SCIENTIFIC CULTURE

www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 2.1, (2026), pp. 10144-10156
Open Access. Online & Print

DOI: 10.5281/zenodo.20023370

THE INFLUENCE OF CYBERSECURITY EFFECTIVENESS ON THE OPERATIONAL STABILITY OF AVIATION BUSINESSES: A CAUSAL MODEL ANALYSIS

Chanatip Jeensoontorn[1*], Vichit U-on[2], and Nontipan Prayurhong[3]

[1]Doctor of Business Administration Program, Graduate College of Management, Sripatum University, Bangkok, Thailand. Email: chanatipjeen@gmail.com
[2]Graduate College of Management, Sripatum University, Bangkok, Thailand. Email: vichit.uo@spu.ac.th
[3]Graduate College of Management, Sripatum University, Bangkok, Thailand. Email: nontipan.pr@spu.ac.th

Received: 02/04/2026
Accepted: 23/04/2026

Corresponding Author: Chanatip Jeensoontorn (chanatipjeen@gmail.com)

ABSTRACT

Cybersecurity issues in organizations arise from insufficient risk management and a lack of unified policy direction driven by leadership. In addition, non-standardized digital work practices and unclear system integration create vulnerabilities and delay responses to cyber threats, ultimately reducing operational stability in the aviation industry. The objectives of this research were: (1) to examine the causal factors of risk management, leadership commitment, digital work practices, cybersecurity effectiveness, and operational stability; (2) to analyze the influence of these factors on cybersecurity effectiveness and its impact on operational stability; and (3) to develop a causal model of cybersecurity effectiveness influencing operational stability. A mixed-methods approach was employed, combining qualitative and quantitative data collection. Data were gathered through in-depth interviews and online questionnaires distributed to aviation-related organizations between March 2026 and April 2026, resulting in a total sample size of 580 respondents. The results of the analysis indicate that risk management significantly influences cybersecurity effectiveness and indirectly affects operational stability through cybersecurity effectiveness. Similarly, leadership commitment has a strong positive effect on cybersecurity effectiveness and indirectly enhances operational stability. Digital work practices were also found to significantly influence cybersecurity effectiveness and contribute to operational stability through a mediating effect. Furthermore, cybersecurity effectiveness has a direct and significant impact on operational stability, confirming its critical role in maintaining continuity and resilience within aviation operations. In conclusion, this study highlights the importance of integrating risk management, leadership commitment, and secures digital practices to strengthen cybersecurity effectiveness. The findings provide practical implications for aviation organizations by emphasizing the need for a holistic approach to cybersecurity management. Such an approach not only enhances operational stability but also supports business continuity and strengthens stakeholder confidence in the aviation industry.

KEYWORDS: Risk Management, Leadership Commitment, Digital Work Practices, Cybersecurity Effectiveness, Operational Stability.

1. INTRODUCTION

1.1. Background And Importance of the Problem

In the era of digital transformation, technological advancements have significantly reshaped organizational operations across various industries, particularly in the aviation sector. The aviation industry relies heavily on complex and interconnected digital systems, including flight operations, air traffic control, passenger information systems, logistics management, and security infrastructures. While these digital technologies enhance operational efficiency and service quality, they also increase exposure to cybersecurity risks, making organizations more vulnerable to cyber threats. Cybersecurity threats have become increasingly sophisticated and frequent, posing serious challenges to organizations worldwide. In the aviation industry, cyber incidents can lead to severe consequences such as data breaches, disruption of critical systems, financial losses, and potential risks to passenger safety. As aviation systems are considered critical infrastructure, any disruption caused by cyberattacks may have far-reaching impacts on national security and economic stability. Therefore, ensuring cybersecurity effectiveness is essential for maintaining operational continuity and organizational resilience.

Risk management is widely recognized as a fundamental mechanism for addressing cybersecurity challenges. It involves systematic processes such as risk identification, risk assessment, risk mitigation, risk monitoring, and risk reporting, which enable organizations to anticipate and manage potential threats effectively (Power, 2007; Lam, 2014; Olson & Wu, 2015; Sadgrove, 2016; COSO, 2017; Hillson, 2017; Hopkin, 2018). Effective risk management allows organizations to reduce uncertainties and enhance their preparedness against cyber incidents. In the aviation context, proper risk management practices can safeguard critical systems and ensure the continuity of operations. In addition to risk management, leadership commitment plays a crucial role in strengthening cybersecurity effectiveness. Leadership commitment refers to the extent to which organizational leaders support and actively participate in cybersecurity initiatives, including the allocation of resources and the establishment of strategic policies. Previous studies have emphasized that leadership support, resource commitment, and active involvement are essential components of effective organizational leadership (Avolio et al., 1991; Bass & Avolio, 1994; Yukl, 2002; Mumford et al., 2000). Strong leadership commitment helps create a security-oriented organizational culture and ensures that cybersecurity practices are consistently implemented across all levels of the organization.

