Center for Management Science Research
ISSN: 3006-5291 3006-5283 Volume 4, Issue 3, 2026

FORTIFYING AVIATION SUPPLY CHAINS IN THE DIGITAL ERA: AN INTEGRATED CYBERSECURITY RISK ASSESSMENT AND STRATEGIC MITIGATION FRAMEWORK FOR PAKISTAN'S AVIATION ECOSYSTEM

Engr. Ghulam Murtaza*[1], Mashal Tariq[2], Maria Hina[3], Jamila Kasi[4]

DOI: https://doi.org/10.5281/zenodo.18953881

Keywords
Aviation Supply Chains; Cybersecurity Risk Assessment; Digital transformation; Critical infrastructure protection; Supply Chain Resilience; Regulatory preparedness; Vendor Governance; Pakistan Aviation sector; Cyber-physical systems; Risk Mitigation Framework.

Article History
Received: 11 January 2026
Accepted: 23 February 2026
Published: 11 March 2026

Corresponding Author: *
Engr. Ghulam Murtaza

Abstract

The high-paced digitalization of air supply chains has transformed the efficiency in operation, coordination and real-time visibility in the chain of stake (airlines, airports, maintenance providers, logistics operators and technology vendors). Nevertheless, an escalation of dependent existence on linked online frameworks has also presented a bigger cyber-attack area of the aviation ecosystem, particularly in developing economies where cybersecurity frameworks in control and organizations are still not fully established. The research focuses on the dynamics of the aviation industry cybersecurity risk in Pakistan and develops an integrated and holistic structure of the risk assessment and mitigation strategic perspective. The research is based on a sequential explanatory mixed-method design which entails the synthesis of both quantitative research findings based on survey research of 150 aviation professionals and the results of qualitative research in which 12 semi structured interviews are used. The association between digitalization, organizational cybersecurity maturity, regulatory preparedness, vendor governance, cybersecurity vulnerabilities and supply chain resiliency were analyzed by using multiple regression and moderation analysis. This is because the findings indicate that digitalization has a significant role to play in these cybersecurity risks and the level of cybersecurity maturity of an organization significantly reduces the threats of cybersecurity exposure. Moderating the relationships between digitalization and vulnerabilities, regulatory preparedness and moderating the negative resiliency contribution to vulnerabilities, vendor governance respectively, digitalization and vulnerabilities. Through empirical evidence, the study advanced the six-layer integrated Cybersecurity Risk Assessment and Strategic Mitigation Framework and proposed that it involves the following: risk identification, risk prioritization, technical controls, organizational governance, regulatory and vendor oversight, and continuous improvement mechanisms. The framework includes a context-dependent roadmap which is particular to the aviation ecosystem of Pakistan but is wider in terms of its application in other past aviation markets as well. This study contributes to the literature of digital supply chain risk theory, critical infrastructure resilience literature and literature on cybersecurity governance since it demonstrates that the resilience of aviation cybersecurity is a multi-layered governance-alignment issue as opposed to a technical control issue. The findings serve useful recommendations to the stakeholders of the aviation industry and the concerned policymakers about the need to enhance the supply chains in the digitalized world.

2. INTRODUCTION

2.1 Background

Aviation industry is rated among the most significant strategic sectors of the global economy with a key role played as an enabler of international trade and economic integration, mobility and national security. In this industry, the aviation supply chain is in the provision of powering operational backbones that ensure the continuance of operations of airlines, airport authorities, maintenance repair and overhaul (MRO) services, and logistics operators, ground handlers, and technology vendors. The aviation supply chains unlike the traditional linear chains are closely linked institutions, which are safety-sensitive and highly time-sensitive systems where a disaster will rapidly propagate across a wide spectrum of consumers. Over the last several years, the establishment of digital, fast moving, and networked flight operations in the entire aviation supply chain (via cloud-based logistics platforms, Internet of Things (IoT)-based trackers, automated maintenance management systems and enterprise resource planning (ERP) integration) have changed the operational efficiency, visibility, and coordination [1].

The digital technologies have previously involved predictive maintenance of airplane parts, real-time in-flight cargo, electronic documentation system, automatic procurement and real- time communication between supply chain partners. One thing is that digital interconnectedness that adds efficiency exposes the cyber-attack surface, however. Since the aviation ecosystem is now more reliant on networked systems, ransomware attacks, phishing campaigns, IoT hacks, data breaches, and supply chain intrusions can now target them [2]. Cyber intrusions do not only result in information loss but in cyber-physical infrastructure like in the aviation sector, they can directly impact on operational continuity, fly-safety, cargo integrity, and national security interests.

Cyber risk is another issue that is augmented by the complexity of the supply chains of aviation. Various stakeholders including airlines, airport management, MRO, logistics and IT vendors are operating with varying degrees of cybersecurity maturity on interdependent digital platforms. A vulnerability on a single node, particularly third-party vendor vulnerabilities, can provide adversaries with a lateral movement i.e. movement on one system to other in that organization and compromise on the mission critical operations. Empirical analysis of supply chain security to date indicates that cyber attackers are highly likely to target nodes that are much weaker than the highly fortified core systems and to attack them directly, in a system that is interconnected [3]. It is an even more concerning phenomenon in the rising economies, where the digital transformation progresses faster than the regulatory governance and institutionalization of cybersecurity.

In terms of Pakistan, the aviation industry is so much transformed in the recent years both digitally. Large airports, airlines, and logistics service providers have changed to digital cargo management platforms, electronic maintenance logs, IoT-based tracking rules, and a cloud- based coordination tool. The operations are performing better and being more transparent, however, along with these advances, there has been no equivalent investment in cybersecurity governance, regulation enforcement, or organizational maturity [4]. The broader cybersecurity ecosystem around Pakistan, however, can be described as disordered institutional directives, absence of sector-specific policies and sufficient technical capability of major infrastructure sectors [5]. This means that despite their aviation supply chains also getting more digitized, they are structurally weak in Pakistan.

The entire world experience promotes the need to fight these weak points. The scale of such high-profile cyber incidents impacting critical infrastructure (such as ransomware attacks of logistics systems, and other software hacks into supply chains) has demonstrated the scale to which so-called domino effect disruptions of interconnection systems may be disrupted [6]. Even though the aviation cyber incidents that are catastrophic have not been reported publicly in Pakistan, the absence of mandatory reporting systems and sharing of threat intelligence across the sector may be used to cover up the latent vulnerabilities. Because of this, the necessity to enhance cybersecurity in aviation supply chains is more than a technical imperative, but a national security imperative to enhance economic resilience.

The conceptualization of this challenge needs to begin with the understanding of the aviation supply chains as cyber-physical ecosystems where digital systems, organizational processes, vendor relations, and regulatory regimes are interacting dynamically. Cybersecurity cannot hence be addressed only with technical controls but requires a comprehensive governance model that encompasses risk identification, organizational maturity, vendor controls and alignment with the regulating authorities. An example of how the aviation supply chain ecosystem is structured is illustrated in Figure 1 in terms of interdependencies among the multi- stakeholders and its digital interfaces.

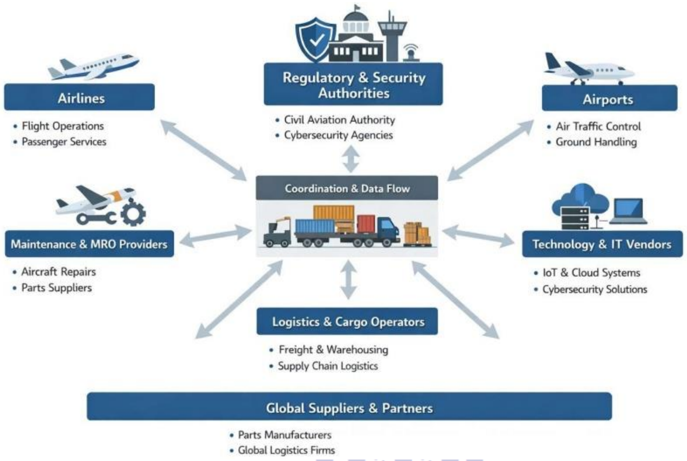

Figure 1: Structure of the Aviation Supply Chain Ecosystem

Nevertheless, the aviation cybersecurity in Pakistan does not possess a synchronized and contextualized governance of the supply chains. The adoption of digital by various parties in the supply chain and logistics sector including airlines, airports, logistics, and maintenance firms have enhanced an increasing reliance on interconnected systems, but cybersecurity maturity and readiness to regulate is skewed and disjointed as are vendor governance processes. Cybercrime is also addressed in general by the existing laws of the country on cybersecurity, such as the Prevention of Electronic Crimes Act (PECA) 2016, without addressing the cybersecurity requirements of the aviation sector or mandating audit frameworks or standardized incident reporting frameworks [7].

