# Securing the Skies: Innovating Cybersecurity Governance for India's Emerging Small Airports

**Shreyas Kumar[1], Surya Pal Gangwar[2], Nakul Singh[3], Rishabh Pagaria[1,] Anika Garg[1] and Saptarishi Das[1]**
[1]Texas A&M University, USA
[2]IIM Indore, India
[3]Independent Researcher

shreyas.kumar@tamu.edu

**Abstract:** Cybersecurity policy and governance are becoming increasingly critical as small airports in India undergo rapid expansion in operational capacity and digital integration under government-led initiatives like the Regional Connectivity Scheme RCS-UDAN. This paper investigates the cybersecurity readiness and governance challenges small airports face, specifically within the transformative context of Uttar Pradesh's civil aviation sector. Uttar Pradesh, India's most populous state, has witnessed significant infrastructure innovation and policy-driven growth in aviation, exemplified by the ambitious Civil Aviation Promotion Policy of Uttar Pradesh 2017, which aimed at enhancing regional connectivity and economic inclusivity. However, this rapid advancement and digitalization, involving extensive integration with national and international air travel networks, has simultaneously introduced substantial cybersecurity vulnerabilities. Utilizing a Public Sector Innovation (PSI) framework, this research evaluates innovative policy approaches and governance mechanisms for managing and mitigating these cybersecurity risks. The study highlights vulnerabilities from increased complexity, limited administrative and technical capacities, and resource constraints typical of smaller airport operations. It argues for the urgent need to develop tailored cybersecurity frameworks that effectively address local contexts while ensuring alignment with broader national and international cybersecurity standards. Key recommendations include establishing clearly defined governance structures for cybersecurity oversight, enhancing multi-stakeholder coordination across different administrative levels, promoting extensive cybersecurity awareness and training programs, and instituting robust and responsive incident management and recovery mechanisms. These policy innovations and governance reforms are crucial not only for safeguarding critical aviation infrastructure but also for supporting sustainable economic growth, resilience, and inclusive development within India's rapidly evolving civil aviation landscape. This paper provides valuable insights for policymakers, regulators, airport operators, and technology providers, offering a strategic roadmap toward comprehensive cybersecurity preparedness for India's small airports.

**Keywords**: Airport cybersecurity, Public sector innovation, Cyber risk governance, Digital aviation policy, RCS-UDAN

## 1. Introduction

India’s aviation sector is experiencing a rapid transformation through ambitious policy interventions like the RCS-UDAN initiative (K. Chandrashekhar et al., 2019), which aims to enhance air connectivity to underserved and unserved regions. At the heart of this transformation lies a growing network of small airports, particularly in populous and economically diverse states such as Uttar Pradesh. The number of operational airports in India has nearly doubled from 74 in 2014 to 157 in 2024 (GOI, 2024) under such regional connectivity programs, reflecting a dramatic expansion of aviation infrastructure into smaller cities and towns. As these airports transition to advanced digital technologies to streamline operations and improve efficiency, they simultaneously face increased exposure to cybersecurity threats. This digital transformation creates the need for policymakers to rethink and innovate cybersecurity governance structures.

Despite the critical importance of aviation to economic development and regional connectivity, cybersecurity at small airports has historically been under-prioritized. Smaller airports often lack the robust IT defenses such as outdated softwares, threat detection systems, trained cybersecurity teams with respect to larger hubs, making them potential weak links in the broader air transport network (Nasscom, 2023). Cyber-attacks on airport systems can disrupt not only local operations but also have cascading effects on the national aviation system and passenger trust. Recent incidents globally underscore that even regional airports are not immune to cyber threats, from ransomware disrupting airport systems to hackers breaching critical infrastructure (Aliyu et el., 2022). This paper addresses the pressing need for robust, localized cybersecurity governance frameworks tailored to the operational realities of small airports. It introduces a Public Sector Innovation PSI framework (OECD-OPSI, 2024), a novel lens to conceptualize governance reform and policy innovation for Small Airports. Through this approach, the paper aims to bridge the gap between policy intent and on-ground implementation in cybersecurity readiness for aviation infrastructure, drawing learnings and insights from international best practices. By situating India’s challenges in a global context, the research seeks to inform a forward-looking strategy to secure the skies over India’s emerging regional hubs.

## 2. Background

India's Regional Connectivity Scheme (RCS-UDAN), launched in 2016 (K. Chandrashekhar et al., 2019), aims to make air travel accessible to the common citizen by enhancing connectivity to regional and remote areas. Under this scheme, Uttar Pradesh has emerged as a key beneficiary, with a number of small airports being developed or upgraded. The state's Civil Aviation Promotion Policy 2017 (Invest UP, 2017) outlined strategies to boost infrastructure, attract private investment, and integrate regional airports with the national aviation network. This policy led to substantial incentives for new airports and routes in the state, which accelerated the growth of small airports in cities like Kanpur, Prayagraj, and Hindon (Ghaziabad). However, the cybersecurity dimension of this expansion and other regional airports within India remain underdeveloped (Aliyu et el., 2022). While physical infrastructure and flight operations received attention, digital security considerations lagged behind. The CAPP 2017, for instance, focused on infrastructure development and service connectivity but did not explicitly mandate cybersecurity measures for new airports. Airport operations have been adopting digital air traffic management systems, electronic ticketing, and IoT-driven surveillance and baggage handling systems, causing them to become increasingly vulnerable to cyber threats. This context sets the stage for assessing cybersecurity not just as a technical issue, but as a governance and policy challenge that requires a tailored and innovative response.