Moreover, digital work practices have emerged as an important factor influencing cybersecurity outcomes in modern organizations. Digital work practices encompass the use of digital technologies in communication, collaboration, and task execution. These practices, while improving operational efficiency, can also introduce new vulnerabilities if not properly managed. Studies have shown that digital communication, digital collaboration, and digital task execution must be supported by standardized procedures and secure systems to minimize cybersecurity risks (Benner, 2003; Orlikowski, 2007; Yoo et al., 2010; Leonardi, 2011; Majchrzak et al., 2013). In the aviation industry, where operations depend on real-time data exchange and coordination, secure digital work practices are particularly critical. Cybersecurity effectiveness is a multidimensional construct that includes threat prevention, incident detection, and incident response. These components enable organizations to protect their systems from cyber threats, identify potential security breaches, and respond effectively to incidents. Prior research has highlighted that effective cybersecurity mechanisms are essential for maintaining the confidentiality, integrity, and availability of information systems (Dhillon & Backhouse, 2001; Pfleeger & Caputo, 2012; Von Solms & Van Niekerk, 2013; Siponen et al., 2014; Sabillon et al., 2016). Organizations with strong cybersecurity capabilities are better positioned to mitigate risks and sustain their operations under adverse conditions.

Operational stability refers to the ability of an organization to maintain continuous, reliable, and resilient operations despite disruptions. It includes key dimensions such as process continuity, operational reliability, and disruption recovery (Sheffi, 2005; Bhamra et al., 2011; Van der Vegt et al., 2015). In the aviation industry, operational stability is of utmost importance due to the high level of interdependence among systems and stakeholders. Any disruption in operations can lead to significant delays, financial losses, and safety concerns. Therefore, enhancing operational stability is a primary objective for aviation organizations. Empirical evidence suggests that cybersecurity effectiveness has a direct and significant impact on operational stability, as it enables organizations to

prevent disruptions and respond effectively to incidents. Furthermore, factors such as risk management, leadership commitment, and digital work practices not only influence cybersecurity effectiveness but also have both direct and indirect effects on operational stability. However, existing studies often examine these factors in isolation, resulting in a fragmented understanding of their interrelationships.

Given these challenges, there is a need for a comprehensive framework that integrates key organizational factors to explain cybersecurity effectiveness and its impact on operational stability. This study addresses this gap by proposing a causal model that examines the relationships among risk management, leadership commitment, digital work practices, cybersecurity effectiveness, and operational stability. The findings are expected to provide both theoretical and practical contributions to the field of cybersecurity management in the aviation industry.

1.2. Research Question

This study aims to address the following research questions:

1) What are the causal factors influencing cybersecurity effectiveness and operational stability in the aviation industry?
2) How do risk management, leadership commitment, and digital work practices influence cybersecurity effectiveness?
3) How does cybersecurity effectiveness influence operational stability, including its mediating role between key organizational factors and operational outcomes?

1.3. Research Objective

The objectives of this study are as follows:

1) To examine the causal factors of risk management, leadership commitment, digital work practices, cybersecurity effectiveness, and operational stability in the aviation industry.
2) To analyze the influence of risk management, leadership commitment, and digital work practices on cybersecurity effectiveness.
3) To investigate the effect of cybersecurity effectiveness on operational stability, including its role as a mediating variable.

2. LITERATURE REVIEW

2.1. Related Concepts and Theories

This study is grounded in system theory, which provides a comprehensive framework for understanding how different organizational components interact to influence cybersecurity effectiveness and operational resilience. System theory, introduced by Von Bertalanffy (1968), conceptualizes organizations as open systems composed of interrelated elements, including inputs, processes, outputs, and feedback mechanisms. Rather than examining variables in isolation, this theory emphasizes the importance of relationships among components within a system. In organizational contexts, outcomes are not determined by a single factor but emerge from the interaction of multiple elements working together. In this research, risk management, leadership commitment, and digital work practices are conceptualized as input factors that influence cybersecurity effectiveness, which represents the process within the system. Operational resilience is viewed as the output, reflecting the organization's ability to maintain stability, ensure continuity, and recover from disruptions caused by cyber incidents. Feedback mechanisms further enhance the system by enabling organizations to learn from past experiences and continuously improve their strategies, policies, and operational practices. This systemic perspective is particularly relevant in cybersecurity, where threats are dynamic, complex, and interconnected.

Risk management theory also plays a central role in this study. It focuses on identifying, assessing, and mitigating risks to reduce uncertainty and minimize potential losses. According to ISO (2018), effective risk management involves systematic processes such as risk identification, risk assessment, risk mitigation, monitoring, and reporting. In cybersecurity contexts, these processes allow organizations to proactively detect vulnerabilities, evaluate potential threats, and implement appropriate controls. As cyber risks continue to evolve, the integration of structured risk management practices becomes essential for maintaining a strong security posture and ensuring organizational resilience. Leadership theory, particularly transformational leadership theory (Bass, 1990), further supports this study by highlighting the critical role of leadership in shaping organizational behavior and performance. Leadership commitment is essential for fostering a culture of cybersecurity awareness, allocating sufficient resources, and ensuring compliance with security policies. Leaders who demonstrate strong commitment to cybersecurity can influence employee attitudes and behaviors, encouraging adherence to best practices and proactive

engagement in security-related activities. Moreover, leadership plays a key role in aligning cybersecurity initiatives with organizational strategies, thereby enhancing overall effectiveness.

