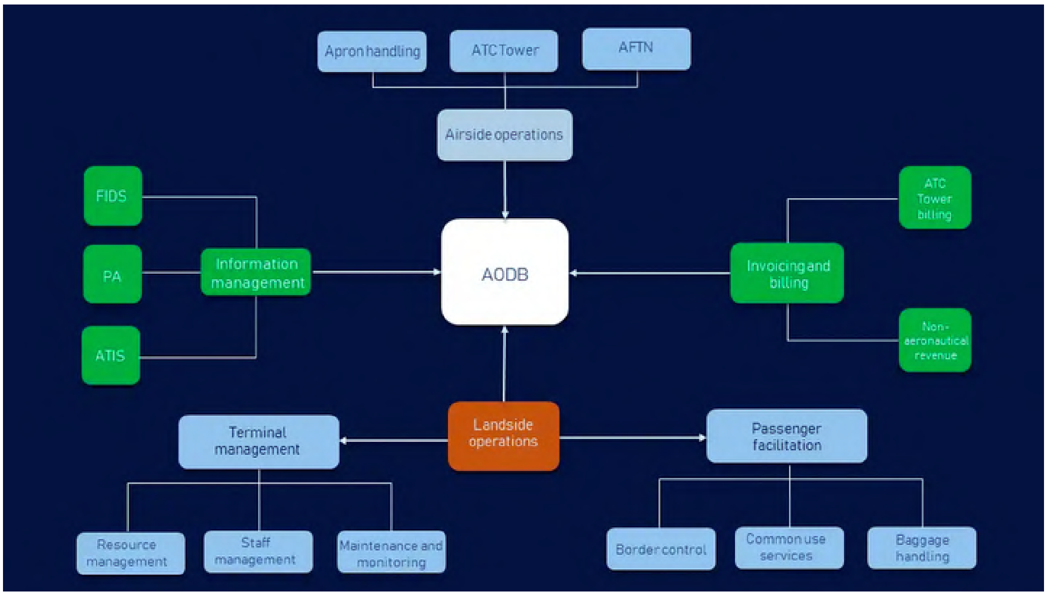
Baggage Handling System

Employee Information

TECHNOLOGIES USED AT AIRPORTS

Securing airports is a complex task as it involves securing an extensive range of connected devices and systems. Every component, from security cameras to baggage handling systems, is prone to cyber-attacks.

Furthermore, the interconnectivity of these systems implies that a single breach can have a cascading effect on the entire airport infrastructure. Therefore, to protect their assets and reputation, airports must prioritize and invest in robust cybersecurity measures.



Source: https://www.altexsoft.com/blog/airport-technology-management-operations-software-solutions-and-vendors/

TECHNOLOGY ADOPTION TRENDS IN AIRPORTS

>80%

- Passenger check-in and boarding
- Common use passenger processing sytems
- Traveller kiosk devices and web-services

>60%

- Communication Systems
- Baggage Handling Systems
- Smart building/ HVAC/ BMS

>50%

- Landside operations control system
- Airside operations control system

>20%

- SCADA
- Connection with other transportation systems

As per reports puplised by Georgia Lykou, Argiro Anagnostopoulou and Dimitris Gritzalis *, Department of Informatics, Athens University of Economics & Business (AUEB), GR-10434 Athens, Greece.

CYBER-SECURITY THREATS AND ITS IMPACTS

CYBER-SECURITY THREATS AND ITS IMPACTS

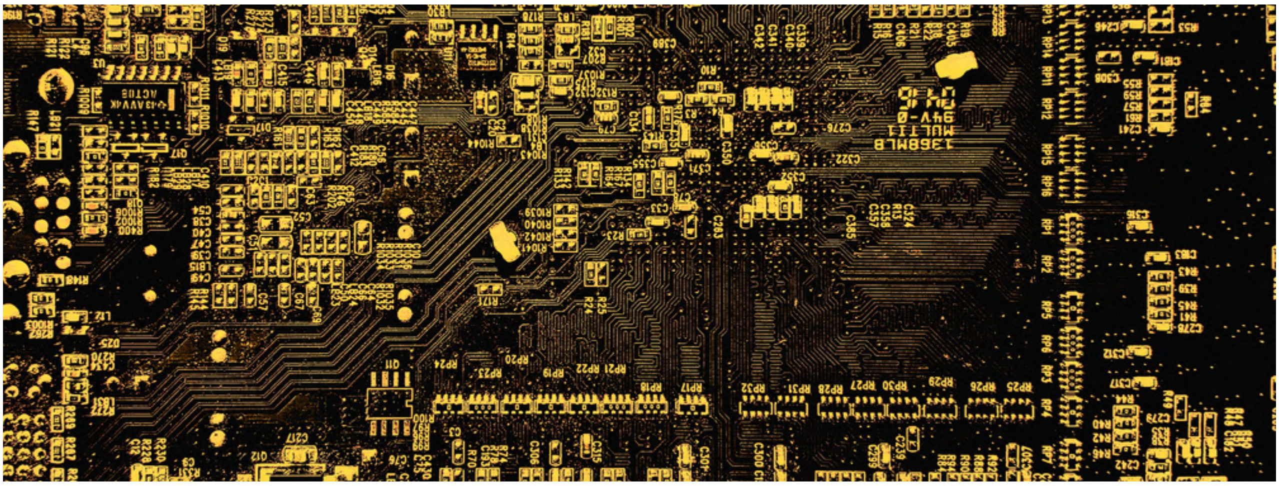
Over the past decade, the aviation industry has been subjected to an increased frequency of attacks alongside other sectors, resulting in a rise in cyberattacks. This trend has been further exacerbated in the aviation industry due to the COVID-19 pandemic, with an average of 50 cyberattacks each year since 2020.