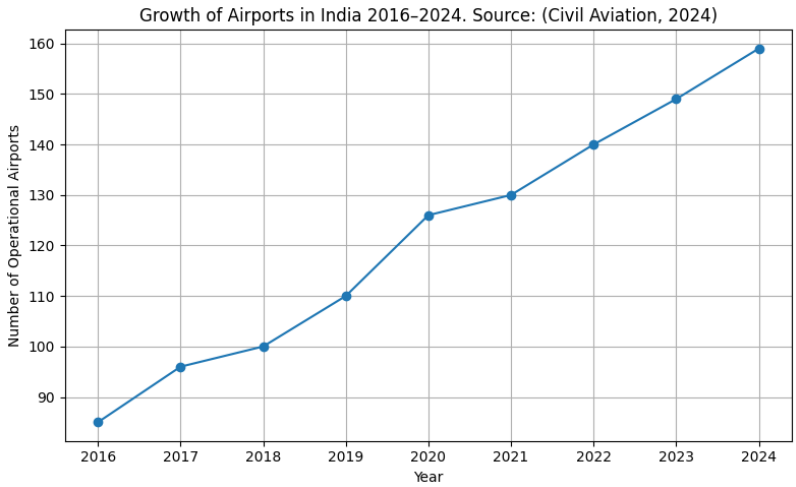


**Figure 1: Illustrates the growth of number of airports at Indian aviation Industry**

Nationally, India's approach to cybersecurity in critical infrastructure has been evolving, but aviation-specific governance frameworks are still nascent. The Directorate General of Civil Aviation DGCA, the primary regulator for civil aviation in India, deals primarily with safety and regulatory compliance for airlines and aircraft. There is currently no dedicated civil aviation cybersecurity regulation equivalent to those seen in other domains like banking or power. Instead, airports largely fall under general IT laws i.e. The Information Technology Act 2000 (Indiacode, 2000), the oversight of agencies like CERT-In Indian Computer Emergency Response Team for vulnerability and incident reporting formed under the Ministry of Communications and Information Technology (Cert-in, 2025) and the Bureau of Civil Aviation Security BCAS responsible for airport security standards, has traditionally emphasized physical security like baggage screening, personnel verification, hijack preparedness, etc over cybersecurity (Civil Aviation, 2024). This governance gap means that small airports, many of which are managed by the Airports Authority of India (AAI) or state governments, do not have a uniform set of cybersecurity guidelines to follow. In contrast, internationally, civil aviation is increasingly recognized as part of nations' critical information infrastructure, with bodies like the International Civil Aviation Organization (ICAO) urging member states to develop aviation cybersecurity strategies. The absence of a strong domestic framework in India puts small airports in a vulnerable position and highlights the need for localized policy innovation that aligns with global standards.

## 2.1 Cybersecurity Threat Landscape for Small Airports

### *2.1.1 Legacy systems with minimal security controls*

Many regional airports still rely on legacy IT and operational technology (OT) systems that were not designed with cybersecurity in mind. Outdated software and hardware, such as older flight information display systems or building management systems, may lack modern authentication or encryption, making them easier targets for intrusion. Attackers can exploit unpatched vulnerabilities in these old systems to gain a foothold in the airport network.

### *2.1.2 Limited budgets and cybersecurity staffing*

Smaller airports operate on tighter budgets and often cannot afford dedicated cybersecurity teams or sophisticated security tools. It is common for an airport's entire IT staff to be just a few individuals who juggle multiple roles. According to industry observers, it is a rare exception for a medium or small airport to have a staff member solely devoted to cybersecurity. This lack of specialized personnel means that threat monitoring, incident response planning, and security training may be minimal or absent. Security executives at such airports struggle to keep up with rising threats amidst constrained resources, leading to reactive postures.

### *2.1.3 Dependence on outsourced IT services*

Small airports frequently outsource their IT maintenance and support to third-party vendors due to lack of in-house expertise. While this can be cost-effective, it introduces risks if vendor contracts do not include stringent cybersecurity clauses or service level agreements. A notable case underscoring this vulnerability occurred at Albany International Airport in December 2019, when a ransomware attack encrypted the airport's entire database via their outsourced IT provider, forcing the operator to pay a six-figure ransom to regain access (Cybersecurity Insiders, 2019) . The incident revealed how an airport's cybersecurity is only as strong as that of its least secure contractor. After the attack, Albany Airport cut ties with the vendor, but only in the aftermath of a costly breach.