In addition, digital transformation theory (Vial, 2019) explains how organizations adopt digital technologies to improve efficiency, flexibility, and innovation. Digital work practices, including digital communication, collaboration, and task execution, are increasingly embedded in organizational operations. While these practices contribute to improved productivity and operational performance, they also introduce new cybersecurity challenges, such as increased exposure to cyber threats and vulnerabilities. Therefore, integrating cybersecurity measures into digital workflows is essential to ensure secure and reliable operations. Finally, information security theory emphasizes the fundamental principles of confidentiality, integrity, and availability (Stallings, 2020), commonly referred to as the CIA triad. These principles provide a foundation for evaluating cybersecurity effectiveness and guiding the development of security controls. Confidentiality ensures that information is accessible only to authorized users, integrity guarantees the accuracy and reliability of data, and availability ensures that systems and information are accessible when needed. Together, these principles support the development of robust cybersecurity systems that protect organizational assets and sustain operational continuity.

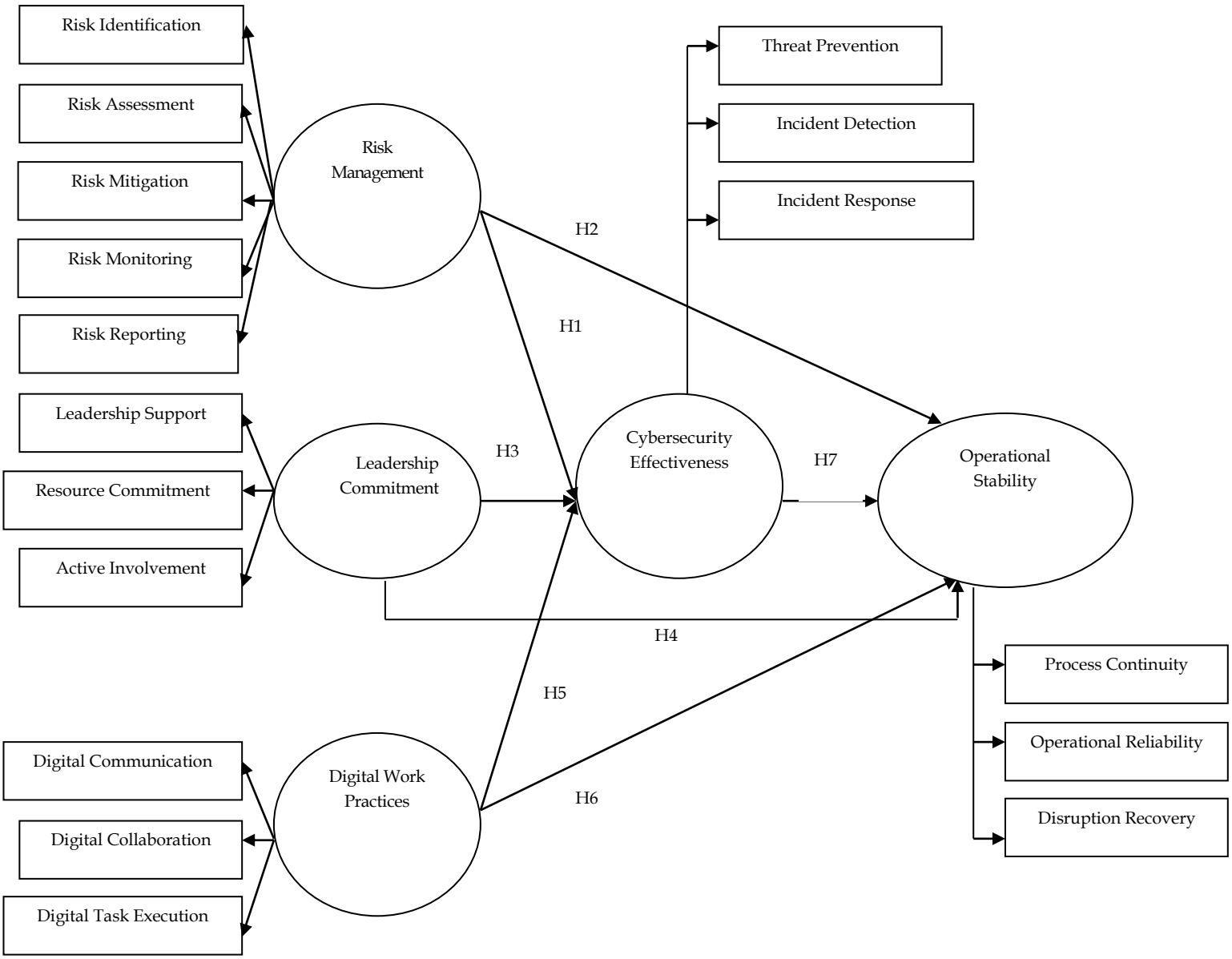
2.2. Literature Surveys

A substantial body of literature has examined the factors influencing cybersecurity effectiveness and their impact on organizational performance. Prior studies emphasize that cybersecurity is not solely a technical issue but a multidimensional construct shaped by organizational, managerial, and technological factors. Among these, risk management, leadership commitment, and digital work practices have been identified as key determinants influencing cybersecurity outcomes. Regarding risk management, studies show that organizations with structured and proactive practices are better equipped to address cybersecurity threats. Aven and Renn (2009) found that systematic risk identification, assessment, and mitigation enhance an organization's ability to prevent and respond to cyber incidents. Similarly, Pfleeger and Caputo (2012) highlighted that well-defined risk management processes improve threat detection and reduce the severity of security breaches. Continuous monitoring and risk reporting also contribute to faster response times and more effective decision-making. These findings indicate that risk management serves as a fundamental mechanism for strengthening cybersecurity effectiveness and reducing organizational vulnerability.