Given the aviation industry's access to highly sensitive information such as passports and payment records, it has become a prime target for cybercriminals. While data security is a top priority in this sector, there is an even greater concern: the safety of passengers and crew. The avionic systems used in aircraft, including communication, navigation, flight control, and anti-collision technology, are essential for safe air travel. A breach of any of these systems could be catastrophic, resulting in hijacking or even a plane crash.

THE MODUS OPERANDI OF MALWARE ATTACKS AND RISKS

The aviation industry comprises a complex and interconnected network of stakeholders, each representing a potential vulnerability for malicious actors to exploit. Cyber attacks can occur via various entry points, including reservation systems, digital air traffic control, in-flight entertainment systems, cabin crew and cockpit instruments, and cargo handling systems.

Moreover, airlines are increasingly relying on advanced technological solutions to optimise their operations, reduce costs, and enhance efficiency. However, outsourcing IT departments and utilizing third-party vendors and commercial off-the-shelf (COTS) software can lead to a lack of robust security measures, increasing the risk of cyber attacks.



MAJOR CYBER SECURITY THREATS FACED BY THE AVIATION INDUSTRY

Ransomware

A ransomware attack, carried out by cybercriminals, involves the encryption and holding hostage of digital assets like computer systems or files. These attackers then demand a ransom from the victim as a condition for restoring access.

Social Engineering

Scam artists may impersonate airport officials or related organisations to deceive unwary customers and vendors.

Internal Security Threat

An internal security risk refers to potential threats to the security of an organisation that originate from within the organisation itself. These risks are associated with individuals or entities already affiliated with the organisation, such as employees, contractors, or business partners.

Supply Chain Attack

A supply chain attack is a type of cyber attack that targets the interconnected network of vendors, suppliers, and service providers within an organisation's supply chain.
Instead of directly targeting the primary organisation, the attacker seeks to compromise the systems or software of one of the suppliers or service providers with the ultimate goal of infiltrating the target organisation.

Malware

Malware, also referred to as malicious code and malicious logic, is an overarching term used to describe any software or firmware intended to perform an unauthorised process that will have an adverse impact on the confidentiality, integrity or availability of a system.

Denial of Services

When users of a system or service are not able to access relevant data, services or other resources, this can be accomplished by exhausting the service and its resources or overloading the components of the network infrastructure

CYBER-SECURITY THREATS AND ITS IMPACTS

Major cyber-attacks on airports

2022

Low-cost airline fell prey to ransomware attack in India

- led to the delayed departures of several flights.
While the airline was able to contain and rectify the situation and resume operations within a few hours, it left many passengers stranded at different airports.

2022

Canadian airline faced a cyberattack

- caused flight delays and operational glitches for five days.
The attack was reportedly due to a data breach at the company’s third-party service provider, which provides passenger management software solutions (e.g. check-in and boarding) for the airlines.

2021

Personal data of 4.5 million passengers were compromised

- of the largest aviation IT companies that caters for nearly 90% of airlines globally with its in-house Passenger Service System, was hit by a massive cyberattack in which hackers targeted servers containing personal data records of passengers dating back to a decade.

2020

British airline company fell prey to one of the biggest cyberattacks

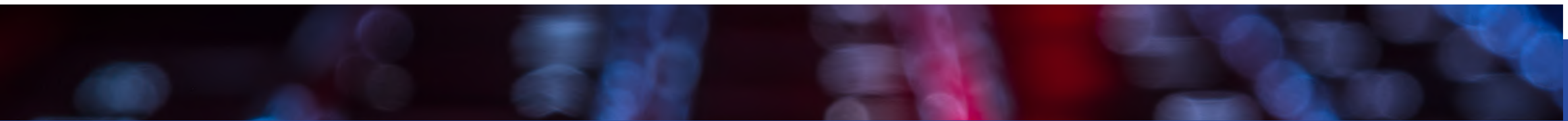
- personal data of nearly 9 million customers, including the credit card information of 2,000+ customers, was compromised. The company received major backlash and is now facing a class-action lawsuit seeking around £18 billion in damages.