### *2.1.4 Interconnection with larger networks*

Small airports are not siloed; they connect with airlines, reservation systems, national air traffic control, and sometimes with larger hub airports' systems for data exchange. This interconnection means a breach at a small airport could potentially serve as a pivot point into broader aviation networks or disrupt services like ticketing and baggage handling that are linked with airline central systems. For example, a cyber incident at a regional airport's communications system could propagate delays or alerts to the national level. In Europe's aviation sector, it has been recognized that a weak link in one airport can impact others, motivating a common security approach. The extensive interconnection in aviation amplifies the potential impact of any single cyber incident (ENISA, 2016; Eurocontrol, 2021).

### *2.1.5 IT/OT convergence and lack of segmentation*

Airports rely on both Information Technology (IT) systems like administrative networks, ticketing, etc, and Operational Technology (OT) systems like runway lighting controls, HVAC, fueling systems, baggage conveyors (Georgia et al., 2018). In many small airports, these networks are not properly segregated. The lack of network segmentation means that a malware infection on the corporate network could spill over into OT systems that manage safety-critical operations. For instance, ransomware could simultaneously disable an airport's website and its baggage sorting system, doubling the disruption. This convergence of IT and OT without adequate isolation was a factor in the Bristol Airport cyber incident in the UK 2018 (BBC, 2018), where a ransomware attack took down flight information screens for two days. Airport officials had to resort to manual whiteboards for flight updates, illustrating how an IT breach which targeted display systems had IT and operational consequences like delays in baggage handling and passenger processing.

### *2.1.6 Increasing sophistication of threats*

The cyber threat landscape is continuously evolving, with threat actors employing increasingly sophisticated techniques to compromise systems and networks. The aviation sector, being a critical infrastructure, has witnessed a rise in the sophistication of cyber attacks, with threat actors employing advanced techniques to compromise systems and networks (Cyfirma, 2024). Talking about the incident that took place in August 2024, Seattle-Tacoma International Airport faced a ransomware attack that disrupted core operations and forced

manual workarounds. The incident, linked to a $6 million ransom demand, exposed critical weaknesses in outdated airport systems and emphasized the need for stronger cybersecurity protections (The Record, 2024).

## 3. Related Work

As small and regional airports increasingly integrate with national aviation infrastructure and digitize core operations, their exposure to cybersecurity threats grows significantly. Unlike major international hubs, these small facilities often lack the financial and human capital needed to implement robust security protocols. Studies by Georgia et al. (2018) and Romy et al. (2024) highlight systemic limitations in these airports, including minimal IT staffing, outdated systems, and weak implementation of essential cybersecurity measures such as firewalls and network segmentation. The presence of legacy operational technology (OT) systems without proper integration into cybersecurity planning further exacerbates vulnerabilities. Elochukwu et al. (2021) note that adversaries often exploit these weaknesses to access broader aviation systems, identifying small airports as soft entry points within interconnected networks.

The aviation sector more broadly has emerged as a high-value target for both financially motivated and state-sponsored cyberattacks. Ransomware, supply chain intrusions, and politically motivated hacks have increased in frequency and sophistication, as documented by Schafer (2022), Cyfirma (2024), and Elochukwu et al. (2021). Advanced persistent threats (APTs) now employ diverse tactics—from phishing to credential stuffing often aimed at IT infrastructure that lacks robust defenses. Real-world cases such as the Albany International Airport ransomware attack (Cybersecurity Insiders, 2019), the Cleveland Hopkins malware breach (News5 Cleveland, 2019), and the politically charged Vietnam airport hack (Forbes, 2016) underscore the reality that small and mid-sized airports are no longer peripheral—they are now primary targets in the global threat landscape.

Despite the presence of international standards like ISO/IEC 27001, the NIST Cybersecurity Framework, and ICAO's Cybersecurity Strategy (Masike M., 2023; Mohammed, K., 2023; ICAO, 2024), a significant gap exists between policy and implementation especially in the Indian context. Nasscom (2023) and Civil Aviation (2024) reports reveal the absence of aviation-specific cybersecurity mandates, resulting in airports operating under generalist IT laws such as the Information Technology Act, 2000. Regulatory responsibility is fragmented across agencies like DGCA, CERT-In, and BCAS, leading to overlapping mandates and ambiguous enforcement, particularly for resource-constrained airports. This fragmented governance structure often causes compliance fatigue and partial security implementations, increasing the risk of cyber incidents (Georgia et al., 2018).

Recognizing these constraints, recent literature emphasizes the importance of contextual and adaptive cybersecurity governance. Scholars like Nickolaos K. et al. (2020) and OECD-OPSI (2024) argue that a multi-layered approach combining technical controls, human resource development, and collaborative governance is essential. The Atlantic Council (2019) reinforces this view, asserting that aviation cybersecurity cannot be managed in silos and requires synchronized efforts across regulators, operators, vendors, and other stakeholders. These studies point toward the need for governance models that are responsive to local conditions and flexible enough to evolve with emerging threats.

This body of research forms the foundation for introducing the Public Sector Innovation (PSI) framework as a flexible, scalable, and context-sensitive approach to cybersecurity governance.