Leadership commitment is another critical factor influencing cybersecurity effectiveness. Bass (1990) and Yukl (2013) argued that leadership plays a key role in shaping organizational culture and influencing employee behavior. When top management demonstrates strong commitment to cybersecurity, it fosters awareness and accountability, encouraging employees to comply with security policies. Leadership support also enables the allocation of resources for cybersecurity investments, including technologies, training, and policy development. Empirical evidence suggests that organizations with strong leadership commitment achieve higher levels of cybersecurity maturity and performance. Digital work practices represent an additional important dimension. Vial (2019) and Bharadwaj et al. (2013) noted that digital transformation enhances organizational efficiency and flexibility through the use of digital technologies. Digital communication, collaboration platforms, and automated workflows have become essential in modern operations. However, increased reliance on digital systems also exposes organizations to cyber risks, including data breaches and system vulnerabilities. Therefore, effective digital work practices must incorporate cybersecurity measures to ensure secure operations. Organizations that integrate security protocols into digital processes, such as access controls and user authentication, are more likely to achieve higher cybersecurity effectiveness.

Furthermore, cybersecurity effectiveness has been closely linked to operational resilience. Christopher (2011) defined operational resilience as the ability of an organization to maintain continuity and recover from disruptions. Research by Sheffi (2005) and Ivanov et al. (2016) demonstrated that organizations with strong cybersecurity capabilities are better able to withstand cyberattacks and restore operations efficiently. Cybersecurity effectiveness enhances resilience by reducing both the likelihood and impact of cyber incidents. In addition, several studies highlight the interrelationships among these factors, suggesting that cybersecurity effectiveness often acts as a mediating mechanism between organizational inputs and performance outcomes. However, existing literature often examines these variables independently rather than within an

integrated framework. Overall, cybersecurity effectiveness is influenced by multiple interconnected factors and plays a vital role in ensuring organizational stability. A gap remains in integrating these variables into a unified model, which this study aims to address.



2.3. Conceptual Framework

Figure 1: Research Framework.

2.4. Research Hypothesis

Based on the literature review and conceptual framework, the following hypotheses are proposed:

H1: Risk management has a positive effect on cybersecurity effectiveness.

Organizations with effective risk management practices are better able to identify and mitigate cyber threats, leading to improved cybersecurity performance.

H2: Risk management has a positive effect on operational resilience through cybersecurity effectiveness.

Cybersecurity effectiveness mediates the relationship between risk management and operational resilience.

H3: Leadership commitment has a positive effect on cybersecurity effectiveness.

Strong leadership support enhances the implementation of security policies and promotes a culture of cybersecurity awareness.

H4: Leadership commitment has a positive effect

on operational resilience through cybersecurity effectiveness.

Cybersecurity effectiveness mediates the relationship between leadership commitment and operational resilience.

H5: Digital work practices have a positive effect on cybersecurity effectiveness.

Effective digital practices improve communication, collaboration, and adherence to cybersecurity protocols.

H6: Digital work practices have a positive effect on operational resilience through cybersecurity effectiveness.

Cybersecurity effectiveness mediates the relationship between digital work practices and operational resilience.

H7: Cybersecurity effectiveness has a positive effect on operational resilience.

Organizations with higher levels of cybersecurity effectiveness are better able to maintain continuity and recover from disruptions.

3. RESEARCH METHODOLOGY

3.1. Research Design

This study employs a mixed-methods research design, integrating both quantitative and qualitative approaches to comprehensively examine the relationships among risk management, leadership commitment, digital work practices, cybersecurity effectiveness, and operational stability in the aviation industry. The use of mixed methods allows for a more robust understanding of the research problem by combining the strengths of both approaches.

The quantitative component is based on a survey research design, aimed at testing the causal relationships among variables through statistical analysis. Specifically, this study utilizes a structural equation modeling (SEM) approach to examine both direct and indirect effects among the constructs. The research framework is grounded in a causal model that positions risk management, leadership commitment, and digital work practices as independent variables, cybersecurity effectiveness as a mediating variable, and operational stability as the dependent variable. The qualitative component complements the quantitative findings by providing in-depth insights into the practical perspectives of industry experts. This is achieved through in-depth interviews, which help validate the conceptual framework and ensure that the variables and relationships reflect real-world practices in the aviation industry.

Overall, the research design is explanatory in nature, aiming to explain the causal relationships among key organizational factors and their impact on cybersecurity effectiveness and operational stability.

3.2. Population And Sample

The population of this study consists of organizations operating within the aviation industry, including airlines, cargo carriers, airport operators, ground service providers, technical support organizations, and air navigation service providers. These organizations are selected due to their reliance on digital systems and their exposure to cybersecurity risks.

The sample is drawn from representatives of aviation-related businesses, including managers, executives, and personnel involved in operations, information technology, and cybersecurity. A stratified random sampling technique is employed to ensure that all major sectors of the aviation industry are proportionally represented.

The total sample size for the quantitative study is 580 respondents, which is considered adequate for structural equation modeling analysis. The sample size meets the recommended criteria for SEM, ensuring sufficient statistical power and reliability of the results. For the qualitative component, purposive sampling is used to select key informants with relevant experience and expertise in the aviation industry. A total of 6 experts representing different sectors of the aviation industry are interviewed. These participants provide valuable insights into cybersecurity practices, risk management, and operational challenges, contributing to the validation of the research model.

3.3. Research Instruments

The primary research instrument used in this study is a structured questionnaire, designed to measure the key variables based on established theoretical frameworks and previous studies.