Most aviation stakeholders possess partial cybersecurity controls at the organizational level (such as firewalls and antivirus solutions with limited or absent monitoring capabilities, organized systems to assess risks and very little or no cybersecurity governance teams, etc). The example of vendor-specific systems, in particular, third-party logistics software and maintenance management systems, creates an added exposure since it is in that case that there may not be a consistency of the internationally perceived standards [8]. As a consequence, this makes this shaky cybersecurity dilemma systemic in the supply chain ecosystem.

In addition, digitalization has intricate power of risk. As much as the capabilities to perform that are induced by automation and also by IoT tracking and cloud based operations, the same presents renderable the access points that the adversary can enter. Organizations risk becoming involuntarily exposed to a more operation by setting up unsecure digital growth, in the absence of risk-based prioritization and risk-based mitigation frameworks. It is also enhanced by the fact that a harmonized approach to cyber security does not exist among the supply chain actors, which contributes to the risk of cascades.

Therefore, there is a kind of a paradox in the situation of the aviation supply chains of Pakistan: the digital integration has provided improved efficiency and simultaneously brought about greater cyber-vulnerability to them in a poorly-developed regulatory and institutional framework. The absence of the empirically based and aviation-specific model of cybersecurity risks evaluation and mitigation framework appropriate to the reality of Pakistan operations is a striking void. In the absence of such a framework, vulnerabilities can persist and be a threat to the continuity of operation, economic stability interests, and national security.

The study does have a number of contributions to the literature and practice of cybersecurity in the aviation supply chains. First, it builds up on the scholarship literature by introducing empirical data in a context of an emerging economy where digital transformation processes are already underway making incursence of wholly institutionalized cybersecurity governance. A significant part of the current literature is dedicated to technologically advanced jurisdictions; this study gives some information concerning the structural issues of emerging aviation ecosystems [9].

Second, the study will be an empirical test that will construct and evidence a multi-variable conceptual model to develop a relationship between digitalization, maturity of organizational cyber security, vendor governance, regulatory preparedness, vulnerabilities, and supply chain resilience. The paper brings together the mediating and moderating relationships to contribute to the advancement of theories about the relationship between technological expansion and methods of government structures in which the outcomes of cybersecurity are mediated.

Thirdly and most crucially the research is making a suggestion of a six-layered integrated Cybersecurity Risk Assessment and Strategic Mitigation Framework, which is specifically proposed to the Aviation Supply Chain Ecosystem of Pakistan. In comparison to generic frameworks on cybersecurity, the given model also considers the situational reality, including their dependency on vendors, outdated infrastructure, fragmentation of regulations, and capacity limits, which makes them more practical. **Table 1** summarizes the key dimensions of digital technologies adopted in aviation supply chains and their associated cybersecurity risks.

Table1: Digital Technologies and Associated Cyber Risks in Aviation Supply Chains

Digital Technology	Operational Function	Associated Cyber Risk
IoT-based tracking devices	Real-time cargo and component tracking	Device exploitation, spoofing, lateral network movement
Cloud-based maintenance systems	Electronic aircraft maintenance logs	Data breaches, misconfiguration vulnerabilities
ERP&SCM systems	Procurement and logistics coordination	Ransomware, credential compromise
Automated logistics platforms	Scheduling and routing optimization	Supply chain in filtration attacks
Vendor-integrated software	Third-party service integration	Malicious software updates, weak authentication

Taken together, the introduction establishes the urgency of securitizing the aviation supply chains against cyber threat in the digital realm. It incorporates cybersecurity not only as a technical problem but as a governance problem as a system that needs a systemic organizational, regulatory and technological response. The subsequent parts of this paper are based on this model to empirically explore cybersecurity risk dynamics and come up with a holistic cybersecurity risk reduction model in the context of the Pakistani aviation ecosystem.

3. Literature Review and Theoretical Foundations

3.1 Aviation Supply Chains as Cyber-Physical Systems

The aviation supply-chainsare considered to be one of the most intricate and significant safety-critical supply chain set-ups globally. The aviation supply chains also introduce digital systems that deal directly with functional and operational safety, unlike the more common industrial supply chains that regulate the flow of material and information mainly. There is a group of airlines, airport operators, maintenance repair and overhaul (MRO) vendors, logistics vendors, ground handlers, and aviation IT vendors in a highly-close knit ecosystem where real-time coordination is essential to guarantee an operating continuity. This integration is rendering supply chains in the aviation industry into cyber-physical systems, that is, the digital infrastructures are becoming nonseparable to the physical flight operations, cargo flow and maintenance operations [10].

The digital networks can be disrupted in the operating-safety and reliability of the cyber-physical networks in real-time. To illustrate, the hacked maintenance databases might slow the logistics planning and aircraft maintenance processes, the cargo tracking systems pitch forked could disorganize the logistics planning, vendor systems that were hacked might leak the sensitive data of the operations process. The complexity of the aviation supply chains implies that the vulnerabilities are not confined solely to any specific organizations, as it can be propagated throughout the ecosystem. According to literature on critical infrastructure resilience, highly coupled systems become even more susceptible to causal failures unless digital interdependences are ensured adequately [11].

Aviation is also a unique industry owing to the safety standards and the interdependence of regulations in the world. The digital platform of aircraft maintenance, time scheduling of planes, and cargo management cannot allow any error to pass through that the tolerance margin is almost zero. This means that cybersecurity of supply chains in the aviation sector needs to be re-conceptualized outside of the traditional notion of IT risk management; it needs to encompass not only the operational technology (OT) or embedded systems but also sensors and cloud-based coordination platforms that use IoT. Control in threat modeling and risk governance is more complex because of this multi-layer integration.

A supply chain perspective in aviation is a networked ecology and characterized by inter-organizational trust, exchange of data and digital dependency. Integration in vendor systems with airline systems or airport systems is often done by application programming interfaces (APIs) and by the use of shared databases. This type of integration encourages efficiency but puts in place additional exposure points. Empirical research indicates that cross-system supply chain between adversaries are frequently employed to bypass robust perimeter security in fundamental frameworks [12]. Thus, cybersecurity governance must not be applied to specific organizations alone but the entire supply chain architecture.

In other emerging economies such as Pakistan, where digital transformation has gone on without the relevant institutional fortification, the degree of technology maturity of aviation supply chains appears to be in a state of heterogeneity. The bigger airlines could be more advanced on the digital front: their platforms could be more detailed and sophisticated whereas smaller logistics operators could be having partially digitized or more old-fashioned systems. This inequality implies that there is greater systemic risk available because there is always a possibility of the enemies attacking weaker nodes before they can infiltrate the interdependent networks. The perception of aviation supply chains as cyber-physical systems thus provides a platform of vulnerability and resilience of cybersecurity and its results. Figure 2 illustrates the interdependent cyber-physical structure of aviation supply chains and the digital interfaces connecting stakeholders.