## 4. Methodology

This research study uses a qualitative, multi-method approach to examine and improve cybersecurity governance for small airports in India, integrating policy analysis, international benchmarkings, and real-world case studies to understand more about the cybersecurity attacks. Thus, the methodology is designed to ensure a comprehensive and practical understanding of the challenges and solutions in this sector.

### 4.1 Policy and Document Analysis

A foundational step in this research involved a systematic review of key national and state-level policy documents relevant to aviation and cybersecurity. This included the National Cyber Security Policy 2013 (Meity, 2013), Civil Aviation Promotion Policy of Uttar Pradesh 2017 (Invest UP, 2017), and operational guidelines from CERT-In (Cert-in, 2025). Document analysis allowed the identification of existing gaps, overlaps, and inconsistencies in current policy frameworks affecting small airports. This qualitative approach is widely recognized for its ability to extract nuanced insights from official texts and is particularly useful in governance studies where policy context shapes practical outcomes.

### 4.2 Review of International Cybersecurity Frameworks

The review of international cybersecurity frameworks in this study included the NIST Cybersecurity Framework CSF (Mohammed, K., 2023), ISO/IEC 27001 (Masike M., 2023), and the ICAO Cybersecurity Strategy in the U.S (ICAO, 2024). These frameworks were chosen because each is globally recognized, widely adopted, and specifically designed to address the unique cybersecurity risks and regulatory needs of critical infrastructure sectors like aviation. They offer structured, risk-based approaches, promote operational resilience, and support compliance with both national and international requirements, making them ideal benchmarks for small airport cybersecurity governance

### 4.3 Case Studies

We conducted case-study analyses of notable cybersecurity incidents involving airports, with a focus on smaller or regional airports where possible. The cases examined included the Albany International Airport ransomware attack (2019) in the US (Cybersecurity Insiders, 2019), the hack of Vietnam's Hanoi and Ho Chi Minh airports (Forbes, 2016), and several other less publicized breaches or disruptions such as periodic DDoS attacks on airport websites, and the Cleveland Hopkins Airport malware incident in 2019 (News5 Cleveland, 2019). Each case study was analyzed to understand how the attack occurred, what governance or preparedness gaps it revealed, and how the airport and authorities responded. These real-world examples grounded our understanding of threat impact and the efficacy of existing governance measures. We also briefly noted any known incidents in India's aviation sector for instance, the 2021 data breach of Air India's passenger system (Forbes, 2021).

#### *4.3.1 Albany International Airport (USA), 2019*

On Christmas Day 2019, Albany International Airport in New York was hit by a ransomware attack that encrypted its administrative servers and backup systems (Cybersecurity Insiders, 2019). The attackers gained access through LogicalNet, the airport's outsourced IT provider, and spread the Sodinokibi ransomware throughout the network. As a result, important documents like archives and HR records were locked, though no passenger or airline data was affected. The airport had no usable backups and ultimately paid a ransom to regain access, with insurance covering most of the cost. Operations for travelers were not disrupted, but the incident exposed major risks in relying on third-party IT vendors and lacking internal cybersecurity controls. After the attack, the airport ended its contract with LogicalNet and improved its internal systems. This study helps examine the importance of strong vendor oversight and having robust backup and recovery plans to mitigate these attacks in small airports.

#### *4.3.2 Vietnam airports hack, 2016*

On July 29, 2016, hackers believed to be from China attacked Vietnam's two airports, Hanoi and Ho Chi Minh, as well as the national airline's website. The attackers took over flight information screens and public address systems, posting political messages about the South China Sea dispute and causing confusion among thousands of passengers. The check-in systems were also hit, forcing staff to switch to manual processing and resulting in delays for nearly 100 flights. In addition, the hackers stole and leaked personal data of over 400,000 frequent flyer members. This event highlighted the geopolitical risks and propagandas these airports might face and the urgent need for strong incident response plans and cyber resilience, especially against politically motivated attacks (Forbes, 2016).

#### *4.3.3 Cleveland Hopkins Airport (USA), 2019*

In April 2019, Cleveland Hopkins International Airport experienced a ransomware attack that disrupted its baggage and flight information displays as well as its email systems. For almost a week, the airport's digital screens went dark and staff had to rely on manual processes to keep passengers informed. While city officials initially downplayed the incident, the FBI later confirmed the presence of ransomware on the airport's network. Importantly, no flight operations or safety systems were affected, and there were no ransom demands. The airport worked with federal authorities to investigate and recover from the attack. This case shows the importance of transparency, quick response, and having backup communication systems in place (News5 Cleveland, 2019).

#### *4.3.4 Air India data breach (India), 2021*

In 2021, Air India announced a major data breach after hackers compromised the airline's passenger service system, which was managed by the third-party vendor SITA. The breach affected about 4.5 million passengers, exposing sensitive information such as names, passport numbers, ticket details, and frequent flyer data. While

credit card CVV numbers were not leaked, the incident raised concerns about the security of personal data in the aviation sector. Air India was not the only airline affected, as the breach impacted several global carriers using SITA's systems. This breach highlighted the aviation industry's vulnerability to supply chain attacks and the need for stronger data protection and vendor risk management (Forbes, 2021).