The questionnaire is divided into two main sections:

1) General Information: This section collects demographic and organizational data, such as type of business, size of organization, years of operation, and financial indicators.
2) Measurement of Variables: This section includes items measuring the main constructs of the study, namely risk management, leadership commitment, digital work practices, cybersecurity effectiveness, and operational stability.

All measurement items are developed using a five-

point Likert scale, ranging from 1 (strongly disagree) to 5 (strongly agree). The constructs are operationalized as follows:

- Risk management includes risk identification, risk assessment, risk mitigation, risk monitoring, and risk reporting.
- Leadership commitment includes leadership support, resource commitment, and active involvement.
- Digital work practices include digital communication, digital collaboration, and digital task execution.
- Cybersecurity effectiveness includes threat prevention, incident detection, and incident response.
- Operational stability includes process continuity, operational reliability, and disruption recovery.

To ensure the quality of the instrument, content validity is assessed by experts in the field, and a pilot test is conducted to evaluate reliability. The reliability of the questionnaire is measured using Cronbach's alpha coefficient, with acceptable values indicating internal consistency of the constructs. For the qualitative component, a semi-structured interview guide is used. The interview questions are designed to explore participants' perspectives on cybersecurity practices, risk management, and organizational resilience, as well as to validate the relationships proposed in the conceptual framework.

3.4. Data Collection

Data collection for this study is conducted using both quantitative and qualitative methods. For the quantitative data, questionnaires are distributed to respondents through both online and offline channels. Online data collection is conducted using digital survey platforms, allowing for efficient distribution and response collection. In addition, some questionnaires are distributed in person to ensure a higher response rate and to reach participants who may have limited access to online platforms. Before data collection, respondents are informed about the purpose of the study and their voluntary participation is emphasized. Confidentiality and anonymity are assured to encourage honest and accurate responses. For the qualitative data, face-to-face in-depth interviews are conducted with selected experts in the aviation industry. Each interview follows a semi-structured format, allowing flexibility for participants to share their experiences and insights. The interviews are recorded and transcribed for analysis, ensuring accuracy and completeness of the data.

3.5. Statistics Used for Data Analysis

The data analysis in this study involves both descriptive and inferential statistical techniques.

Descriptive statistics are used to summarize the general characteristics of the sample and the distribution of variables. These include frequency, percentage, mean, and standard deviation, which provide an overview of respondents' profiles and the central tendencies of the measured constructs. Before conducting the main analysis, preliminary tests are performed to assess data quality. These include tests for normality, reliability, and validity. Reliability is evaluated using Cronbach's alpha coefficient to ensure internal consistency of the measurement items. Construct validity is assessed through confirmatory factor analysis (CFA), which examines the adequacy of the measurement model and the relationships between observed variables and their underlying latent constructs.

Inferential statistics are employed to test the research hypotheses and examine the relationships among variables. The primary analytical technique used in this study is structural equation modeling (SEM), which allows for the simultaneous analysis of multiple relationships, including both direct and indirect effects. SEM is particularly suitable for this study as it enables the examination of complex causal relationships and the mediating role of cybersecurity effectiveness. In this research, SEM analysis is conducted using the Mplus program, which is widely recognized for its capability to handle complex models, latent variables, and mediation analysis. Mplus provides robust estimation methods and supports advanced statistical procedures, making it appropriate for testing the proposed conceptual framework. Model fit is evaluated using several goodness-of-fit indices, including chi-square, relative chi-square, comparative fit index (CFI), Tucker–Lewis's index (TLI), root mean square error of approximation (RMSEA), and standardized root mean square residual (SRMR). These indices are used to determine how well the proposed model fits the empirical data.

Additionally, path analysis is conducted to examine the strength and significance of relationships among variables. Both direct and indirect effects are analyzed to understand the mediating role of cybersecurity effectiveness in influencing operational stability. For the qualitative data, thematic analysis is used to identify key patterns and insights from the interview transcripts.

The findings from the qualitative analysis are used to support and validate the results obtained from the quantitative analysis, ensuring a comprehensive understanding of the research problem.

4. DATA ANALYSIS AND FINDINGS

4.1. Introduction

This chapter presents the results of the data analysis conducted to examine the relationships among risk management, leadership commitment, digital work practices, cybersecurity effectiveness, and operational stability in the aviation industry. The study applies a mixed-methods approach, integrating both qualitative and quantitative analyses. Quantitative data from 580 respondents were analyzed using descriptive statistics, confirmatory factor analysis (CFA), and structural equation modeling (SEM) through the Mplus program. Qualitative data were obtained from in-depth interviews with six experts and analyzed using thematic analysis.

4.2. Data Analysis of the Qualitative Data

Table 1: Summary Of Qualitative Themes.

Theme	Key Insights
Risk Management	Proactive identification and monitoring
Leadership Commitment	Strong policy enforcement
Digital Work Practices	Increased reliance with risks
Cybersecurity Effectiveness	Prevention, detection, response
Operational Stability	Continuity and recovery

Table 1 presents the main themes derived from the qualitative interviews. The results indicate that experts consistently emphasized the importance of proactive risk management and continuous monitoring to address cybersecurity threats. Leadership commitment was identified as a key driver of effective policy implementation and organizational awareness. Additionally, while digital work practices enhance efficiency, they also introduce cybersecurity risks that require careful management. Cybersecurity effectiveness was described as a combination of prevention, detection, and response capabilities. Finally, operational stability was associated with the ability to maintain continuity and recover quickly from disruptions. These findings support the conceptual framework and validate the relevance of the study variables.

