STUDY ON CYBER THREAT PERCEPTION IN THE INDIAN CIVIL AVIATION SECTOR WITH RESPECT TO DELHI AIRPORT

A thesis submitted to the
University of Petroleum and Energy Studies

For the Award of
Doctor of Philosophy
in Management

BY
Lt Col Anjan Kumar Sinha

Dec 2020

SUPERVISOR (S)
Dr. Binod Kumar Singh
Dr Bharat Bhusan Pandey

UPES
UNIVERSITY WITH A PURPOSE

Department of General Management
School of Business
University of Petroleum & Energy Studies
Dehradun- 248007, Uttarakhand

STUDY ON CYBER THREAT PERCEPTION IN THE INDIAN CIVIL AVIATION SECTOR WITH RESPECT TO DELHI AIRPORT

A thesis submitted to the
University of Petroleum and Energy Studies

For the Award of
Doctor of Philosophy
in Management

BY
Lt Col Anjan Kumar Sinha
(SAP ID- 500026384)

Dec 2020

Internal Supervisor

Dr. Binod Kumar Singh

Assistant Professor - Selection Grade

Department of General Management

School of Business

University of petroleum and Energy studies, Dehradun

External Supervisor

Col (Dr.) Bharat Bhushan Pandey, Retd

UPES
UNIVERSITY WITH A PURPOSE

Department of General Management
School of Business
University of Petroleum & Energy Studies
Dehradun – 248007, Uttarakhand

March 2021

DECLARATION

I declare that the thesis entitled ***Study on Cyber Threat Perception in the Indian Civil Aviation Sector with respect to Delhi Airport*** has been prepared by me under the guidance of **Dr. Binod Kumar Singh**, Department of General Management, School of Business, University of Petroleum and Energy Studies, Dehradun. No part of this thesis has formed the basis for the award of any degree or fellowship previously.

(Anjan Kumar Sinha)

UPES
UNIVERSITY WITH A PURPOSE

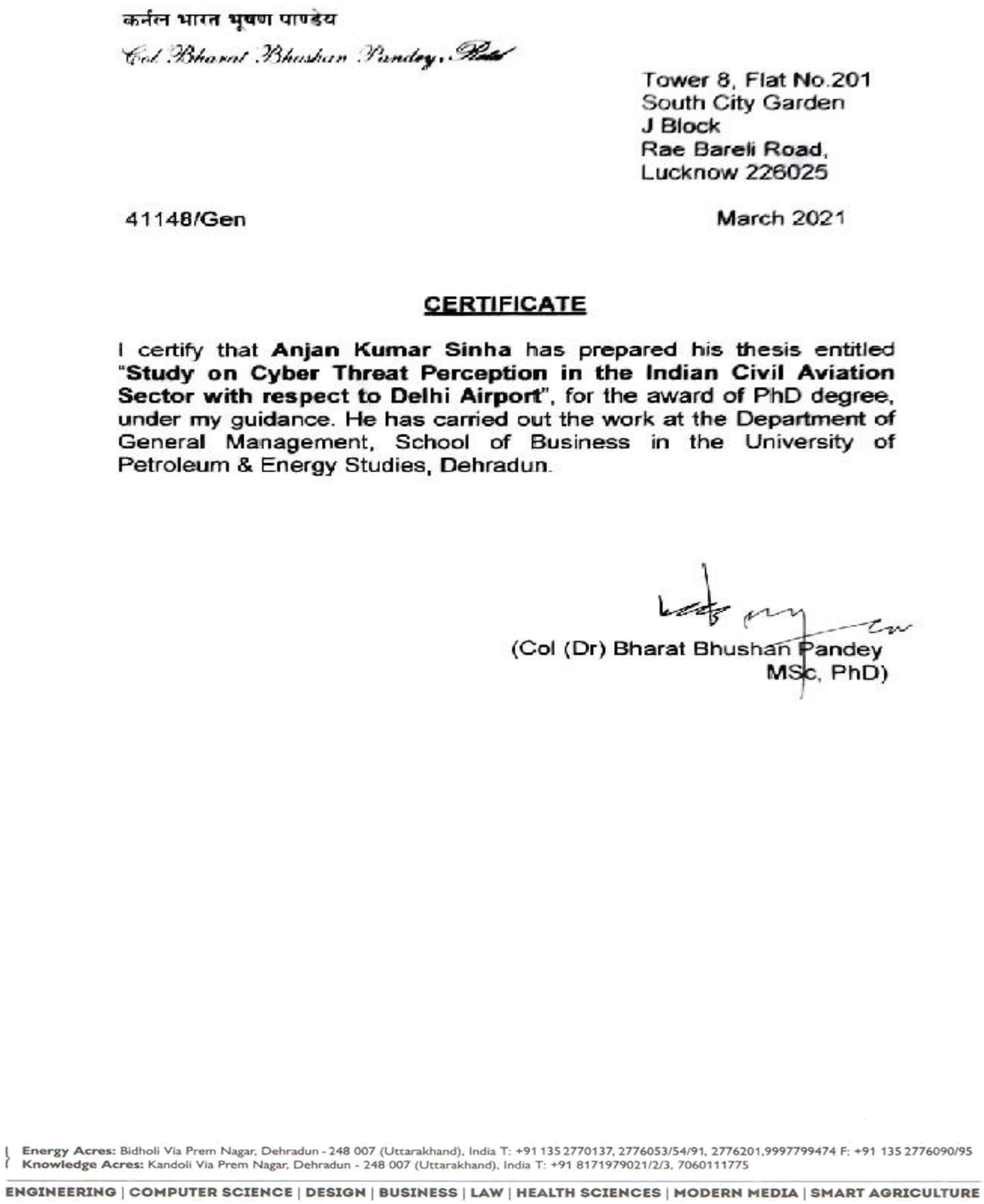
Great Place To Work®
Certified
APR 2019–MAR 2020
INDIA