### 4.4 Comparative Analysis

Finally, a comparative analysis between Indian practices and international practices. This involved juxtaposing our findings on Indian governance gaps with the measures taken in other jurisdictions. For instance, India's lack of a clear incident reporting mechanism for airports with the EU's requirement that aviation OES (Operators of Essential Services) report significant incidents within 72 hours to authorities. We also compared institutional arrangements: whereas India does not yet have an aviation-specific cybersecurity unit, countries like the UK have the Civil Aviation Authority working jointly with the national cybersecurity center to oversee aviation cyber resilience. These comparisons helped highlight areas where India could learn from or adapt successful models used elsewhere, while also noting differences in context

## 5. Policy Recommendations

To address the identified gaps, this section outlines a series of policy recommendations aimed at building a strong and context-aware cybersecurity governance structure for India's small airports. These proposals focus on enhancing localization, promoting efficient resource use, and fostering collaboration across stakeholders.

### 5.1 Localized Cybersecurity Frameworks

India's national cybersecurity ecosystem includes several structured frameworks that are designed to safeguard critical digital infrastructure. Notable among these are the ISO/IEC 27001 standard (Masike M., 2023), the NIST Cybersecurity Framework (Mohammed, K., 2023), the National Cyber Security Policy 2013 (Meity, 2013), and the ICAO Cybersecurity Strategy for the aviation sector (ICAO, 2024). While each offers valuable guidance, this study would focus on two prominent key Indian frameworks the CERT-In Guidelines for Critical Infrastructure and the NCIIPC Framework given their prominence in government policy and relevance to civil infrastructure.

#### *5.1.1 Limitations of CERT-In and NCIIPC for small airports*

The CERT-In, 2025 guidelines, issued by the Ministry of Electronics and Information Technology, require airports to comply with a strict set of controls, such as reporting cyber incidents within six hours, maintaining security logs for 180 days, and conducting regular vulnerability assessments. These measures assume the presence of mature IT infrastructure and a dedicated cybersecurity workforce. However, most small airports operate with minimal technical staff, rely on outsourced IT support, and lack the tools needed to implement or monitor these controls effectively. Thus, the compliance burden imposed by CERT-In (Cert-in, 2025), while justified for large entities, often exceeds the operational capabilities of smaller airports and their day to day operations.

Secondly, the NCIIPC framework emphasizes the protection of critical information infrastructure through asset classification, continuous monitoring, threat intelligence sharing, and incident response readiness. It is typically applied to high-impact sectors such as banking, energy, and major transportation hubs. While aviation could fall under this industry. Although, small airports are rarely categorized as critical unless they serve defense or high-security functions. Moreover, the framework presumes a level of cyber maturity that includes in-house Security Operations Centers (SOCs), tiered governance, and technical redundancy. These resources are far beyond what a small airport can realistically maintain.

#### *5.1.2 Public Sector Innovation (PSI)*

While not a cybersecurity standard itself, the Public Sector Innovation (PSI) framework, as conceptualized by the OECD Observatory of Public Sector Innovation (OECD-OPSI, 2024), offers a flexible governance lens focused on collaborative decision-making, iterative learning, and adaptation in resource-constrained settings. In the aviation context, PSI can help bridge the gap between top-down cybersecurity mandates and the operational realities of small airports by supporting the localized, pragmatic implementation of more structured standards like NIST or ISO 27001. PSI emphasizes collaborative governance, iterative learning, and innovation in resource-constrained settings. In the context of aviation, it can be used to support the localized implementation of more structured standards by aligning them with ground realities at small airports.

Compared to more rigid compliance-oriented frameworks, PSI emphasizes responsiveness to local needs and fragmented institutional environments, which are conditions that typify many small airports in India. While risk

management frameworks such as NIST CSF or COBIT provide robust technical guidance, they often assume the presence of dedicated cybersecurity personnel, advanced infrastructure, and clear lines of accountability assumptions that do not always hold in decentralized or under-resourced airport settings.

Public Sector Innovation (PSI) has been successfully employed in various policy and infrastructure domains characterized by resource constraints, fragmented governance, and the need for locally tailored solutions. For example, during India's Smart Cities Mission, urban local bodies were empowered to develop city-specific digital infrastructure using approaches such as co-creation with stakeholders, iterative experimentation, and decentralized decision-making. Similarly, during the COVID-19 pandemic, countries like Estonia and India leveraged PSI principles to rapidly adapt digital health and vaccination systems to local capacities, despite differing infrastructure levels across regions (OECD-OPSI, 2024; World Bank, 2021).

These examples help build a solid foundation and provide a clearer understanding of the challenges faced by India's small airports such as limited technical expertise, budgetary constraints, operational heterogeneity, and the need for coordination among multiple agencies.