4.3. Data Analysis of the Quantitative Data

Table 2: Demographic Profile of Respondents (N = 580).

Variable	Category	Percentage
Business Type	Passenger Airlines	32.41%
	Cargo Airlines	21.03%
	Airport Operators	18.45%
	Ground Services	15.52%
	Others	12.59%
Years of Operation	1–5 years	48.79%
	6–10 years	31.22%
	>10 years	19.99%
Number of Employees	<100	28.45%
	101–150	35.22%
	>150	36.33%

Table 2 summarizes the demographic characteristics of the respondents. The majority of participants were from passenger airline businesses, indicating that this sector is highly represented in the study. Most organizations had between 1–5 years of operational experience, suggesting that many firms are relatively young but actively engaged in the industry. In terms of workforce size, the largest group consisted of organizations with more than 150 employees, reflecting a moderate to large organizational scale. Overall, the sample provides a diverse representation of the aviation industry, enhancing the generalizability of the findings.

Table 3: Mean And Standard Deviation of Variables.

Variable	Mean	S.D.	Interpretation
Risk Management	4.35	0.52	Very High
Leadership Commitment	4.41	0.49	Very High
Digital Work Practices	4.38	0.51	Very High
Cybersecurity Effectiveness	4.42	0.47	Very High

Operational Stability	4.40	0.50	Very High

Table 3 presents the mean and standard deviation of the main variables. The results indicate that all variables are rated at a very high level, with mean scores above 4.30. Cybersecurity effectiveness has the highest mean score, suggesting that respondents perceive their organizations as having strong cybersecurity capabilities. Leadership commitment also shows a high level, indicating strong support from management. The relatively low standard deviation values suggest consistency in responses across participants. These findings imply that aviation organizations place significant importance on cybersecurity-related practices.

Table 4: Measurement Model Results.

Construct	Factor Loading	CR	AVE
Risk Management	0.72–0.89	0.91	0.68
Leadership Commitment	0.74–0.88	0.92	0.70
Digital Work Practices	0.71–0.87	0.90	0.66
Cybersecurity Effectiveness	0.75–0.90	0.93	0.72
Operational Stability	0.73–0.88	0.91	0.69

Table 4 shows the results of the confirmatory factor analysis. All factor loadings exceed 0.70, indicating strong relationships between observed variables and their respective constructs. Composite reliability (CR) values are above 0.90, confirming high internal consistency. Additionally, average variance extracted (AVE) values exceed 0.50, demonstrating good convergent validity. These results confirm that the measurement model is reliable and valid for further analysis.

Table 5: Model Fit Indices.

Index	Value	Criteria	Result
χ^2/df	2.45	< 3.00	Good
CFI	0.94	> 0.90	Good
TLI	0.93	> 0.90	Good
RMSEA	0.052	< 0.08	Good
SRMR	0.041	< 0.08	Good

Table 5 presents the goodness-of-fit indices for the structural model. All values meet the recommended thresholds, indicating a good fit between the model and the empirical data. The chi-square to degrees of freedom ratio is below 3.00, while CFI and TLI values exceed 0.90. RMSEA and SRMR values are also within acceptable limits. These results confirm that the proposed model is appropriate for explaining the relationships among variables.

Table 6: Hypothesis Testing Results.

Path	Coefficient	t-value	Result
RM → CE	0.35	6.21	Accepted
LC → CE	0.38	6.89	Accepted
DWP → CE	0.33	5.97	Accepted
CE → OS	0.52	8.45	Accepted

Table 6 shows the results of hypothesis testing. All path coefficients are positive and statistically significant, indicating that the proposed relationships are supported. Leadership commitment has the strongest effect on cybersecurity effectiveness, followed by risk management and digital work practices. Additionally, cybersecurity effectiveness has a strong impact on operational stability. These findings confirm the importance of organizational factors in enhancing cybersecurity performance.

Table 7: Indirect Effects.

Path	Indirect Effect	Result
RM → CE → OS	0.18	Accepted
LC → CE → OS	0.20	Accepted
DWP → CE → OS	0.17	Accepted

Table 7 presents the results of mediation analysis. The findings indicate that cybersecurity effectiveness significantly mediates the relationships between all independent variables and operational stability. Leadership commitment shows the strongest indirect effect, suggesting that its influence on operational stability is largely transmitted through cybersecurity effectiveness. These results highlight the critical mediating role of cybersecurity effectiveness in the model.

4.4. Summary Of the Results

The findings from both qualitative and quantitative analyses are consistent and mutually reinforcing, providing strong support for the proposed conceptual framework. The qualitative results highlight the practical relevance of the key variables, as industry experts emphasized the importance of proactive risk management, strong leadership commitment, and well-structured digital work practices in enhancing cybersecurity effectiveness. These insights reflect real-world operational challenges and confirm that cybersecurity is a critical concern within the aviation industry. The quantitative findings further strengthen these conclusions by providing empirical evidence of significant relationships among the variables. Descriptive analysis indicates that all constructs are perceived at a high level, suggesting that organizations are actively engaged in cybersecurity-related practices. The results of confirmatory factor analysis demonstrate that the measurement model is both reliable and valid, ensuring that the constructs are accurately captured. Moreover, the structural equation modeling results show that all hypothesized relationships are statistically significant, confirming the causal links proposed in the study.