2018

Largest British airline company had a major data breach

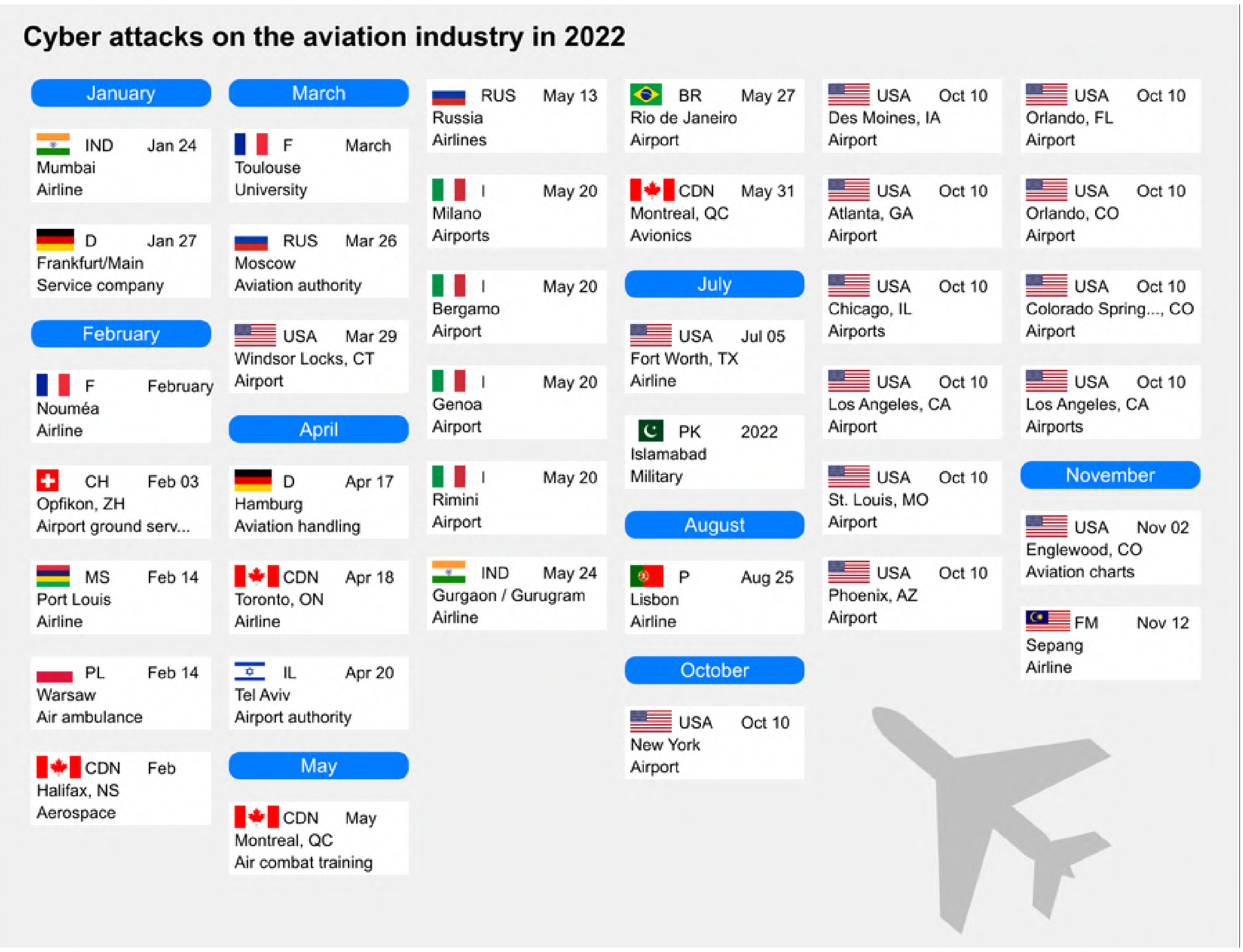
- personal data of over 400,000 customers and staff were compromised.
An investigation was conducted by the Information Commissioner's Office (ICO), which found that the breach occurred due to inadequate security measures taken by the airline to protect its customers’ data. As a result, the British airline company was fined a whopping £20 million.

Source: https://www.manageengine.com/log-management/cyber-security/cyber-security-in-aviation-risks-and-mitigation.



CYBER-SECURITY THREATS AND ITS IMPACTS

An overview of cyber-attacks on the aviation industry



Cyber attacks on the aviation industry in 2022

January			
IND	Jan 24	Mumbai	Airline
D	Jan 27	Frankfurt/Main	Service company
February			
F	February	Nouméa	Airline
CH	Feb 03	Opfikon, ZH	Airport ground serv...
MS	Feb 14	Port Louis	Airline
PL	Feb 14	Warsaw	Air ambulance
CDN	Feb	Halifax, NS	Aerospace
March			
F	March	Toulouse	University
RUS	Mar 26	Moscow	Aviation authority
USA	Mar 29	Windsor Locks, CT	Airport
April			
D	Apr 17	Hamburg	Aviation handling
CDN	Apr 18	Toronto, ON	Airline
IL	Apr 20	Tel Aviv	Airport authority
May			
CDN	May	Montreal, QC	Air combat training
RUS	May 13	Russia	Airlines
I	May 20	Milano	Airports
I	May 20	Bergamo	Airport
I	May 20	Genoa	Airport
I	May 20	Rimini	Airport
IND	May 24	Gurgaon / Gurugram	Airline
BR	May 27	Rio de Janeiro	Airport
CDN	May 31	Montreal, QC	Avionics
July			
USA	Jul 05	Fort Worth, TX	Airline
PK	2022	Islamabad	Military
August			
P	Aug 25	Lisbon	Airline
October			
USA	Oct 10	New York	Airport
USA	Oct 10	Des Moines, IA	Airport
USA	Oct 10	Atlanta, GA	Airport
USA	Oct 10	Chicago, IL	Airports
USA	Oct 10	Los Angeles, CA	Airport
USA	Oct 10	St. Louis, MO	Airport
USA	Oct 10	Phoenix, AZ	Airport
USA	Oct 10	Orlando, FL	Airport
USA	Oct 10	Orlando, CO	Airport
USA	Oct 10	Colorado Spring..., CO	Airport
USA	Oct 10	Los Angeles, CA	Airports
November			
USA	Nov 02	Englewood, CO	Aviation charts
FM	Nov 12	Sepang	Airline

Source: https://konbriefing.com/en-topics/cyber-attacks-2022-ind-aviation.html

HOW CAN AIRPORTS AVOID CYBER ATTACKS?