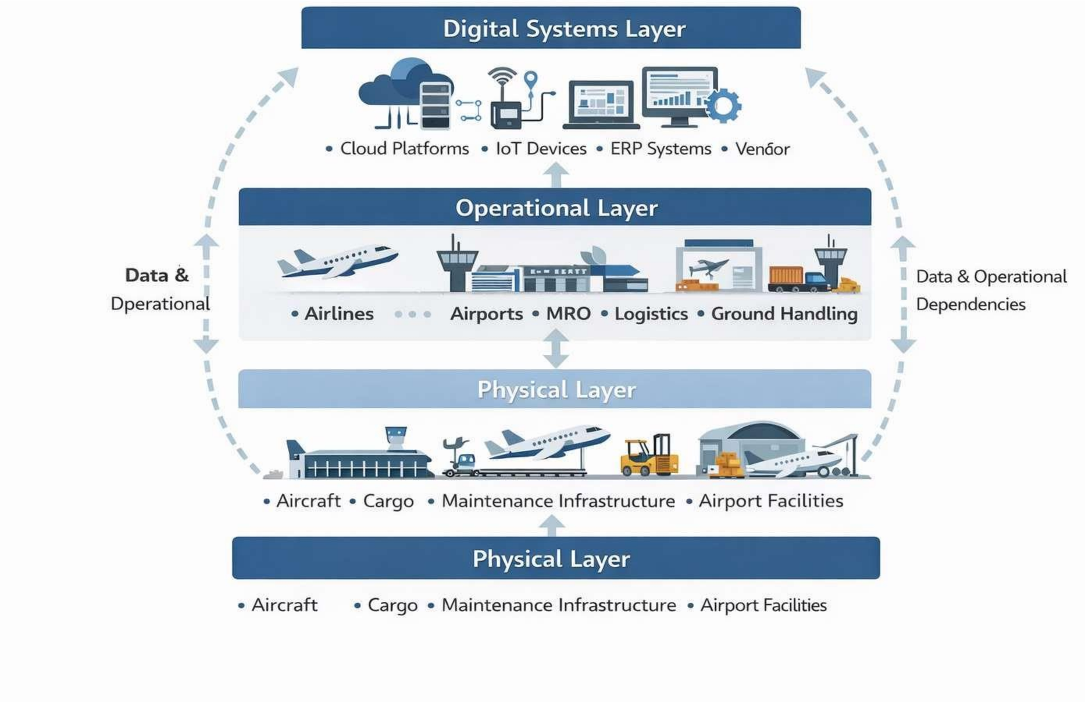
Digital Systems Layer
• Cloud Platforms • IoT Devices • ERP Systems • Venốor
Operational Layer
• Airlines • • • Airports • MRO • Logistics • Ground Handling
Physical Layer
• Aircraft • Cargo • Maintenance Infrastructure • Airport Facilities
Physical Layer
• Aircraft • Cargo • Maintenance Infrastructure • Airport Facilities
Data & Operational
Data & Operational Dependencies

Figure 2: Cyber-Physical Interdependencies in Aviation Supply Chains

3.2 Digitalization and Cyber Risk Expansion

The pursuit of cost optimization and operational efficiency and visibility has struck the drive of the digital transformation of the aviation supply chains. Documentation, blockchain- enabled, predictive maintenance algorithms, logistics based on the internet of things (IoT)- based tracking, and cloud-based logistics services have fundamentally transformed the way supply chain operations are performed [13]. They are applied to monitor aircraft parts in real-time, automated procurement process, aircraft route data, and making complex decisions based on data.

Nevertheless, the literature points at a similar aspect that is repeated over time fingered out-that digitalization expands the amount of attack on sensitive infrastructure systems [14]. Every single device that is linked, every cloud interface, and embedded software platform are all possible entry points of bad actors. The IoT devices in particular have a propensity to be deployed without built-in inbuilt security measures, and that makes it a welcome target. Misconfigurations of the clouds, insecure APIs and ineffective authentication protocols compound the exposure risks.

Digitalization and cybersecurity vulnerability are not connected linearly but conditionally. Although through digital means it has made operations more resilient to well managed setups, when inadequately managed digital transformation is undertaken, it creates systemic vulnerability. The supply chain studies on digitalization have identified that vulnerable effects take place because digitalization of the supply chain technologies and subsequent investments in the governance, monitoring, and training of workforce occur concurrently [15]. At the ecosystems, where the continuality of the operations is the primary issue in aviation, the mentioned vulnerabilities can be translated into flight delays and essential cargo damage and critical disruptions.

In Pakistan, the adoption of digital in the aviation industry is rapidly catching up yet, policies that govern cybersecurity have not been updated alike [16]. The interviews and evaluation of industry resources indicate that the need to digitize platforms is being applied by a substantial number of aviation stakeholders due to the same reasons of predominantly operational efficiency, and cybersecurity concerns are regarded as secondary/ reactive. This is not a specific imbalance but a more general tendency in emerging economies, in which digital innovation has frequently led elements of regulatory consolidation and institutional maturity, behind.

Digitalization is thus conceived by the literature as a two-sided sword: It enhances performance and connectivity, and on the other hand, exposes the organization to cyber. This two-sidedness emphasizes that cybersecurity risk assessment should become the inseparable component of digital transformation strategies. Table 2 summarizes key digital technologies adopted in aviation supply chains and corresponding cyber risk categories.

Table2: Digitalization in Aviation Supply Chains and Associated Cyber Risk Categories

Digitalization Dimension	Operational Benefit	Cyber Risk Category
IoT cargo tracking	Real-time visibility	Device exploitation, spoofing
Cloud maintenance platforms	Data centralization	Data breaches, ransomware
ERP/SCM integration	Process automation	Credential compromise
Vendor software integration	Cross-platform coordination	Supply chain infiltration
Digital documentation systems	Reduced manual errors	Phishing, social engineering

3.3 Cybersecurity in Critical Infrastructure Contexts

The very concept of cybersecurity of critical infrastructure sectors (i.e. in the aviation industry) is completely different than cybersecurity in the normal sphere of the commercial IT industry. The nature of critical infrastructure systems can be defined as the high level of interdependency, significance of national security and the lack of tolerance to disrupt the functioning [17]. Within this context, cyber activities may have physical effects that isolate transport systems, trade income and economic equilibrium.

International standards such as NIST Cybersecurity Framework and International Civil Aviation Organization (ICAO) Cybersecurity Strategy provide a systematic means of detecting, responding to and recovering through to protecting against cyber threats. The frameworks are oriented towards layered defense mechanisms, governance and risk-based prioritization integration. But the performance of implementation largely relies on the capacity of the institutions and the enforcement of the rules.

With developed aviation markets, according to research, will also demand the audit of cybersecurity, incident reporting, and following the requirement to certify the vendor [18]. Conversely, in emerging economies, cohesive systems of governance and resource constraints are common, which also hinder regular enforcement [19]. The cybersecurity ecosystem in Pakistan demonstrates such fragmentation that many agencies cope with the elements of the responsibilities and the guidance regarding the aviation cybersecurity is rather less [20].

Moreover, owing to the geopolitical character and the existence of transnational groups of threat agents, the probability of exposure to such an essential sector of the economy as the aviation one is greater. The attack by adversaries can be done in order to spy on the supply chain systems, disrupt the economy, or to destroy it. Without a single threat intelligence communication and national level cybersecurity centre, organizations are not proactive but reactive in managing risks.

The literature therefore defines regulatory preparedness as an important factor in defining the cyber security resilience. In the absence of sector-specific requirements and institutional controls organizations can apply sporadic or weak security controls. This understanding offers details on the theoretical positioning of the regulatory preparedness as a moderating variable on the impact on cybersecurity outcomes in the aviation supply chains.

3.4 Conceptual Model Development

Based on the analyzed sources, the given research conceptualizes the aviation supply chain cybersecurity as the multi-variable system, which is affected by technological, organizational and regulatory factors. Digitalization, despite the fact that it is required to work efficiently, exposes it to cyber-threats. The exposure is mediated by the organizational cybersecurity maturity-the absence of maturity in organizational processes including governance structure, workforce training, monitoring capabilities and incident response mechanisms-mechanisms. Vulnerability dynamics are also affected by regulatory preparedness and vendor governance by providing minimum standards that have overseeing processes.

The conceptualized cybersecurity vulnerabilities are viewed as the direct consequence of these interacting variables and the end-performance metric, which is resilience, or the ability to withstand, identify, react and remedy cyber events. Figure 3 demonstrates the conceptual research model that will aid in supporting the current study.