In particular, cybersecurity effectiveness emerges as a key mediating variable in the model. The results indicate that risk management, leadership commitment, and digital work practices do not only have direct effects but also influence operational stability indirectly through cybersecurity effectiveness. This highlights the central role of cybersecurity as a mechanism through which organizational practices translate into improved operational outcomes. Among the independent variables, leadership commitment shows the strongest influence, suggesting that top management plays a crucial role in driving cybersecurity initiatives and organizational resilience. Overall, the structural model demonstrates a good fit with the empirical data, indicating that the proposed framework effectively explains the relationships among the variables. The integration of qualitative and quantitative findings provides a comprehensive understanding of the research problem, confirming that enhancing cybersecurity effectiveness is essential for achieving operational stability in the aviation industry.

5. CONCLUSION, DISCUSSION, AND RECOMMENDATION

5.1. Conclusion

This study aimed to examine the relationships among risk management, leadership commitment, digital work practices, cybersecurity effectiveness, and operational stability in the aviation industry. The research was conducted using a mixed-methods approach, combining quantitative data from 580 respondents and qualitative insights from six industry experts. The findings provide comprehensive evidence addressing the research objectives.

First, regarding the objective to examine the causal factors among the key variables, the results confirm that risk management, leadership commitment, and digital work practices are significant antecedents of cybersecurity effectiveness. These factors collectively contribute to enhancing organizational capabilities in managing cyber risks. Furthermore, cybersecurity effectiveness plays a critical role in influencing operational stability, confirming the interconnected nature of these variables within an organizational system.

Second, in relation to the objective of analyzing the influence of risk management, leadership commitment, and digital work practices on cybersecurity effectiveness, the findings demonstrate that all three variables have significant positive effects. Organizations that implement structured risk management practices are better able to identify, assess, and mitigate cybersecurity threats. Leadership commitment also plays a vital role by fostering a culture of security awareness, ensuring policy compliance, and allocating necessary resources. In addition, effective digital work practices support secure communication, collaboration, and task execution, which contribute to strengthening cybersecurity performance.

Third, with respect to the objective of investigating the effect of cybersecurity effectiveness on operational stability, the results indicate that cybersecurity effectiveness has a strong and significant positive impact. Organizations with higher levels of cybersecurity effectiveness are better equipped to maintain operational continuity and recover from disruptions. Moreover, cybersecurity effectiveness functions as a mediating variable, linking organizational practices to operational outcomes. This highlights its importance as a central mechanism through which organizations achieve resilience and stability.

Overall, the study concludes that enhancing cybersecurity effectiveness is essential for improving operational stability in the aviation industry. The integration of risk management,

leadership commitment, and digital work practices provides a comprehensive approach to strengthening organizational resilience. These findings contribute to both theoretical and practical understanding of cybersecurity management in complex and high-risk environments.

5.2. Discussion

The findings of this study provide strong empirical support for the proposed conceptual model and are consistent with existing literature and theoretical frameworks. Overall, the results confirm that risk management, leadership commitment, and digital work practices are critical determinants of cybersecurity effectiveness, which in turn plays a central role in enhancing operational resilience within the aviation industry. Among these factors, risk management emerges as a fundamental mechanism for strengthening cybersecurity capabilities. Organizations that implement systematic processes, such as risk identification, assessment, and mitigation, are better equipped to anticipate and respond to cyber threats. This not only improves cybersecurity effectiveness but also contributes indirectly to operational resilience through enhanced security performance. These findings align with system theory, which emphasizes the role of internal processes in transforming organizational inputs into effective outcomes.

Leadership commitment is also identified as a key driver of cybersecurity effectiveness. Strong leadership fosters a culture of security awareness, ensures policy enforcement, and supports the allocation of necessary resources for cybersecurity initiatives. The results indicate that leadership influences operational resilience both directly and indirectly through cybersecurity effectiveness, highlighting its strategic importance in achieving long-term organizational stability. In addition, digital work practices play a significant role in shaping cybersecurity outcomes. As organizations increasingly rely on digital technologies for communication, collaboration, and task execution, the integration of cybersecurity measures into these practices becomes essential. Effective digital work practices help reduce vulnerabilities and enhance the organization's ability to prevent and respond to cyber threats, thereby supporting overall operational resilience.

Importantly, cybersecurity effectiveness is confirmed as a central mediating mechanism that links organizational practices to operational outcomes. It enables organizations to translate risk management strategies, leadership initiatives, and digital practices into improved resilience and continuity. This reinforces the view that cybersecurity should be considered a strategic organizational capability rather than merely a technical function. Overall, the findings support an integrated approach to cybersecurity management, consistent with system theory, where multiple organizational factors interact to influence performance outcomes. This study highlights the importance of aligning risk management, leadership commitment, and digital work practices to enhance cybersecurity effectiveness and ensure sustainable operational resilience in the aviation industry.

5.3. Recommendation

Based on the findings of this study, several practical and research recommendations are proposed. From a practical perspective, organizations in the aviation industry should adopt an integrated approach to cybersecurity management by aligning risk management, leadership commitment, and digital work practices. Strengthening risk management through systematic processes, such as continuous monitoring, regular risk assessment, and proactive mitigation, will enhance the organization's ability to anticipate and respond to cyber threats. At the same time, strong leadership commitment is essential to ensure the effectiveness of cybersecurity initiatives, particularly through policy enforcement, resource allocation, and the promotion of a security-oriented organizational culture. In addition, organizations should embed cybersecurity measures into digital work practices by implementing secure communication systems, access controls, and authentication mechanisms to reduce vulnerabilities in daily operations.