Type of attack	Prevention Methodology - An overview
Ransomware	Regular backups, employee training and awareness, endpoint protection, patch management, network security, email security, access control, multi-factor authentication, incident response plan, collaboration and information sharing, security audits and assessments, vendor security, continuous monitoring and legal and regulatory compliance.
Social Engineering	Phishing awareness programs, verification protocols, secure communication channels, strict access control, background checks, employee vigilance, secure physical access, regular security awareness campaigns and collaboration with industry stakeholders.
Internal Security Threat	Employee background checks, access control and least privilege, user activity monitoring, endpoint security, encryption, multi-factor authentication, anonymous reporting channels, code of conduct and policies, incident response plan, employee reviews and audits and privileged access management.
Supply chain attack	Vendor risk management, supply chain mapping, contractual safeguards, continuous monitoring, diversification of suppliers, supplier audits, resilience planning, information sharing, regulatory compliance, employee training, third-party security assessment and secure communication channels.
Malware	End point protection, regular software updates, email security, web security, network security, application whitelisting, USB device control, secure configuration, multifactor authentication, data backup and recovery and security audits and assessments.
Denial of Services	Network security, distributed denial or service (DDOS) protection, bandwidth management, load balancing, incident response plan, cloud-based services, traffic filtering and rate limiting, access control, redundancy and failover systems, monitoring and anomaly detection and collaboration with internet service providers.

ADDRESSING THIRD-PARTY RISK

A comprehensive examination of the notable and mounting hazard to the aviation industry.

As the aviation industry experiences exponential growth, driven by technological innovations such as automation, supply chain, IoT, and artificial intelligence, it's crucial to identify potential risks arising from third-party sources.

These risks need to be managed without compromising commercial profitability goals or damaging the reputation of the organisation. Such risks may include but are not limited to data breaches, loss of corporate assets, and misappropriation of intellectual property.

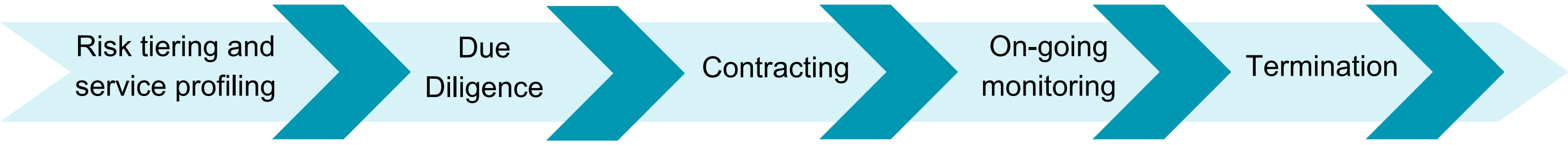
High Interdependency

Increasing Attacks

Critical Infrastructure

a coordinated and streamlined approach is essential while working with third-party eco-systems to build a cyber-resilient infrastructure

"A Case Study: BIAL's Approach to Third-Party Risk Management."



Risk tiering and service profiling	Due Diligence	Contracting	On-going monitoring	Termination
Identify Risk	Assess Risk	Manage Risk	Monitor Risk	Manage Risk
Risk tiering questionnaire is filled up	Information Security team reviews the risk	Contract sign-off subject to satisfying the policies	Continuous monitoring of the systems are ensured	Supplier has to sign off on the terminal clause

This approach not only mitigates risk but also enhances the organisation's comprehension of the entire system within the ecosystem.

BARRIERS TO INCREASING CYBER RESILIENCE

BARRIERS TO INCREASING CYBER-RESILIENCE

Policy levels exhibit a fragmented approach

The current practices of information security management systems and corporate governance are limited to individual organisations, which can result in cybersecurity risks being managed only within the organisation's perimeter. However, this approach is inadequate when dealing with a System-of-Systems architecture, as it can result in blind spots and a lack of understanding of residual risks from interconnection points in the supply and value chains. This can be further compounded by ambiguous accountability related to cyber resilience. To mitigate these risks, it is necessary to adopt an approach that extends beyond the organisation's perimeter and accounts for the interconnections and dependencies within the system.

Insufficient allocation of resources towards building resilience capabilities

The rapid shift to remote working, coupled with downsizing of the workforce and changes in operating models, has intensified the need for increased vigilance and attention to counter adversarial cyber activities. The aviation industry faces a challenging dilemma: while their exposure to cyberattacks remains high given their broad, complex and intricate attack surface, their ability to fund and resource cybersecurity defence has been significantly constrained. Striking a balance between operational, financial, and cybersecurity risks is vital for achieving long-term growth, prosperity, and resilience for both the organisation and the industry as a whole.