#### *5.1.3 Policy innovation*

Policy innovation within the PSI framework means creating cybersecurity policies that are forward-looking and tailored to the specific needs and risks of small airports. Instead of applying a one-size-fits-all approach, policies should be flexible enough to address emerging threats like AI-driven or drone-enabled attacks. For example, a state-level cybersecurity charter could set minimum security standards, but allow each airport to adapt how they meet those standards based on their local resources and challenges. Regularly updating these policies is critical to ensure they keep pace with technological changes and evolving threats (Georgia et al., 2018). These adaptive policies are especially important as small airports often operate with older systems and less robust cybersecurity defenses, making them attractive targets for cybercriminals. By focusing on context-sensitive and regularly updated policies, small airports can build resilience and better protect their operations and passengers.

#### *5.1.4 Institutional innovation*

Institutional innovation involves creating or reforming governance structures to clarify who is responsible for cybersecurity. For small airports, this could mean establishing dedicated cybersecurity teams or integrating cybersecurity oversight into existing operational bodies. Research shows that clear roles and accountability are essential for effective cybersecurity management, particularly in environments where resources are limited and staff often wear multiple hats (Georgia et al., 2018). Having well-defined governance structures helps ensure that critical cybersecurity tasks-like monitoring threats, responding to incidents, and training staff-are not overlooked. This is important because fragmented responsibilities can lead to gaps in security, making it easier for attackers to exploit weaknesses.

#### *5.1.5 Collaborative governance*

Collaborative governance is a key principle of PSI, advocating for structured cooperation among regulators, airport operators, technology vendors, law enforcement, and academic experts. Sharing threat intelligence and best practices across these groups enhances collective defense capabilities and helps everyone stay ahead of new threats. International organizations such as the International Civil Aviation Organization (ICAO) and industry platforms like Aviation-ISAC play a crucial role in facilitating this collaboration by providing guidance, sharing information, and supporting capacity building (ICAO, 2024). This multi-stakeholder approach is vital because no single organization can address all the cybersecurity challenges facing the aviation sector. By working together, stakeholders can develop more effective solutions and respond more quickly to incidents (Atlantic Council, 2019).

#### *5.1.6 Adaptive regulation*

Adaptive regulation means moving away from rigid checklists and instead focusing on performance-based standards that can change as needed. For example, regulations can be tiered so that smaller airports have different requirements than large international hubs, and regulatory sandboxes can be used to safely test new technologies before full-scale deployment. This flexibility allows small airports to innovate and improve their cybersecurity without being overwhelmed by unrealistic compliance demands (Atlantic Council, 2019). This ensures that operations are going hand in hand while taking the cybersecurity of small airports into consideration.

### 5.2 Dedicated Cybersecurity Cells and Roles

Small airports often lack specialized teams to handle cybersecurity, making them more vulnerable to attacks. To address this, each airport should appoint a dedicated Cybersecurity Officer or form a small cybersecurity cell, either individually or by pooling resources with nearby airports. These officers or teams would be responsible for conducting regular risk assessments, monitoring for threats, and leading the response during a cyber incident. For greater efficiency, a centralized Security Operations Center (SOC) managed by the Airports Authority of India (AAI) or state governments can oversee and support multiple airports at once (PwC, 2024). This approach ensures that even airports with limited budgets have access to expert monitoring and quick response capabilities. Mandating these roles through national policy, similar to the TSA's requirements in the United States, creates clear accountability and helps prevent gaps in security coverage.

### 5.3 Cross-Sector Coordination Mechanisms

Cybersecurity in airports is not just an IT issue-it requires teamwork across many sectors. Airports should set up formal coordination between aviation management, IT departments, law enforcement, CERT-In (Cert-in, 2025), and emergency services. A national Aviation Cybersecurity Committee can provide overall strategy and guidance, while regional teams handle day-to-day incidents and practice regular drills. Joining international platforms like Aviation-ISAC allows Indian airports to share and receive threat intelligence from airports worldwide, making it easier to stay ahead of new threats. Domestically, CERT-In (Cert-in, 2025) can manage a secure alert system for rapid communication during cyber incidents. This kind of structured, cross-sector collaboration is proven to improve response times and reduce the impact of attacks, as highlighted by ICAO (ICAO, 2024) and industry studies.

### 5.4 Capacity Building and Training Programs

People are a key line of defense against cyber threats, so regular training is essential. Airports should launch role-specific cybersecurity training for IT staff, airport managers, and frontline employees, ensuring everyone understands their part in keeping systems secure. Training should include practical exercises like cyber drills, simulated phishing attacks, and response to outages to ensure that staff know what to do in real situations. Scholarships and exchange programs can help smaller airports learn from larger, more experienced ones, building a pipeline of skilled cybersecurity professionals. Research shows that ongoing education and awareness programs are critical for building resilience and reducing the risk of successful attacks (ACI World, 2024; ICAO, 2024; Georgia et al., 2018).

## 6. Strategy

A phased strategy ensures that small airports can systematically build their cybersecurity capabilities, starting from basic risk identification to ongoing improvement. Each phase is designed to be practical, scalable, and aligned with international best practices like the NIST Cybersecurity Framework and ICAO Cybersecurity Strategy (ICAO, 2024; Mohammed, K., 2023). Below, each phase is described in simple language, with suggested timelines for implementation.