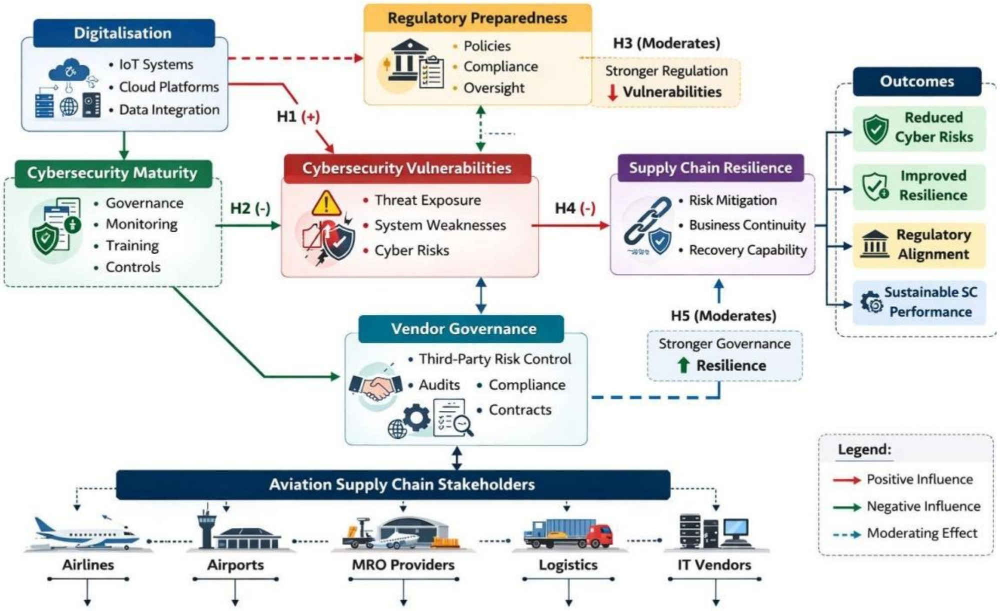

Figure3: Conceptual Model of Aviation Supply Chain Cybersecurity

This conceptual framework is based upon and unites systems theory, risk governance theory, and critical infrastructure resilience literature with the view towards offering a comprehensive perspective through which empirical research could be conducted. It recognizes that the risk of cybersecurity in aviation supply chain emerges due to transformed levels of interdependence among technological advancement, organizational ability and regulatory control.

3.5 Hypotheses Development

With further development based on the theoretical framework presented in the previous section, this paper further elaborates a set of theoretically-grounded-hypotheses in attempts to empirically examine the relationships between digitalization, organizational cybersecurity maturity, regulatory preparedness, vendor governance, cybersecurity vulnerabilities and supply chain resilience in the case of the aviation ecosystem is Pakistan. These hypotheses will be informed by the critical infrastructure cybersecurity sources, the digital supply chain risk theory and governance-based resilience models [21].

3.5.1 Digitalization and Cybersecurity Vulnerabilities

Aviation supply chain digital transformation introduces intertwined platforms, workflow automation, internet of things and cloud-based co-ordination. Although these technologies offer increased visibility of the operations and efficiency, there are also increased access points that give the adversaries the technology access. Every new interface, integration with a particular vendor or a new device expands the attack surface and introduces possible entry vectors of a cyber intrusion.

However, empirical studies in digital supply chain settings indicate that increased digital interconnectivity is also correlated with increased exposure to ransomware, phishing, supply chain and credentials infiltration attacks, and other attacks when the governance mechanisms involved in them remain underdeveloped [22]. In addition, in IoT deployments, the authentication protocols are generally weak, and the firmware security is poor, and can be easily used to exploit the system, especially when used logistical and maintenance applications [23].

Digitalization in the developing aviation spheres such as Pakistan is often resource- INTensive whereby investment in cyber security does not necessarily increase in line with increases in technology [24]. As a result, organizations may assume cloud platform and automation systems without implementing systematic risk examination and constant evaluation systems. This imbalance denotes the existence of positive dependence between the strength of digitalization and the degrees of cybersecurity vulnerability in the presence of low governance maturity level. Therefore, the first hypothesis is formulated as follows:

H1: Digitalization of aviation supply chain systems is positively associated with cybersecurity vulnerabilities.

3.5.2 Organizational Cybersecurity Maturity and Vulnerability Reduction

The maturity of organization cybersecurity reflects how far organized policies, dedication to leadership, employee training, monitoring and response to incidents capabilities have been institutionalized in an organization. Established organizations will tend to have layers of defense in place and periodic risk assessment, testing of its vulnerabilities and incident reporting policies in which certain standards such as NIST or ISO 27001 are adhered to [25].

Critical infrastructure resilience literature notes that cybersecurity maturity is an important factor that influences the ability of an organization in responding and detecting threats before they cause disruption of organizational processes [26]. The high rates of maturity in organizations are more likely to use multi-factor authentication, network segmentation, endpoint detection systems and structure vendor risk assessment. Conversely, simple perimeter protection features like firewalls and antivirus software are more relied upon in low-maturity organizations and may lack enough power to counter-act advanced persistent threats.

The organizational maturity mediates in determining whether or not the digital exposure in the aviation supply chains, where digital integration involves multiple stakeholders, will become vulnerable or resilient. At the high level of maturity, the degree of digitalization can potentially be a strengthener of performance without its connection with a considerable vulnerability. Systemic fragility might deteriorate when the degree of maturity is low with regards to digital expansion. Accordingly, the second hypothesis is proposed:

H2: Organizational cybersecurity maturity is negatively associated with cybersecurity vulnerabilities in aviation supply chains.

3.5.3 Regulatory Preparedness as a Moderating Influence

Regulatory preparedness that encompasses the sector-specific cybersecurity requirements, and implementation mechanisms, audit requirements and formal reporting of incidents; In well-regulated aviation settings, cybersecurity regulations are made institutional with the mandatory evaluation, certification requirement and regulatory control [27].

According to the literature, regulatory clarity is likely to reduce the degree of heterogeneity that exists between the practice of the cybersecurity by the stakeholders of the supply chain and offer the minimum compliance requirements of the protection provided to the digital infrastructure [28]. Organizations may face inconsistent and/or inadequate controls in the location of regulating regimes that are either disorganized or unclear - as in the case of aviation cybersecurity in Pakistan [29].

Preparedness towards regulation consequently influences the intensity of the connection between digitalization and vulnerability. In places where the enforcement of regulations is adopted the digital growth could be facilitated with organized risk control. In this case poor regulation, the digitalization may compound the risks of exposure due to variable security implementation. Regulatory preparedness, thus, is a conceptually seen moderating variable in the relationship between digitalization and vulnerability causing the third hypothesis:

H3: Regulatory preparedness moderates the relationship between digitalization and cybersecurity vulnerabilities, such that stronger regulatory preparedness weakens the positive relationship between digitalization and vulnerabilities.

3.5.4 Cybersecurity Vulnerabilities and Supply Chain Resilience

The aviation industry supply chain resilience is the capability of organizations to stop, notice, react and recover the cyber-attacks without creating any major disruption to its work. The resilience also encompasses the business continuity planning, fast reinstatement of the systems, incident containment and adaptive learning systems.

Resilience theoretical models also focus on the vulnerability exposure direct influence on the organizational resilience to continue operations in an unfavourable environment [30]. Across tight coupling, any weaknesses of one stakeholder within an aviation ecosystem may be passing on in networks that may result in cascading disruptions. An example is a violated vendor software may have an implication on the acquisition of airline schedules, but violated maintenance databases may have an implication on delayed aircraft operations.

Empirical evidence provided by supply chain security studies has been able to indicate that the more vulnerable it is, the less resilient it is as the detection speed is slower, and containment and recovery measures are poor [31]. The vulnerability exposure which can decrease the resilience capacity could be significant in the aviation scenario in Pakistan where no structured aviation incidents responding mechanisms are yet established. Accordingly, the fourth hypothesis is formulated:

H4: Cybersecurity vulnerabilities are negatively associated with supply chain resilience in aviation ecosystems.

3.5.5 Vendor Governance and Resilience Enhancement

The aviation supply chains have become extremely dependent on providing IT facilities, maintenance programs, logistics platform, and digital integration solutions by third parties. Vendor governance can be described as the systems through which organizations manage to measure, monitor and impose cybersecurity requirements on third-party providers.

In literature on the progress of the security of the supply chain, it has been highlighted that the vulnerability in the entire chain of digital ecosystems is usually from third-party systems [32]. This is because of weak practices by the vendors when it comes to securing their core systems; they become vulnerable to being infiltrated, compromised by malicious updates to software and credential theft. Systematic and rigorously-managed vendor vetting, cybersecurity contractual terms as well as audit compliance measures, on the other hand, have a role to play in systemic risk mitigation.

Vendor governance in turn affects the conversion of vulnerabilities into its resilience outcomes. Although the vulnerabilities may exist, the strong vendor oversight efforts may result in the prevention of the escalation to the large-scale disruption by minimizing risks at the nodes located in the periphery. Governance of vendor in this study is conceptualized as a moderating variable that moderates the relationship that exists between vulnerability and resilience. That is why the fifth hypothesis is proposed:

H5: Vendor governance moderates the relationship between cybersecurity vulnerabilities and supply chain resilience, such that stronger vendor governance weakens the negative impact of vulnerabilities on resilience.

3.5.6 Summary of Hypotheses

To generalize on the theoretical propositions, Table 3 presents the summary of hypotheses that were formulated in the current study.