Rising intricacy and uncertainty

The aviation industry is a complex web of interconnected and interdependent actors, each with a crucial role to play. From supplying products to operating and integrating them, every entity contributes to the overall system's maintenance and functionality, including its subsystems. This intricate network has earned the industry the moniker "system of systems". Unfortunately, the sub-systems often developed independently of one another, with different organisations designing, integrating, and managing them at their discretion. This insular approach resulted in a lack of clarity in understanding the whole architecture, leading to ambiguous accountability. Although individual systems must function autonomously, they must also maintain interoperability and integration with all interconnected systems to ensure operational efficiency and overall cyber resilience.

Absence of clarity and transparency

It is widely agreed that having access to prompt and useful threat intelligence would significantly enhance a company's security. Regrettably, sharing such information between industry participants and government agencies is infrequent and limited by the absence of effective and standardized data-sharing frameworks. Additionally, navigating intricate and ever-changing data privacy laws and national security regulations both within and beyond an organisation presents significant challenges. These challenges raise concerns about legal responsibility and potential reputational harm if incorrect information is shared.

APPROACH TO CYBER RESILIENCE

ACHIEVING RESILIENCE IN CYBER SECURITY

To address barriers and challenges, decisive and collective action is required at 3 different levels.

Global Level

1. Foster a global consensus on regulations.
2. Establish a baseline for cyber resilience.
3. Encourage continuous assessments and industry benchmarking.
4. Develop information-sharing frameworks and standards.

Country Level

1. Establishing a structured approach for building skills
2. Acknowledging and incentivizing transparent communication concerning incidents
3. Cultivating a proactive stance on cybersecurity culture.

Organisation Level

1. Implementation of organisational cyber resilience principles
2. Implementation of ecosystem-wide cyber resilience principles

---

At the organisational level, the cyber resilience principles should mainly focus on fostering a culture of cyber resilience, integrating cyber resilience into business resilience practices and going beyond compliance.

HOW CAN AIRPORT STAKEHOLDERS COLLABORATE IN PROMOTING CYBER SECURITY CULTURE

HOW AIRPORT STAKEHOLDERS CAN COLLABORATE IN PROMOTING CYBER SECURITY CULTURE

Having a well-defined comprehension of the roles and duties of each stakeholder involved is crucial. The regulator shall mandate, or the airports shall proactively constitute a periodic joint working group to discuss and understand the systems involved in the eco-system, and the possible threats that could impact the organisations along with the mitigation measures and the procedure to deal with the threats.

Proposed framework for a collaborative approach.

Framework for addressing cyber security threats	Applicability
Classification of all data and/or assets according to a predefined data policy or classification, and the development of a business impact analysis on the criticality for each of the individual systems.	Airport operators, Airlines, Operating regulatory bodies, Ground handling agencies (GHA), Border Control, Customs, Service Providers, Cargo
Identify critical data and information systems software and hardware used by aviation industry operators, including airports, aircraft operators, ATS providers, communications service providers, ground handling agents, maintenance, repair and overhaul service providers operations.	Airport operators, Airlines, Operating regulatory bodies, GHAs, Border Control, Customs, Service Providers, Cargo

IDENTIFICATION PHASE

Framework for addressing cyber security threats	Applicability
Define common risk assessment criteria to ensure comparability.	Airport operators, Airlines, Operating regulatory bodies, GHAs, Border Control, Customs, Service Providers, Cargo
Establish mechanisms (at national, regional and international level) to share cyber threat information with trusted partners on the basis of sensitivity of information and data.	States, Governments, Industry partners and relevant entitites
Identify common internal and external threats that may impact aviation data and systems.	Airport operators, Airlines, Operating regulatory bodies, GHAs, Border Control, Customs, Service Providers, Cargo

RISK ASSESSMENT PHASE

continued..

Framework for addressing cyber security threats	Applicability
Identify known actors, including hackers, criminal organisations, insiders who are classified based on their skill level, available resources, and motives	Airport operators, Airlines, Operating regulatory bodies, GHAs, Border Control, Customs, Service Providers, Cargo
Study attack vectors — the avenue or channel an attacker uses to conduct an attack.	Airport operators, Airlines, Operating regulatory bodies, GHAs, Border Control, Customs, Service Providers, Cargo
Identify likely targets of cyber-attacks including IT systems and the data contained within or conveyed by these systems.	Airport operators, Airlines, Operating regulatory bodies, GHAs, Border Control, Customs, Service Providers, Cargo
Create a comprehensive inventory of potential targets, including their criticality to airport, airline and service provider operations; number of users served; vendors; software versions, patches, and updates; and data stored and exchanged.	Airport operators, Airlines, Operating regulatory bodies, GHAs, Border Control, Customs, Service Providers, Cargo

RISK ASSESSMENT PHASE

Framework for addressing cyber security threats	Applicability
Identification of information security roles and responsibilities of its employees connected stakeholders.	Airport operators, Airlines, Operating regulatory bodies, GHAs, Border Control, Customs, Service Providers, Cargo
Development of a process for establishing and enforcing strategic/tactical planning, policies and procedures which support both cybersecurity activities and, ultimately, the operational activities of the concerned organisation	Airport operators, Airlines, Operating regulatory bodies, GHAs, Border Control, Customs, Service Providers, Cargo
Adoption of a cybersecurity framework established either by its national government or an international standard (e.g. ISO 27001)	Airport operators, Airlines, Operating regulatory bodies, GHAs, Border Control, Customs, Service Providers, Cargo
Prioritisation of the necessary funding for establishing and maintaining a secure cyber environment	Airport operators, Airlines, Operating regulatory bodies, GHAs, Border Control, Customs, Service Providers, Cargo

DETERMINATION OF VISION

It is highly necessary for the entity to prioritize security considerations in every stage of the aviation information and communication technology systems' life cycle, from design and development to operation, maintenance, and secure disposal of hardware and software.