This is to certify that the thesis entitled “**Study on Cyber Threat Perception in the Indian Civil Aviation Sector with respect to Delhi Airport**”, is being submitted by **Anjan Kumar Sinha** in fulfillment for the award for the award of DOCTOR OF PHILOSOPHY in Management (Aviation) to the University of Petroleum & Energy Studies. Thesis has been corrected as per the evaluation reports dated 15/02/2021 and all the necessary changes/modifications have been inserted /incorporated in the thesis.

Signature of Supervisor

Dr Binod Kumar Singh
Assistant Professor - Selection Grade
Department of General Management,
School of Business,
University of Petroleum and Energy Studies, Dehradun

Date**:** 30 March 2021



कर्नल भारत भूषण पाण्डेय

Col. Bharat Bhushan Pandey, Retd

Tower 8, Flat No.201
South City Garden
J Block
Rae Bareli Road,
Lucknow 226025

41148/Gen

March 2021

CERTIFICATE

I certify that **Anjan Kumar Sinha** has prepared his thesis entitled "**Study on Cyber Threat Perception in the Indian Civil Aviation Sector with respect to Delhi Airport**", for the award of PhD degree, under my guidance. He has carried out the work at the Department of General Management, School of Business in the University of Petroleum & Energy Studies, Dehradun.

(Col (Dr) Bharat Bhushan Pandey
MSc, PhD)

ABSTRACT

08 Mar 14, Malaysia – MH 370 Airliner disappears after take-off from Kuala Lumpur for Beijing and till date what exists is multiple theories from being shot to hijacking of airplane and so on. 24 Mar 2015, German wings 9525 another fatal crash in Alps, cause-suicide mission by Co-pilot, Killing all 144 passengers on board. The study gets motivated by these two incidents and many more of such types like that of 9/11 wherein technology takes a back seat however advance it may be with inbuilt redundancies to be predominantly driven by the man behind the machine. Thus, to understand whether safety-security of Airports is only a tech component or to do something from a human intention, attitude and behavior as given in social foundations of Airport security. Thus, there is a requirement to study the cognitive perceptive minds in enhancing the Aviation security. Protection Motivation theory (PMT) by Rogers in 1975 included these concepts in depth and this theory has been adequately tested and studied with respect to study of human psychology, fear, and reprisal. The key issue in the Protection Motivation Theory (PMT) points at how fear of contact can itself affect perception, behavioral preferences, behaviors, and health. COVID-19 pandemic has shown that how fear can bring down any business. Within three months of restricted Air space big names like Virgin Atlantic, Jet suite has filed for bankruptcy. Centre of Aviation (CAPA) in its March 20 report asserted that by May 20 most airlines will be bankrupt and primarily due to lack of collaboration of governments and the national self-interest. Cost of security though not infinite however difficult to measure especially in complex business of Aviation. Available data talks of technical know-how of managing threat perception however there remains the biggest challenge in getting into a human mind and understanding security from their perspective. The biggest stakeholders in the aviation sectors are the people travelling. Hence an effort has