### 6.1 Phase 1: Assessment and Planning

The first step is to understand what needs protection. Airports should conduct a thorough audit of all their IT and operational systems, including hardware, software, and data assets. This involves identifying key vulnerabilities, mapping out current risks, and evaluating how existing processes and staff roles contribute to cybersecurity. At this stage, airport management should also set up a dedicated cybersecurity governance structure, such as appointing a Cybersecurity Officer or forming a small cybersecurity cell. This phase creates a clear baseline for future improvements and ensures everyone knows their responsibilities from the start.

### 6.2 Phase 2: Policy Implementation and Capacity Building

Once the risks and needs are identified, the next phase is to put rules and training in place. Airports should develop or update cybersecurity policies, covering areas like network segmentation, access controls, and incident response. These policies should be flexible enough to adapt to new threats and technologies. Simultaneously, airports must launch targeted training programs for all staff, from IT teams to frontline workers, so everyone understands basic cyber hygiene and what to do during an incident. Establishing regional or centralized Security Operations Centers (SOCs) can help smaller airports share resources and expertise. This phase also includes setting up communication channels with law enforcement and national agencies for coordinated response.

### 6.3 Phase 3: Technology Deployment and Pilot Program

With policies and training in place, the focus shifts to upgrading technology and testing solutions. Airports should roll out modern cybersecurity tools, such as firewalls, intrusion detection systems, and backup solutions, prioritizing the most critical systems first. Pilot programs can be launched at select airports to test new technologies and procedures in real-world conditions. Lessons learned from these pilots should be used to refine the approach before scaling up to all airports. This phase also includes regular cyber drills and exercises to ensure readiness and fine-tune incident response plans

### 6.4 Phase 4: Evaluation, Feedback, and Continuous Improvement

Cybersecurity is not a one-time project but an ongoing effort. Airports should schedule regular independent audits and reviews to assess the effectiveness of their cybersecurity measures. Feedback from staff and incident reports should be used to update policies, improve training, and invest in new technologies as threats evolve. Sharing best practices and lessons learned across airports helps raise the overall standard and keeps everyone aligned with national and international requirements. This phase ensures that the cybersecurity program remains effective and resilient in a changing threat landscape

## 7. Discussion

### 7.1 Benefits

Implementing the proposed Public Sector Innovation (PSI) framework offers small airports a structured yet flexible approach to cybersecurity governance. By fostering collaboration between regulators, airport operators, and technology vendors, PSI ensures that policies adapt to evolving threats like AI-driven attacks or third-party vulnerabilities, as seen in the Albany Airport ransomware case. This model also promotes resource efficiency-critical for budget-constrained airports-by enabling shared Security Operations Centers (SOCs) and regional cybersecurity cells. Aligning with global standards like NIST, ICAO (Mohammed, K., 2023; ICAO, 2024) ensures compliance while allowing localized customization, such as tiered regulations for differently sized airports. Over time, this approach builds institutional expertise, reduces human error through targeted training, and strengthens trust in India's aviation infrastructure (ICAO, 2024).

### 7.2 Challenges

Airport cybersecurity spans IT (data systems), OT (physical operations), and IO (public-facing services). Each presents distinct risks from outdated IT infrastructure to fragmented OT oversight and vulnerable communication channels. The PSI framework can help address these through innovation in technology, organization, and policy. But resource gaps, regulatory overlap, and limited data access complicate implementation. Effective PSI adoption must recognize how these domains interact within India's aviation context.

Despite its advantages, implementing PSI faces significant hurdles. Small airports often lack funds for advanced tools or dedicated staff, forcing reliance on outdated systems vulnerable to attacks like the 2016 Vietnam airport hack (Forbes, 2016). Rapidly evolving threats–such as ransomware targeting IoT devices–outpace policy updates, creating gaps even in proactive frameworks. Regulatory complexity further complicates efforts: overlapping mandates from agencies like DGCA, CERT-In, and state governments can confuse accountability, delaying incident responses (Cert-in, 2025). Additionally, coordinating cross-sector stakeholders like different airlines and various IT vendors remains difficult, as seen in the fragmented response to the Air India data breach (Forbes, 2021). Finally, resistance to change in bureaucratic systems and dependence on third-party vendors introduce persistent risks, requiring ongoing vigilance (Aliyu et al., 2022; Schafer, 2022).

### 7.3 Limitations

First, limited access to detailed incident data from Indian airports, due to privacy concerns or underreporting, restricts the depth of empirical analysis. Second, cybersecurity recommendations are based on current threats, but the rapid adoption of technologies like AI and quantum computing may soon render some strategies obsolete. Third, the PSI framework's success depends on sustained political will and funding, which can vary across states or administrations. Finally, while international case studies e.g., Bristol Airport (BBC, 2018) provide insights, India's unique governance landscape may require adjustments to borrowed models. Despite these constraints, the research offers a foundational roadmap for policymakers to balance innovation and security in small airports (Future Airport, 2024).