Modifications, revisions, updates, and upgrades must be secured for existing systems.
From the design stage, physical and logical safeguards should be implemented to guarantee the continual maintenance of confidentiality, integrity, and availability of systems and data.

To achieve this, a multi-layered approach should be employed, including but not limited to:

PROTECTION PHASE

A. ADMINISTRATIVE CONTROLS

1. Establishing stringent security standards, policies, and procedures.
2. Implementing access management protocols to regulate system entry.
3. Preventing tampering with systems and data.
4. Developing and enforcing policies governing the utilisation of hardware, software, applications, and data.
5. Protecting digital property rights through the implementation of anti-tamper solutions, legal clauses, and restrictions on sharing software code.

B. QUALITY CONTROLS

1. Ensuring the security of the hardware and software supply chain.
2. Establishing disaster, emergency, and contingency plans.
3. Conducting regular cybersecurity reviews and audits.

C. TECHNICAL CONTROLS

1. Access control policies
2. Firewalls and other network security components
3. Data protection and encryption
4. Data destruction in adherence to the policy
5. Malware and intrusion detection systems
6. Network integrity measures
7. Strong password policies
8. Continuous patch management
9. Log management policies and program

D. PHYSICAL CONTROLS

1. Ensure that data centers, communication facilities, and other hardware locations are appropriately secured with restricted access.
2. Utilize physical access control systems that include multi-factor authentication, biometric systems, and authorized access.
3. Develop contingency plans that incorporate remote backup systems in the event of primary system loss.
4. Implement an Electronic Waste (e-waste) Management system for discarded computers, airport and office electronics equipment, and other devices.
5. Establish a clear process for disposing of e-waste.

MONITORING AND REPORTING PHASE

TRAINING AND AWARENESS

It's essential for each entity to ensure that the security of critical information systems is entrusted to trained and appropriately recruited personnel. These individuals should have access to a well-defined training syllabus, guidelines, and content to assist them in operating, handling, installing, and maintaining critical information systems. Moreover, all associated personnel should receive regular and periodic training on cybersecurity awareness.

CONTINUOUS MONITORING

1. Ensure compliance with information security requirements that align with the organisation's mission, business functions, national laws, regulations, and requirements.
2. Maintain awareness of the latest threats and communicate regularly with management regarding changes in threat levels and risk assessment reports.
3. Conduct regular reviews of security controls to ensure their effectiveness and identify any areas that need improvement.

INCIDENT REPORTING

Timely and accurate reporting of cyber incidents allows for swift responses, enabling organisations to contain and mitigate potential damages. It facilitates the sharing of crucial threat intelligence, empowering others to bolster their defenses against similar attacks.

Additionally, reporting incidents contributes to a collective understanding of emerging cyber threats, aiding in the development of more robust cybersecurity strategies and regulations. This transparency not only safeguards individual entities but also fosters a collaborative environment where shared knowledge becomes a potent tool in the ongoing battle against cyber adversaries.

POST-EVENT ANALYSIS

A post-event analysis is crucial for organisations as it serves as a valuable learning mechanism after an incident or event. By dissecting the details of what occurred, organisations gain insights into the vulnerabilities that were exploited and the effectiveness of their response measures.

This analysis helps in refining and strengthening security protocols, identifying areas for improvement, and implementing preventative measures to avoid similar incidents in the future. The knowledge gained from post-event analysis not only enhances an organisation's overall resilience but also contributes to the evolution of proactive cybersecurity strategies.

In essence, it transforms incidents into opportunities for growth, ensuring that lessons learned today fortify the defenses of tomorrow.

To ensure the effectiveness of the aforementioned framework, it's crucial to adopt a continuous collaborative approach.

Here are some recommendations to achieve that objective.

01 Fostering meaningful partnership and trust

One of the most effective ways airports can heighten security awareness is by fostering collaboration with airlines through partnership and trust. This involves establishing and nurturing mutual understanding and respect between airport and airline security stakeholders. Regular communication, transparent information sharing, joint decision-making, and collaborative problem-solving can help build a strong and cohesive security community. By developing such partnerships, airports can foster a culture of recognition and appreciation to further enhance security measures.

02 Collaborating and organising engagement activities

Airports can further enhance security awareness by collaborating with airlines to organise and participate in engagement activities. These initiatives aim to increase the involvement of airline staff and passengers in security matters and can encompass a wide range of activities such as training sessions, workshops, simulations, exercises, quizzes, surveys, and rewards. By offering engagement activities, airports can create a positive and interactive learning environment, which fosters a culture of security awareness among all stakeholders.

03 Creating and upholding coordination mechanisms

One effective approach for airports to enhance security awareness is by creating and upholding coordination mechanisms to foster collaboration and cooperation between airport and airline security teams as well as other stakeholders. Coordination mechanisms can come in various forms, such as committees, working groups, task forces, meetings, reports, and audits. These mechanisms guarantee alignment and consistency of security policies and standards, as well as effective resolution of security issues and challenges.