Table3: Summary of Hypotheses

Hypothesis	Relationship Examined	Expected Direction
H1	Digitalization → Vulnerabilities	Positive
H2	Cybersecurity Maturity → Vulnerabilities	Negative
H3	Regulatory Preparedness × Digitalization → Vulnerabilities	Negative Moderation
H4	Vulnerabilities → Resilience	Negative
H5	Vendor Governance × Vulnerabilities → Resilience	Negative Moderation

Together, these hypotheses make the conceptual framework operational and permit an empiricalexplorationofthemulti-dimensionaldynamicsofthecybersecuritythreatina viation supply chain in Pakistan.

4. Research Methodology

4.1 Research Design

The research design applied on this research study consists of a sequential explanatory mixed research design, which is founded on a pragmatic research paradigm. The methodological pluralism is required because of the dynamism of technological, organizational and regulatory variables that interplay in such a manner that cybersecurity risks in aviation supply chains are complicated. Single-method techniques may be inadequate because they are only sufficient to capture two patterns that can be quantified, and the richness of interaction in interdependent cyber-physical ecosystems. That is why the combination of quantitative and qualitative methods creates a deeper detail of the explanation, validity, and practical implementation [33].

This research design has two stages, which are relatively different, but they are combined. In Phase I quantitative data is collected in a structured survey given to stakeholders in the aviation supply chain of the Pakistani territory. This step facilitates preliminary statistical testing of the relationships on the basis of variables that are hypothesized on digitalization, maturity of cybersecurity, regulatory preparedness, vendor governance, vulnerabilities, and resilience. Phase II will involve semi structured interviews with a sample of them to put into perspective and gain deeper insight into and meaning of the quantitative findings.

The chronological arrangement of the explanation helps in assuring qualitative realization with the assistance of empirical trends that are determined in the quantitative stage.

This design will contribute to increasing internal validity because it provides the possibility of triangulating the outcomes, support of frameworks that will be based on both statistical and experiential insights of a particular sector [34]. The sequential mixed method research design to be applied in this research design is presented in Figure 4.

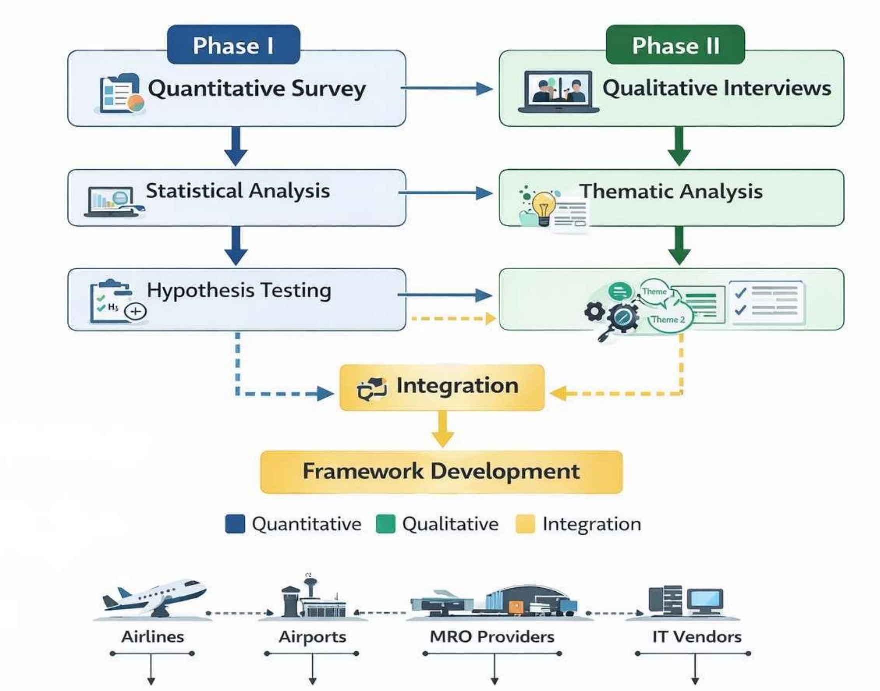

Figure 4: Sequential Explanatory Mixed Method Research Design

The pragmatic paradigm upon which this design is constructed appreciates the fact that the risk of cybersecurity is not only calculable (measurable using a set of constructs), but it can also be socially instilled (constituting organization behaviour and regulatory contexts). In turn, this method is in line with the purpose of the research to create a context-dependent and practical cybersecurity scheme on the aviation ecosystem in Pakistan.

4.2 Population and Sampling

4.2.1 Study Population

Pakistan has important stakeholders in its aviation supply chains, which form the population of interest. These include:

- Airlines
- Airport operators
- Maintenance, Repair, and Overhaul (MRO) providers
- Logistics and cargo operators
- Ground handling companies
- Aviation IT vendors

The combination of these actors is associated with the digital and operational nodes in the aviation ecosystem. The vulnerabilities of this ecosystem to cybersecurity cannot be effectively evaluated by putting the lenses onto a single one of the types of organizations since vulnerabilities tend to permeate and pervade interconnected systems [35].

The intended respondents comprise those in the field of IT governance, cybersecurity control, supply chain alignment, operational management or regulatory controls. This made sure that the people who took part were well versed with digital infrastructure, risk exposure and organizational practices.

4.2.2 Sampling Technique

This was done using a stratified purposive sampling strategy to cover various categories of the major stakeholders. The organizational type has been stratified depending on the variability in digital maturity and cyber security governance. In every stratum, purposive sampling of respondents was done depending on their positions and decision-making duties.

This will help to enhance the validity of the collected information since data is not collected using ignorant individuals who simply happen to be employees but informed individuals (knowledgeable informants). Stratified purposive sampling is particularly adequate when conducting a critical infrastructure study due to access limitations and fear of violating research participant confidentiality and the viability of a random sampling methodology [36].

A total of 150 respondents in the number of approximately 50 aviation organizations were used in the quantitative stage. Each organization provided 2-4 respondents to reflect various approach in the organizational hierarchies.

Not only is this sample size acceptable in the statistical sense of the regression analysis it has sufficient power to test a hypothesis as well. A sample of 120- 200 is normally considered sufficient to complete the multivariate analysis in the literature of cybersecurity research concerning the infrastructures sectors of importance [37]. Table 4 gives the method of distributing respondents in the various categories of stakeholders.

4.2.3 Sample Size Determination

Table4: Sample Distribution Across Aviation Stakeholders

Stakeholder Category	Estimated Organizations	Respondents per Organization	Expected Sample Size
Airlines	10	2–4	25–30
Airport & Ground Handling	10	2–3	20–25
MRO Providers	10	2–3	20–25
Logistics & Cargo Firms	10	2–3	20–25
Aviation IT Vendors	10	2–4	25–30
Total	50	–	~150

On the qualitative stage, 12 semi-structured interviews were conducted with top IT Managers, Cybersecurity Leaders and Supply Chain Leaders. This figure aligns with the qualitative research norms that tend to allow a minimum of 10-15 interviews to be given to achieve a data saturation in research based on the industry [38].

4.3 Measurement Instruments

4.3.1 Instrument Development

The survey tool will be created by following the well-known frameworks of cybersecurity and supply chain risks, including the models of constructs used by the National Institute of Standards and Technology (NIST) Cybersecurity Framework; the principles of cybersecurity embraced by the International Civil Aviation Organization (ICAO); and digital supply chain risk models [39].

The questionnaire included five point Likert scale items (1 = Strongly Disagree to 5 = Strongly Agree) according to which the following constructs were measured:

- Digitalization Level (5 items)
- Organizational Cybersecurity Maturity (7 items)
- Cybersecurity Vulnerabilities (6 items)
- Regulatory Preparedness (4 items)
- Supply Chain Resilience (5 items)
- Vendor Governance (4 items)

Measurement multiple item measurement helps to obtain a better comprehension of construct validity and consistency since latent variables are depicted wholesomely.

4.3.2 Reliability and Validity

A pilot study was conducted on 15 respondents as a refinement of the instrument. The construct reliability was assessed by means of Cronbach alpha on all the scales exceeding the threshold value of 0.70. Table 5 summarizes construct reliability results.

Table5: Construct Reliability (Pilot Testing)

Construct	Number of Items	Cronbach's Alpha	Interpretation
Digitalization	5	0.81	Reliable
Cybersecurity Maturity	7	0.87	Highly Reliable
Vulnerabilities	6	0.79	Reliable
Regulatory Preparedness	4	0.75	Reliable
Resilience	5	0.83	Highly Reliable
Vendor Governance	4	0.78	Reliable

The content validity was established with the help of the expert review presented by the experts in the field of aviation cybersecurity and IT governance. Certain amendments have been made to enhance understandability and introduce sensual relation with the Pakistani Aviation Environment.