## 8. Conclusion

As India's aviation ecosystem expands to connect every corner of the nation, the digitalization of small airports must be matched by equally robust cybersecurity governance. The stakes are high: these emerging airports are not only gateways for millions of new passengers but also nodes in a critical infrastructure network that underpins economic activity and public safety. Through the lens of Public Sector Innovation, this paper has advocated for a multi-stakeholder, context-sensitive approach to developing cybersecurity policy and governance for India's small airports.

## References

ACI World. (2024) 'Cybersecurity for Airport Managers', ACI World.

Aliyu, A., Adamu, M., Musa, A., & Haruna, M. (2022) 'Cyber-security challenges in aviation industry: A review of current trends'. Available at: https://www.mdpi.com/2078-2489/13/3/146

Atlantic Council. (2019) 'Aviation Cybersecurity: Scoping the Challenge', Atlantic Council.

BBC. (2018) 'Cyber attack led to Bristol Airport blank screens', BBC.

Cert-in. (2025) 'Guidelines on Information Security Practices for Government Entities', Cert-in.

Chandrashekhar, I. K., & Nivea, T. (2019) 'A Critical Review on Regional Connectivity Scheme of India'. Available at: https://www.sciencedirect.com/science/article/pii/S2352146520304178

Choudhary, N., Nour, M., Francesco, S., Praveen, G., & Helge, J. (2020) 'A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports'. Available At: https://ieeexplore.ieee.org/abstract/document/9252856/citations?tabFilter=papers#citations

Civil Aviation. (2024) 'Annual Report 2024', Civil Aviation.

Cyfirma. (2024) 'The Changing Cyber Threat Landscape asia-pacific (APAC) Region - Volume 1', Cyfirma.

Cybersecurity Insiders. (2019) 'Ransomware Attack on Albany Airport on Christmas 2019', Cybersecurity Insider.

Elochukwu, U., Mohamed Amine Ben, F., Hanan, H., Miroslav, B., Robert, A., Christos, T., & Xavier, B. (2021) 'Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends'. Available At: https://arxiv.org/abs/2107.04910

ENISA. (2016) 'Securing Smart Airports', ENISA.

Eurocontrol. (2021) 'Aviation under attack from a wave of cybercrime', Eurocontrol.

Forbes. (2016) 'Hacking Attack At Vietnam Airports Another Chapter In South China Sea Dispute', Forbes.

Forbes. (2021) 'Air India Data Breach: Hackers Access Personal Details Of 4.5 Million Customers', Forbes.

Georgia, L., Argiro, A., & Dimitris, G. (2018) 'Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience'. International Journal of Environmental Research and Public Health. Available At: https://pmc.ncbi.nlm.nih.gov/articles/PMC6339064/

GOI. (2024) 'India's Soaring Skies with Inclusive and Booming Aviation', GOI.

ICAO. (2024) 'Aviation Cybersecurity', ICAO.

Indiacode. (2000) 'Information Technology Act, 2000', Indiacode.

Invest UP. (2017) 'Uttar Pradesh Civil Aviation Promotion Policy 2017', Invest UP.

Invest UP. (2023) 'Civil Aviation Sector', Invest UP.

Masike, M. (2023) 'Management of enterprise cyber security: A review of ISO/IEC 27001:2022'. Available At: https://ieeexplore.ieee.org/abstract/document/10051114

Meity (Ministry of Electronics and Information Technology). (2013) 'National Cyber Security Policy -2013', Meity.

Mohammed, K. (2023) 'NIST Cybersecurity Framework'. Available At: https://jsaer.com/download/vol-10-iss-8-2023/JSAER2023-10-8-150-157.pdf

Nasscom. (2023) 'Enhancing Cybersecurity at Indian Aviation', Nasscom.

News5 Cleveland. (2019) 'Cleveland Hopkins Airport recovers from computer malware attack; FBI investigates, News5 Cleveland'.

OECD-OPSI. (2024) 'Building Anticipatory Capacity in Governments: Reflections and resources from project LIMinal's closing event', OECD-OPSI.

PwC. (2024) 'Tracing the rise of GCCs in India as cybersecurity powerhouses', PwC.

Romy, J., & Saurabh, T. (2024) 'The Role of Small Airports in the Distribution and Logistics of Local Produce in India: A Proposal for Business Efficiency'. Available At: https://koreascience.kr/article/JAKO202417743214402.page#ref-1

Schafer, J. (2022) 'Cyber Threats to the U.S. Aviation Industry: A Review of Recent Incidents and Emerging Risks'. Journal of Homeland and National Security Perspectives. Available At: https://hnspjournal.org/wp-content/uploads/2023/01/jhnsp-7.1-final-draft-cyber-threats-us-aviation-schafer-january-2023-3.pdf

The Record. (2024) 'Port of Seattle says 90,000 people impacted in 2024 ransomware attack', The Record.

World Bank. (2021) 'Digital Platforms for covid-19 Vaccination Delivery', World Bank.