04 Effective & consistent communication channels

To enhance security awareness, airports can collaborate with stakeholders by establishing effective and consistent communication channels. These channels should facilitate the sharing of relevant and timely information about security threats, procedures, and regulations, as well as provide feedback and guidance on best practices. Communication channels may include newsletters, webinars, posters, brochures, videos, and social media. By utilizing multiple and diverse communication channels, airports can reach a wider audience and reinforce their security messages.

05 Adopt and promote new technological innovations

Airports can significantly enhance their security protocols by actively collaborating with airlines to adopt and promote new technological innovations. These advancements include but are not limited to biometric identification, artificial intelligence, blockchain, robotics, and smart devices. By exploring and implementing these new solutions, airports can significantly improve the efficiency and effectiveness of their security operations, leading to better security outcomes and an enhanced competitive edge. Additionally, this adoption of innovation and technology can result in a more seamless and convenient security experience for customers, further improving the overall travel experience.

06 Conduct regular awareness sessions

It's crucial to educate current employees on cyber security to safeguard systems and respond effectively in the event of a cyber attack. One effective approach is to conduct regular awareness sessions on cyber security in every department of the company.

Moreover, it's advisable to enlist the services of cyber security experts with specialized knowledge in aviation IT and systems. In addition to training current cyber security experts on this technology, members of the aviation industry can also contribute to training future cyber security professionals.

CASE STUDY: INDUSTRY BEST PRACTICES

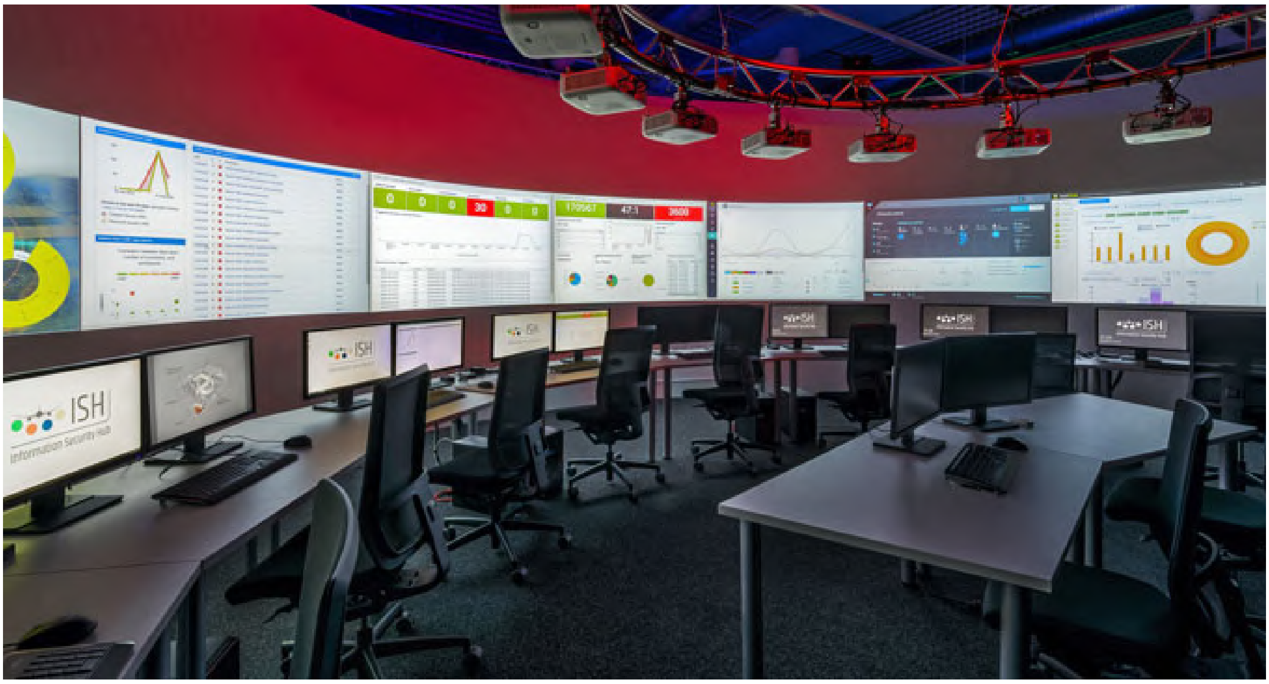
1. MUNICH AIRPORT'S NEW INFORMATION SECURITY HUB

With the spread of digitalisation in recent years, there has been a massive increase in the number of attacks on the IT systems of companies and public authorities in Germany. Munich Airport has also become the target of cyberattacks on a daily basis. The airport has already taken a proactive approach to develop strategies for defending against cyberattacks and new approaches to fight against cybercrime.

"First of all, we focus on creating the overall awareness for security issues in our corporation," says Marc Lindike, Head of Information Security Assurance at Flughafen München GmbH (FMG). "Second, we concentrate on strong prevention measures, solid security perimeters and defence mechanisms in case of a successful breach of the perimeter."

Some years ago, Munich Airport also introduced a security awareness programme for the entire staff to highlight the importance of cybersecurity. "This programme shows positive results," Lindike adds.

Moreover, the airport recently opened its own Information Security Hub (ISH) – a competency centre where the airport operating company FMG and IT specialists will work together with experts from the European aviation industry.