4.4 Data Collection Procedure

Data collection occurred in two phases.

Phase I: Quantitative Survey

The email was sent with 852 survey links that were distributed and sent through officially organizational means. Participants were informed about the protection of confidentiality and voluntary participation. After every week of four weeks, reminder emails were sent in a bid to improve the response rates.

Phase II: Qualitative Interviews

The respondents who consented to participate in the follow up were either interviewed using the secure video conferencing software or on-site confidential meetings. Each interview took between 30 and 45 minutes and was audio-taped with their consent. Due to the organizational privacy, transcriptions have been anonymised.

Figure 5 outlines the two-phase data collection process.

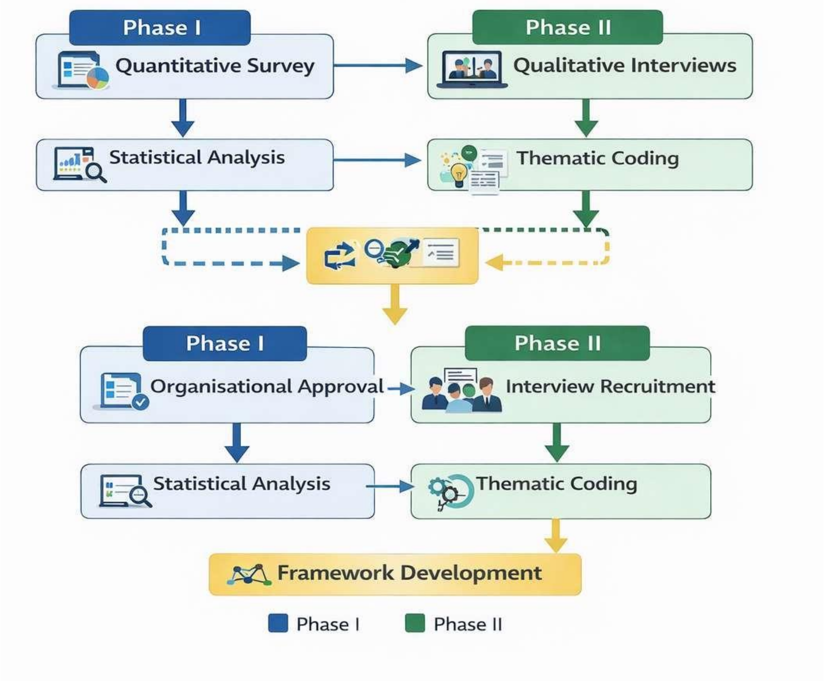

Figure5: Two-Phase Data Collection Process

2. 4.5Data Analysis Techniques

4.5.1 Quantitative Analysis

Quantitative data were analyzed using SPSS software. The analytical procedure included:

- Descriptive statistics (means, standard deviations)
- Reliability analysis (Cronbach's alpha)
- Pearson correlation analysis
- Multiple regression analysis to test hypotheses
- Moderation analysis for H3 and H5

Regression modeling is applicable to establish the predictive associations of the independent and dependent variables and moderation testing investigates the effects of interaction of the regulatory preparedness and vendor governance.

4.5.2 Qualitative Analysis

Thematic analysis is a six-step analytical method that was taken to analyze the qualitative data collected through interview;

1. Familiarization with data
2. Generating initial codes
3. Searching for themes
4. Reviewing themes
5. Defining and naming themes
6. Producing the report

Government areas of weaknesses, risks associated with the vendor, regulatory constraints, and digital maturity and resiliency practices were coded. The NVivo software was applied in assisting in the systematic coding and clustering of themes.

Table 6 provides examples of coding outcomes.

Table 6: Examples of Qualitative Codes and Themes

Code	Theme	Interpretation
“Outdated systems”	Legacy Infrastructure Risk	Exposure due to obsolete technology
“Vendors not audited”	Vendor Governance Weakness	Lack of third-party oversight
“No incident reporting policy”	Regulatory Gap	Absence of formal compliance
“Training limited”	Maturity Deficiency	Low organizational preparedness

5. Results

5.1 Descriptive Statistics

The present state of the digitalization in cybersecurity, regulating correctness, vendor control, vulnerability, and supply chain perseverance of the aviation supply chain stakeholders in Pakistan was analyzed in descriptive mode.

The results indicate that the degree of digitalization is moderate (Mean = 3.84, SD = 0.61) and the use of the IoT systems, cloud platforms and integrated logistics software is at a significant degree. Nonetheless, the scores on cybersecurity maturity are lower (Mean = 3.21, SD = 0.74) which appears to be due to the fact that the system of governance and monitoring has not changed to the extent of the technological adoption.

The mean of cybersecurity vulnerabilities is medium-to-high (Mean = 3.67, SD = 0.69), which proves that the exposure to the cyber threat is seen by the respondents as significant. The score of regulatory preparedness was also relatively low (Mean = 2.98, SD = 0.81) since there was the lack of sector specific enforcement and control. The level of supply chain resilience was moderate (Mean=3.32, SD=0.66) which points to the partial but insufficient readiness to respond to cyber disruptions. Vendor governance also received average marks (Mean = 3.18, SD = 0.72), which indicated careless attention to the third party risks management.

Table 7 summarizes descriptive statistics for all constructs.

Table7: Descriptive Statistics of Study Constructs

Construct	Mean	Standard Deviation	Interpretation
Digitalization	3.84	0.61	Moderately High
Cybersecurity Maturity	3.21	0.74	Moderate
Vulnerabilities	3.67	0.69	Moderately High
Regulatory Preparedness	2.98	0.81	Low–Moderate
Supply Chain Resilience	3.32	0.66	Moderate
Vendor Governance	3.18	0.72	Moderate

Descriptive findings depict a vital lapse of digital adoption and cybersecurity developing at an accelerated pace than institutionalization of cybersecurity. It is conducive to the theoretical suggestion that the absence of alignment in place of governance signifies the augmentation of the danger of exposure [40].

5.2 Reliability and Validity Assessment

The Cronbach alpha was used to assess internal consistency reliability of the total data. The value of all constructs exceeded 0.70 and was a good sign of acceptable reliability.

The inter-item correlation analysis and the factor loading study were used to check the construct validity. All items had loadings above 0.60 that implied convergent validity.

These results indicate that measurement instrument is also statistically strong and is suitable to test hypothesis.

5.3 Correlation Analysis

Pearson correlation analysis was conducted to examine the strength and direction of relationships among variables.

The results reveal:

- A significant positive correlation between Digitalization and Vulnerabilities ($r = 0.52, p < 0.01$).
- A significant negative correlation between Cybersecurity Maturity and Vulnerabilities ($r = -0.61, p < 0.01$).
- A significant negative correlation between Vulnerabilities and Resilience ($r = -0.58, p < 0.01$).
- A moderate positive correlation between Vendor Governance and Resilience ($r = 0.49, p < 0.01$).

These correlations provide preliminary support for H1, H2, and H4.

Table 8 presents the correlation matrix.

Table 8: Correlation Matrix

Variable	1	2	3	4	5	6
1. Digitalization	1					
2. Cybersecurity Maturity	−0.29*	1				
3. Vulnerabilities	0.52**	−0.61**	1			
4. Regulatory Preparedness	−0.34**	0.48**	−0.42**	1		
5. Resilience	−0.21*	0.56**	−0.58**	0.44**	1	
6.Vendor Governance	−0.18*	0.39**	−0.47**	0.41**	0.49**	1

- p < 0.05, ** p <0.01

The negative correlation between maturity and vulnerabilities highlights the importance of governance structures in mitigating cyber risk within aviation ecosystems.

5.4 Regression and Hypothesis Testing

5.4.1 Testing H1 and H2

A multiple regression analysis was done, where Vulnerabilities were taken as the dependent variable and Digitalization and Cybersecurity Maturity were taken as predictors.

Results show:

- Digitalization significantly predicts Vulnerabilities ($\beta = 0.41, p < 0.001$).
- Cybersecurity Maturity significantly predicts Vulnerabilities ($\beta = -0.53, p < 0.001$).
- Model $R^2 = 0.49$, indicating 49% variance explained.

These findings support:

- **H1 (Supported):** Digitalization increases vulnerability exposure.
- **H2 (Supported):** Higher cybersecurity maturity reduces vulnerabilities.