been made to understand people flying through the Delhi Airport (being the largest in India) to understand Cyber threat perception of Indian Civil Aviation. The IOT and operational technologies in the Cyber-Physical systems is evolving despite that Aviation Industry remains vulnerable to wireless technologies in today’s emerging cyber-crime threats. Extensive literature survey was done to identify the gaps in studies i.e., to understand Aviation Cyber Security from the cognitive domain.

A mixed study of qualitative and quantitative wherein survey questionnaire is sought among 297 travelers and past studies of human behaviour and cognition using PMT is applied as to see whether making people more aware of the threats will we be able to change security intentions of people? The factors chosen from the past study does appear significant in the field of aviation too and hence we do deduce that people do appreciate the nature of Cyber threat in Civil Aviation.

A mixed form research wherein variables are deduced through literature survey and ascertained. A mixed survey is carried out online through snowballing effect and also, through classroom participation from the passengers flying through Delhi Airport. The responses are collected are cleaned and factors ascertained using Principal Component Analysis and Factor analysis for reliability measurement and validation. For Research objective one, data analysis is done using regression analysis based on P-values and R^2 and hypothesis testing. Structural Equational Modelling is used using Partial least Square to come to conclusive model making that was the research objective two. Statistical tools such as Factor analysis for variables and their relationships, Hypothesis testing using SPSS and PLS SEM for modelling/Framework has been used.

There are numerous bodies and agencies working towards freezing of framework for Aviation Cyber Security however none has come to conclusive so far. Further, all frameworks seek for mitigating technical challenges and functional procedures however the human behavioural aspects on mitigating cyber threats are rarely studied and a theory related to it specifically in an Aviation sector. The governments across have taken large measures in ensuring the safety of critical asset. This study helps us and to make one realise that Air travel are no longer for leisure and business rather an important transportation model, safety of which is also in hands of the people using this mode.

The study leaves a scope for future researchers and academicians and even the government regulatory bodies to talk more openly about Aviation Cyber security. There remains a huge task in creating awareness among masses and also to evaluate the cost of security in this field which is highly relevant for business sustenance. COVID-19 has been explicit in getting the business of Aviation down globally and it is nothing but the same theory of PMT which is in practice and the same can only be revived through enabling threat perception. Further, Artificial Intelligence and block chain security are the technological aspects to make the entire system more robust however man behind the machine will always be leading factor in predominant security even in Aviation Industry.

ACKNOWLEDGEMENT

With deep sense of gratitude, I wish to extend my sincere thanks to my esteemed supervisor Dr. Binod Kumar Singh for his guidance, intellectual inputs, and constant motivation throughout the course of the study. I feel highly obliged to them for devoting a lot of precious time in going through this work and making a number of creative suggestions. Their love and affection have really gone a long way in the successful completion of the study.

I am thankful to Col (Dr) Bharat Bhushan Pandey, Dr. Nikhil Kulshrestha, and Dr. DP Singh Professor, School of Business, for his friendly disposition, and constant encouragement and moral support, which always inspired me to go ahead in my research work with confidence and zeal.

I highly appreciate the cooperation and affection extended by all the faculty and staff of School of Business, University of Petroleum and Energy Studies, which has made my stay very productive and beneficial here. My friends in the department deserve my warm thanks for their wonderful helping attitude, and for providing a jovial environment at the workplace.

I cannot signoff without acknowledging the contribution of a large group of colleagues, friends, Staff at Delhi Airport and respondents for responding to my questionnaire and cooperating fully.

My efforts could never meet the success without the blessings, incessant support, love, trust and patience of my parents, siblings, Children and special thanks to my wife *Shrawani* for her constant encouragement, moral support and appreciation.