Picture - Munich Airport's new Information Security Hub

2. AIRBUS AND SITA'S SECURITY OPERATIONS CENTER SERVICES

"Cyberattacks are a very real threat, with the potential for huge knock-on effect in an industry as interwoven as the air transport industry," says Vivien Eberhardt, Director, SITA Cybersecurity.

"Layers upon layers of infrastructure could be impacted, with the consequence on global travel reverberating across the world. That is why the industry has placed such a high priority on cybersecurity to ensure that it stays one step ahead of a potential attack."

To meet this demand, last year SITA partnered with Airbus to develop the Security Operations Center (SOC) – a tailored, industry-wide response to cybersecurity. The new incident detection services provide airlines, airports and other air transport industry stakeholders with information about unusual cyber activity that may impact their business.

By joining forces, SITA and Airbus can provide the most advanced cybersecurity solutions for the industry. "Together we will use our expertise to detect cyber activity relevant to airlines and airports," adds Eberhardt. "When requested, the joint Security Operations Center Services will provide appropriate containment and remedial action that a company's digital assets are safe from attacks."

CONCLUSION

In the end, the development of a collaborative culture among airport stakeholders is essential to strengthen defenses against cyber threats and promote a robust cybersecurity stance within the aviation industry. The intricate nature of modern airport operations, alongside the interconnectivity of information systems, emphasizes the necessity of a unified and cooperative approach to cybersecurity.

The cooperation between airport stakeholders such as government agencies, airlines, airport authorities, service providers, and technology vendors is vital to establish a comprehensive and resilient defense against the ever-evolving hazard of cyber threats. The exchange of information, best practices, and intelligence regarding potential threats contributes to a collective understanding of emerging risks, enabling stakeholders to implement proactive measures and react quickly to potential breaches.

A cybersecurity culture of collaboration not only enhances the technical aspects of defense but also promotes a shared responsibility for preserving the integrity and safety of airport operations. This collaborative mindset permeates throughout the entire aviation ecosystem, from top-level decision-makers to front-line staff, emphasizing the importance of cybersecurity awareness, training, and adherence to established protocols.

The propagation of a culture of cybersecurity among airport stakeholders not only safeguards critical infrastructure but also boosts the confidence of passengers and business partners in the reliability of air travel. Trust is paramount in the aviation industry, and a collective commitment to cybersecurity reinforces the industry's dedication to the safety, privacy, and well-being of all stakeholders.

In conclusion, ***the concerted efforts of airport stakeholders in nurturing a cybersecurity culture significantly contribute to the overall resilience and adaptability of the aviation sector in the face of an ever-changing threat landscape. By working together, sharing knowledge, and aligning strategies, airport stakeholders can effectively navigate the challenges posed by cyber threats, ensuring the continued safety and security of air travel in an increasingly digital world.***

REFERENCES

World Economic Forum & Deloitte. (2021). Pathways Towards a Cyber Resilient Aviation Industry. Insight Report, 2021.

The Cybersecurity Landscape for Airports: Threats and Mitigation. (2023, June). https://colortokens.com.

Rise in Cyberattacks in Aviation Post-Pandemic - GlobalSign. (2022, November). GlobalSign. https://www.globalsign.com/en/blog/aviation-rise-cyberattacks-post-pandemic

BEUMER Group. (2023, October 26). Cybersecurity for airports: Safeguarding against today's threats - BEUMER Group.

Reed, J., and Reed, J. (2023, June 14). Increasing insider cyber threats pose risks to aviation. Avionics International.

Xti, S. (2022, September 27). Top cyber threats faced by the aviation industry - SOCRADAR. SOCRadar® Cyber Intelligence Inc. https://socradar.io/top-cyber-threats-faced-by-the-aviation-industry/

Warren, K. (2023, June 28). Cyber Security in Aviation Facing Increased Challenges: A variety of moving pieces makes it hard to mount a. Transport Security International Magazine. https://www.tsi-mag.com/cyber-security-in-aviation-facing-increased-challenges-a-variety-of-moving-pieces-makes-it-hard-to-mount-a-proactive-defense-against-hackers

Dimitrova, M. (2018, February 27). Cybersecurity – industry collaboration key to meeting "very real threat of cyberattacks." Future Travel Experience. https://www.futuretravelexperience.com/2018/02/cybersecurity-industry-collaboration-key-to-meeting-very-real-threat-of-cyberattacks/

Airport Management. (2023, November 12). How can airports collaborate with airlines to enhance security awareness? www.linkedin.com. https://www.linkedin.com/advice/0/how-can-airports-collaborate-airlines-enhance#communication-channels

Kazda, A., Badánik, B., and Serrano, F. (2022). Pandemic vs. Post-Pandemic Airport Operations: Hard Impact, Slow Recovery. Aerospace, 9(12), 810. https://doi.org/10.3390/aerospace9120810

Cybersecurity in aviation: Risk and mitigation. (2022, December 29). Manage Engine Log360.

IATA. (2019). Aviation Cyber Security Roundtable. Singapore, IATA Regional Office, Asia Pacific.

Eurocontrol EATM. (n.d.). EUROCONTROL EATM-CERT Services. Think Paper #12.

Cyber Security Action Plan. (2022). 39th Session of the International Civil Aviation Organisation, 2.

Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls. (2018b). MDPI.

Future of aviation. (n.d.). https://www.icao.int/Meetings/FutureOfAviation/Pages/default.aspx

Kempegowda
INTERNATIONAL
AIRPORT
BENGALURU