5.4.2 Testing H3 (Moderation by Regulatory Preparedness)

Interaction analysis was carried out introducing a Digitalization*Regulatory Preparedness term. The interaction term was also found significant (beta=-0.19, p<0.05) meaning that the positive relationship between digitalization and vulnerabilities is less the higher is the regulatory preparedness. Thus, H3 is supported.

The outcome demonstrates that the effects of digital expansion can be reduced with the assistance of regulatory control that is organized.

5.4.3 Testing H4 and H5

Resilience was regressed on Vulnerabilities and Vendor Governance.

- Vulnerabilities significantly negatively predict Resilience ($\beta = -0.46$, $p < 0.001$).
- Vendor Governance positively predicts Resilience ($\beta = 0.33$, $p < 0.01$).
- Interaction term (Vulnerabilities × Vendor Governance) was significant ($\beta = 0.17$, $p < 0.05$).

This indicates that strong vendor governance weakens the negative impact of vulnerabilities on resilience.

Thus:

- **H4 (Supported)**
- **H5 (Supported)**

Table 9 summarizes regression results.

Table9: Regression Analysis Results

Hypothesis	βCoefficient	p-value	Result
H1	0.41	<0.001	Supported
H2	−0.53	<0.001	Supported
H3	−0.19(Interaction)	<0.05	Supported
H4	−0.46	<0.001	Supported
H5	0.17 (Interaction)	<0.05	Supported

In general, the results of the empirical models reveal that the model has a good model explanation strength hence supporting the conceptual model.

5.5 Qualitative Findings

Thematic analysis of 12 interviews yielded five dominant themes:

1. **Uneven Digital Adoption** – Larger aviation organizations have advanced systems, while smaller operators rely on legacy infrastructure.
2. **Vendor Weakness as Primary Risk Vector** – Third-party systems are rarely audited comprehensively.
3. **Regulatory Ambiguity** – Lack of aviation-specific cybersecurity standards.
4. **Limited Workforce Training** – Cyber awareness remains low at operational levels.
5. **Reactive Rather Than Proactive Security Posture** – Incident response mechanisms are underdeveloped.

Table 10 summarizes thematic findings.

Table10: Thematic Analysis Summary

Theme	Supporting Insight	Implication
Digital Asymmetry	Disparity in system maturity	Increased systemic exposure
Vendor Risk	Limited compliance enforcement	Supply chain infiltration risk
Regulatory Gaps	No aviation-specific mandates	Governance fragmentation
Training Deficiency	Minimal cyber drills	Weak incident readiness
Reactive Culture	Post-incident response focus	Low preventive capacity

5.6 Integration of Quantitative and Qualitative Findings

The results can be merged to demonstrate the combination of statistical and experiential results. Quantitative findings suggest that the effect of digitalization escalates predispositions; the interviews show that this is true in the blistering employment procedure lacking systematic management. Regression analysis indicates that maturity lowers risk; sense of leadership and formatted auditing are distinguishing features of interviews.

The hypothetical effect of regulatory preparedness is supported qualitatively by the fact that respondents put a great focus on the absence of compulsory compliance models. Equally, the moderation in regards to vendor governance is in line with interview data results where third- party systems have been described as the weakest link. **Table 11** integrates findings across methods.

Table 11: Integrated Quantitative and Qualitative Insights

Quantitative Finding	Qualitative Confirmation	Interpretation
Digitalization → Vulnerabilities	Rapid adoption without controls	Risk amplification effect
Maturity → Reduced Vulnerabilities	Structured audits reduce exposure	Governance importance
Regulatory Moderation	Lack of aviation cyber policy	Institutional weakness
Vulnerabilities → Lower Resilience	Delayed recovery procedures	Operational fragility
Vendor Governance Moderation	Weak third-party audits	Supply chain exposure

All the empirical results indicate that aviation industry supply chains in Pakistan are at the digitization journey but they are poorly governed. The findings promote the worth of a multi-layered, systematic, and cybersecurity risk assessment and mitigation strategy.

7. Discussion

The research work adds technological, organizational and regulatory perspectives to the unified model of aviation supply chain cybersecurity risk management, adding to the theoretical knowledge in the field. Although previous research has touched the issue of cybersecurity in critical infrastructures and digital supply chains in isolation [41], there was a lack of empirical research on the relationships concerning multi-levels in the aviation ecosystem, which exist in the environment of emerging economies.

First, the research contributes to the research on digital supply chain risk theory in that it has brought in empirical evidence of the two sidedness of digitalization. The glass skull between digitalization and cybersecurity weaknesses makes a case stronger in favor of the reality that the technological growth, despite its immature governance, will place overage on a systemic scale. This observation is relevant to the current body of literature as it demonstrates that the effectiveness of digitalization in increasing risks is acute in resource-intensive settings where the preparedness to regulation is not well developed.

Second, the paper enhances the usefulness of organization maturity models in cyber security governance. The correlation of cybersecurity maturity and vulnerabilities is negative with a considerable impact which is confirmed by the fact that vulnerabilities and structured governance, training, monitoring and commitment to the leadership have significant effects in reducing digital exposure risks. The result aligns with the resilience theory which suggests the significance of the adaptive capacity and the contributions of institutional learning towards enhancing the resilience of a system [42].

Third one is the moderator role of regulatory preparedness that is associated with institutional governance theory. The results reveal that the formal regulatory frameworks mitigate the impacts of the vulnerabilities created by the digitalization. This implies that the risk of cybersecurity is not properly addressed at the organizational level and requires integrated institutional management. Systemic weaknesses in the face of individual organizational efforts in new aeronautical markets where the regulation may be incapable of keeping up with digital innovation may persist.

Fourth, the article broadens the supply chain resilience theory since the vulnerability of the chain is empirically validated as a moderating factor between the resilience and the vendor governance. This brings the systemic relevance of the third-party risk management in linked physical ecosystems that are cyberspace.

Altogether, the theoretical contribution will be to show that aviation cybersecurity resilience is more of multi-layers alignment of governance, and not single technical controls. The theoretical integration has been operationalised into an applied governance model through the proposed six layer framework.

8. Conclusion

In this paper, the author has made a more precise examination of the dynamic of cybersecurity risks at the aviation supply chains in Pakistan within the framework of faster digital transformation. These empirical results prove that the concept of digitalization contributes to exposure to vulnerability significantly, provided it is accompanied by unstructured governance and regulatory readiness. Maturity of organizational cybersecurity is seen to have an essential protective role to play - and vendor governance and regulations are determined to have a moderating nature between vulnerability and resiliency. The study has revealed that the resilience of cybersecurity in aviation ecosystems does not only rely on the technical control but on the integration of multi-layered governance that is based on technological, organizational and regulatory layers. As a way of bridging the identified gaps, a layer six integrated Cybersecurity Risk Assessment and Strategic Mitigation Framework unique to the Pakistani aviation ecosystem was created as a study. The framework gives a clear road map in order to identify risk, priorities, ensure technical safeguards, enhance governance, as well as coordinate regulators and achieve continuous improvement. With the help of the empirical analysis along with the development of the practical frameworks, the current study can be seen as building up on the subject of enhancing cybersecurity governance within the segment of the critical infrastructure in a dual way.

REFERENCES

Wisdom, D. D., Vincent, O. R., Igulu, K. T., Aborisade, D. O., Christian, A. U., Hyacinth, E. A., ... & Olatunbosun, A. M. (2025). The Protection of Industry 4.0 and 5.0: Cybersecurity Strategies and Innovations. In *Computational Intelligence for Analysis of Trends in Industry*4.0 *and* 5.0 (pp. 319-352). Auerbach Publications.

Aghazadeh Ardebili, A., Lezzi, M., &Pourmadadkar, M. (2024). Risk Assessment for Cyber Resilience of Critical Infrastructures: Methods, Governance, and Standards. Applied Sciences, 14(24), 11807.

AGILITY IN PAKISTANI MANUFACTURING FIRMS. Qualitative Research Review Letter, 3(2), 1-26.

Ahmed, W. (2024). Advancements in ADS-B security: a comprehensive survey of vulnerabilities, mitigation strategies, system requirements, and emerging research trends.

Ahmed, W. (2025). Artificial Intelligence in Aviation: A Review of Machine Learning and Deep Learning Applications for Enhanced Safety and Security. Intelligence, 3, 100013.