(Anjan Kumar Sinha)

CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

S. No	Abbreviations	Full Form
1	ATC	Air Traffic Control
2	ANSPs	Air Navigation Service Providers
3	ACRP	Airport Community Research Programme
4	AT CTI	Air Traffic Collegiate Training Initiative
5	AIAA	American Institute of Aeronautics and Astronautics
6	ATM	Air Traffic Management
7	ATM-CNS	Air Traffic Control, Communications Navigation Surveillance
8	AOP	Airport Operations Plan
9	ACRP	Airport Cooperative Research Program
10	AAGR	Average Annual Growth Rate
11	ACARS	Aircraft Communication Address and Reporting System
12	AMS	Aircraft Messaging Security
13	ATM	Air Traffic management
14	ATS	Aviation Transport System
15	ACI	International Airports Council
16	AAI	Indian Airport Authority
17	BYOD	Bring Your Own Device
18	CPNI	Centre for the Protection of National Infrastructure
19	CRMAP	Cyber Risk Management Assessment System
20	CRMAT	Cyber Risk Management Analysis Tool
21	CSCMM	Cyber Security Capability Maturity Model
22	CCC	Computing Community Consortium
23	CII	Critical Information Infrastructure
24	CNS / ATM	Communications, Navigation, Observation Air Traffic
25	CPS	Cyber-Physical System
26	CIA	Central Intelligence agency

S. No	Abbreviations	Full Form
27	CISF	Central Industrial Security Force
28	DDOS	Distributed Denial of Service
29	DIPP	Department of Industrial Policy
30	DGCA	Directorate-General for Civil Aviation
31	ECT	Expectation Confirmation Theory
32	ECA	European Cockpit Association
33	ELPT	Electronic Logbook Protection Team
34	EASA	European Aviation Safety Agency
35	EO	Executive Order
36	ECS	Enhanced Cyber Security Services
37	ECS	Enhanced Cyber Security
38	EO	Executive Order
39	FIPS	Federal Information Processing Standards
40	FMS	Flight Management System
50	FAMs	Federal Air Marshalls
51	FSC	Full-Service Carriers
52	FSLTT	Federal, state, local, sub-national and regional
56	FEMA	Federal Emergency Management Agency
57	GDP	Gross Domestic Product
58	IFALPA	International Federation of Airline Pilot Associations
59	IT	Information Technology
60	IQPC	International Quality and Productivity Centre
61	IATA	International Air Transport Association
62	IDS	Intrusion Detection System
63	IPS	Intrusion Prevention System
64	ICAO	International Civil Aviation Organization
65	ITU	International Telecommunication Union
66	IGIA	Indira Gandhi International Airport

S. No	Abbreviations	Full Form
67	IAAI	India International Airport Authority
68	JCG	Joint Coordination Group
69	LAN	Local Area Network
70	KMO	Kaiser-Meyer-Olkin
71	NIST	National Institute of Standards and Technology
72	NAA	National Airport Authority
73	CANSO	Organization of Civil Air Navigation Services
74	OT	Operational Technology
75	PWC	Price Water Coopers
76	PASR	Preparatory Action on Security Research
77	PDP	Presidential Directives Order
78	PLS	Partial least Square Path Modelling
79	STC	Supplemental Type Certification
80	SETA	Security Education, Training, and Awareness
81	SWIM	System Wide Information Management
82	SESAR	Single European Sky ATM Research
83	TTAT	Technology Threat Avoidance Theory
84	TC	Type Certification
85	TAM	Total Airport Management
86	TDF	Theoretical Domain Framework

CHAPTER 1

INTRODUCTION

1.1 MOTIVATION AND OVERVIEW

1. 08 Mar 14, Malaysia – MH 370 Airliner disappears (Nigel, 2014) after take-off from Kuala Lumpur for Beijing and till date what exists is multiple theories from being shot to hijacking of airplane and so on. 24 Mar 2015, German wings 9525 another fatal crash in Alps, cause-suicide mission by Co-pilot, killing all 144 passengers on board (BEA, 2016). The study gets motivated by these two incidents and many more of such events like that of 9/11 attacks on WTO where technology takes a back seat however advance it may be (with inbuilt redundancies to be predominantly driven by the man behind the machine) to look deep inside into greater depths of human mind. Thus, to understand whether safety-security of Airports is only a tech component or to do something from a human intention, attitude and behaviour as given in social foundations of Airport security (Kirschenbaum,2015). Thus, there is a requirement to study the cognitive perception in enhancing the Aviation security. Protection Motivation theory (PMT) by Rogers in 1975 included these concepts in depth and this theory also has been adequately tested and studied in depth with respect to study of human psychology, fear and reprisal.