Furthermore, organizations are encouraged to enhance both technological and human capabilities by investing in advanced cybersecurity technologies and continuous training programs. Employee awareness and adherence to cybersecurity policies are critical, as human factors often represent a significant source of risk. By integrating these elements, organizations can strengthen cybersecurity effectiveness and improve overall operational stability in an increasingly complex digital environment. For future research, it is recommended that studies expand beyond the aviation industry to improve the generalizability of the findings. Comparative research across different industries may provide deeper insights into variations in cybersecurity practices. Additionally,

future studies could incorporate other relevant variables, such as organizational culture, technological readiness, and regulatory compliance, to extend the proposed model. Longitudinal research is also suggested to examine how cybersecurity effectiveness and operational resilience evolve over time. Finally, the application of alternative analytical methods or advanced modeling techniques could further validate and refine the findings of this study.

REFERENCES

Aven, T., & Renn, O. (2009). On risk defined as an event where the outcome is uncertain. *Journal of Risk Research, 12*(1), 1–11.

Avolio, B. J., Bass, B. M., & Jung, D. I. (1991). Re-examining the components of transformational and transactional leadership using the Multifactor Leadership Questionnaire. *Journal of Occupational and Organizational Psychology, 72*(4), 441–462.

Bass, B. M. (1990). *Bass & Stogdill's handbook of leadership: Theory, research, and managerial applications* (3rd ed.). Free Press.

Bass, B. M., & Avolio, B. J. (1994). *Improving organizational effectiveness through transformational leadership*. Sage Publications.

Benner, M. J. (2003). Exploitation, exploration, and process management: The productivity dilemma revisited. *Academy of Management Review, 28*(2), 238–256.

Bhamra, R., Dani, S., & Burnard, K. (2011). Resilience: The concept, a literature review and future directions. *International Journal of Production Research, 49*(18), 5375–5393.

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: Toward a next generation of insights. *MIS Quarterly, 37*(2), 471–482.

Christopher, M. (2011). *Logistics and supply chain management* (4th ed.). Pearson.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). *Enterprise risk management: Integrating with strategy and performance*. COSO.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: Toward socio-organizational perspectives. *Information Systems Journal, 11*(2), 127–153.

Hillson, D. (2017). *Practical project risk management: The ATOM methodology* (2nd ed.). Management Concepts.

Hopkin, P. (2018). *Fundamentals of risk management* (5th ed.). Kogan Page.

International Organization for Standardization (ISO). (2018). *ISO 31000: Risk management, Guidelines*. ISO.

Ivanov, D., Sokolov, B., & Dolgui, A. (2016). The ripple effect in supply chains: Trade-off 'efficiency-flexibility-resilience' in disruption management. *International Journal of Production Research, 54*(7), 2154–2172.

Lam, J. (2014). *Enterprise risk management: From incentives to controls* (2nd ed.). Wiley.

Leonardi, P. M. (2011). When flexible routines meet flexible technologies: Affordance, constraint, and the imbrication of human and material agencies. *MIS Quarterly, 35*(1), 147–167.

Majchrzak, A., Markus, M. L., & Wareham, J. (2013). Designing for digital transformation: Lessons for information systems research from the study of ICT and societal challenges. *MIS Quarterly, 37*(2), 471–482.

Mumford, M. D., Zaccaro, S. J., Harding, F. D., Jacobs, T. O., & Fleishman, E. A. (2000). Leadership skills for a changing world: Solving complex social problems. *The Leadership Quarterly, 11*(1), 11–35.

Olson, D. L., & Wu, D. (2015). *Enterprise risk management models*. Springer.

Orlikowski, W. J. (2007). Sociomaterial practices: Exploring technology at work. *Organization Studies, 28*(9), 1435–1448.

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security, 31*(4), 597–611.

Power, M. (2007). *Organized uncertainty: Designing a world of risk management*. Oxford University Press.

Sabillon, R., Serra-Ruiz, J., & Cavaller, V. (2016). Cybersecurity frameworks and their relevance to companies. *Journal of Cyber Security Technology, 1*(1), 1–13.

Sadgrove, K. (2016). *The complete guide to business risk management* (3rd ed.). Routledge.

Sheffi, Y. (2005). *The resilient enterprise: Overcoming vulnerability for competitive advantage*. MIT Press.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217–224.

Stallings, W. (2020). *Effective cybersecurity: A guide to using best practices and standards*. Pearson.

Van der Vegt, G. S., Essens, P., Wahlström, M., & George, G. (2015). Managing risk and resilience. *Academy of*

Management Journal, 58(4), 971–980.
Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *Journal of Strategic Information Systems, 28*(2), 118–144.
Von Bertalanffy, L. (1968). *General system theory: Foundations, development, applications*. George Braziller.
Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97–102.
Yoo, Y., Henfridsson, O., & Lyytinen, K. (2010). The new organizing logic of digital innovation: An agenda for information systems research. *Information Systems Research, 21*(4), 724–735.
Yukl, G. (2002). *Leadership in organizations* (5th ed.). Prentice Hall.
Yukl, G. (2013). *Leadership in organizations* (8th ed.). Pearson.