Alam, M., Younas, A., Khan, M., Anwar, A., Gul, S., & Abbas, S. (2025). INTEGRATING SUPPLY CHAIN DIGITALIZATION INTO PROJECT MANAGEMENT: EFFECTS ON OPERATIONAL PERFORMANCEAND THEROLE OF ORGANIZATIONAL

Ali, A. A., & Cheema, A. T. (2025). India's Technological Ascendancy: Implications for Pakistan's Security. Journal of Development and Social Sciences, 6(1), 650–660.

Arshad, N., Ahmad, W., & Manzoor, K. (2024). Unleashing the potential of Pakistan's IT Industry: Building for massive software export growth.

Azmi, F. R., Sukri, N. M., Sundram, V. P. K., Mahmud, N., Zailani, S., & Nordin, N. (2025). Supply Chain Resilience for Manufacturing Industry: A Systematic Review. PaperASIA, 41(3b), 374–393.

Bagul, S. A. (2025). Guarding the Digital Gateway: An In-Depth Analysis of Cybersecurity Challenges in India. In Emerging Trends in Information System Security Using AI & Data Science for Next-Generation Cyber Analytics (pp. 67–92). Cham: Springer Nature Switzerland.

Iqbal, Z., & Shan, R. (2024). Pakistan's Cybersecurity Landscape. CISS Insight Journal, 12(2), P105-131.

Javed, M. D., Taj, S., Khan, R., Awasthi, S., Hassan, H., Xinyue, X., & Khan, M. (2025). Cyber Security Framework for AI-Enabled Robotics and Drone Systems. In Advancing Cybersecurity in Smart Factories Through Autonomous Robotic Defences (pp. 231–262). IGI Global Scientific Publishing.

Jhanjhi, N. Z., & Shah, I. A. (Eds.). (2024). Cybersecurity Measures for Logistics Industry Framework. Igi Global.

Jhanjhi, N. Z., & Shah, I. A. (Eds.). (2024). Navigating cyber threats and cybersecurity in the logistics industry. IGI Global.

Khokhar, R. H., Rankothge, W., Rashidi, L., Mohammadian, H., Ghorbani, A., Frei, B., ... & Freitas, I. (2024). A Survey on Supply Chain Management: Exploring Physical and Cyber Security Challenges, Threats, CriticalApplications, and Innovative Technologies. International Journal of Supply and Operations Management, 11(3), 250–283.

Mustafa, G., Rafiq, W., Jhamat, N., Arshad, Z., & Rana, F. A. (2025). Blockchain- based governance models in e-government: a comprehensive framework for legal, technical, ethical, and security considerations. International Journal of Law and Management, 67(1), 37–55.

Patton, R., &Jahankhani, H. (2025). How Can Existing Cyber Frameworks Be Better Implemented to Ensure Operational Resilience Within the UK Aviation Industry in the Event of a Cyber-Attack Against Its Mission-Critical, Satellite-Based Services?. In Autonomous Revolution: Strategies, Threats and Challenges (pp. 199–239). Cham: Springer Nature Switzerland.

Safraoui, F. (2025). Security Challenges and Air Sovereignty: Between Escalating Threats and the Need for Fortification. Qadim Diyar Beynalxalq Elmi Jurnal, 7(2), 408-419.

Saleem, B., Ahmed, M., Zahra, M., Hassan, F., Iqbal, M. A., & Muhammad, Z. (2024). A survey of cybersecurity laws, regulations, and policies in technologically advanced nations: A case study of Pakistan to bridge the gap. International Cybersecurity Law Review, 5(4), 533–561.

Samad, A., Naz, E., Iqbal, M. J., & Arif, M. S. (2025). STRATEGIC ALIGNMENT BEYOND HISTORY: DEEPENING PAKISTAN-RUSSIA DEFENCE COOPERATION IN A SHIFTING GEOPOLITICAL LANDSCAPE. Journal of Media Horizons, 6(3), 301–317.

Singh, T. (2025). Digital Resilience, Cybersecurity, and Supply Chains. Taylor & Francis.

Talukder, M. B., Hoque, M., & Kumar, S. (2024). Impact of Cybersecurity in the Aviation, Tourism, and Hospitality Industries. In Corporate Cybersecurity in the Aviation, Tourism, and Hospitality Sector (pp. 200–215). IGI Global.

Wisdom, D. D., Vincent, O. R., Igulu, K. T., Aborisade, D. O., Christian, A. U., Hyacinth, E. A., Wu, H., Li, G., & Zheng, H. (2024). How does digital intelligence technology enhance supply chain resilience? Sustainable framework and agenda. Annals of Operations Research, 1–23.

Kashan, A. H., Mehmood, A., Ur, S., Khan, R., Aziz, T., Orakzai, J. K., & ul Islam, M. (2022). Implementation Strategies of Cybersecurity in Pakistan. Journal of Public Policy, 2, 4.

Dhirani, L. L. (2024, January). Data Security, Privacy, and Cyber Policy of Pakistan: A Closer Look. In 2024, IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC) (pp. 1–7). IEEE.

Qasim, M. S., Ahmad, Z., Maqsood, S., Zafar, S., & Azam, M. (2025). ASSESSING CYBERSECURITY CHALLENGES AND RESPONSE READINESS IN PAKISTAN: A COMPREHENSIVE ANALYSIS. Kashf Journal of Multidisciplinary Research, 2(01), 115–125.

Ali, S. M., Razzaque, A., Abbass, H., Yousaf, M., & Ali, S. S. (2025). A novel AI- Based Integrated Cybersecurity Risk Assessment Framework and the resilience of the National critical infrastructure. IEEE Access.

Azam, A., & Ali, N. (2025). Evaluating The Impact Of Financial, Cybersecurity, And Performance Risks On Banking Sector Sustainability: Evidence From Pakistan. Journal of Management & Social Science, 2(1), 541–552.

Malik, Z. U. A., Xing, H. M., Malik, S., Shahzad, T., Zheng, M., & Fatima, H. (2022). Cybersecurity Situation in Pakistan: A Critical Analysis. PalArch's Journal of Archaeology of Egypt/Egyptology, 19(1), 23–32.

Ahmad, S. (2022). Cyber security threat and Pakistan's preparedness: An analysis of national cyber security policy 2021. Pakistan Journal of Humanities & Social Sciences Research, 5(1), 33.

Saleem, B., Ahmed, M., Zahra, M., Hassan, F., Iqbal, M. A., & Muhammad, Z. (2024). A survey of cybersecurity laws, regulations, and policies in technologically advanced nations: A case study of Pakistan to bridge the gap. International Cybersecurity Law Review, 5(4), 533–561.

Iqbal, Z., & us Shan, R. (2024). Pakistan's Cybersecurity Landscape. CISS Insight Journal, 12(2), P105-131.

KHAN, J. A. Cyber Security Threats: A risk Management approach to Smart Cities of Pakistan.

Asif, M., Shah, H., & Asim, H. A. H. (2025). Cybersecurity and audit resilience in digital finance: Global insights and the Pakistani context. Journal of Asian Development Studies, 14(3), 560-573.

Baig, Y. J. (2023). Implementation of Cyber Security in Corporate Sector of Pakistan. International Journal of Advanced Engineering, Management and Science, 9(10), 27-33.

Irfan, M. (2024). A Deep Dive into Cyber Threat Analysis: Formulating Security Strategies for Risk Mitigation.

Haque, E. U., Abbasi, W., Murugesan, S., Anwar, M. S., Khan, F., & Lee, Y. (2023). Cyber forensic investigation infrastructure of Pakistan: an analysis of the cyber threat landscape and readiness. IEEE Access, 11, 40049-40063.

Watto, O. M., Islam, M., Hussain, S. A., & Shahab, M. (2024). Cyber law and cyber security policies in pakistan: a comparative study with USA, canada and australia. Pakistan J Humanit Soc Sci, 12(1), 271-277.

Noor, H., Seelro, D. K., & Ali, S. A. (2024, January). Review of national cybersecurity policies: a case study on Asian countries. In 2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC) (pp. 1-6). IEEE.

Kaifa, U., Yaseen, Z., & Muzaffar, M. (2025). A thematic analysis of Pakistan's cybersecurity policies, regulations and implications. Journal of Climate and Community Development, 4(1), 39-54.

Ibrar, M., Yin, S., Li, H., Karim, S., & Laghari, A. A. (2024). Comprehensive review of emerging cybersecurity trends and developments. International Journal of Electronic Security and Digital Forensics, 16(5), 633-647.