2. The key issue in the Protection Motivation Theory (PMT) points at how fear of contact can itself affect perception, behavioral preferences, behaviors, and health behaviour. COVID-19 pandemic has shown that how fear can bring down any business. Within three months of restricted Air space big names like Virgin Atlantic, Jet suite has filed for bankruptcy. Centre of Aviation (CAPA) in its March 20 report asserted that by May 20 most airlines will be bankrupt and primarily due to lack of collaboration of governments and the national self-interest. This work examines the trend of fear motivation, behaviours, and behavioral change in the field of aviation. The fear-driving model assumes that there is a non-linear, parabolic relationship-generated fear level and the preparation to follow the proposed adaptive behavior. Protection motivation

theory has been used as a framework for influencing and predicting behaviors such as increasing precautionary measures to prevent security threats, precautionary measures against many accidents in Cyber Security, increasing assertive behavior in interpersonal communication," and increasing intention to engaging in behaviour which relates with the preventions of any conflict.

3. The theory measures the behavior of a person when a person is facing a related threat. With certain occasions (e.g., cigarette smoking is connected to lung malignancy). This conduct is straightforwardly impacted by the "coping reaction, which alludes to an individual's ability to play out suggested conduct (this could be stopped smoking thoroughly, reduce the number of cigarettes per day, etc. Facing the net results of the response of an individual threat assessment and evaluation." (Rogers, 1975, 1983).

4. Threat appraisal "alludes to an individual's evaluation of the dimension of the risk presented by the threat. It comprises of apparent vulnerability (the individual's appraisal of the likelihood of the threatening occasion), severity (the severity of the outcomes of the occasion), and rewards (intrinsic and extrinsic rewards of not embracing a prescribed coping reaction)." (Rogers, 1975, 1983). The second cognitive procedure, "coping appraisal alludes and an individual's evaluation of his capacity to adapt to and turn away the potential misfortune or damage coming about because of the risk involved. It includes efficacy driven by self (the trust of the individuals in order to perform the prescribed conduct on their own), the efficacy of the reaction (the efficacy of the proposed conduct) and the cost of the reaction (the apparent open-door costs-money-related, time, and effort-in the context of the proposed conduct). In the smoking precedent, self-efficacy hints at the trusting the person in his or her ability to stop smoking, his or her response to the medical advantage of not smoking, and the cost of the withdrawal of the side effects that the smoker endures when he or she quits smoking. PMT proposes four things (Rogers, 1975, 1983) that will affect a person's expectations to protect him from any tragic or threatening incident. Variables are as follows: -

(a) The seriousness of the damaging or compromising event.

(b) The probability of occurrence of an incident (vulnerability).

(c) The adequacy of the masterminds of preventive developments (reaction viability)

(d) The limit of the person in executing the course of action to reduce the effect of undermining event (self-adequacy).

5. The apparent severity and the vulnerability are utilized to decide the threat appraisal, which demonstrates the gravity the occasion. Higher threat appraisal shows a diminished probability of maladaptive conduct. The threat appraisal has been connected in numerous health-related investigations. The coping assessment, which includes the efficacy of reactions and self-efficacy, focuses on versatile reactions. It determines whether a person can respond to a threat and find a way to maintain a strategic distance from it. As per PMT, the general assessment about threat can be managed by summing up the factors listed above. Thus, before thinking about possible preventive practices, the individual should first reason that the hazard has a clear impact on the person concerned and that the adverse effects of the hazard outweigh the benefits obtained during the current (maladaptive) behavior. The threat induced by an impression of danger severity and threat probability makes individuals evaluate conceivable coping strategies. This coping appraisal process comprises of three synchronous decisions: -

(a) Conviction about the sufficiency (will something work?) of preventive conduct (reaction efficacy).

(b) An evaluation of one's capacity (would I be able to do this?) effectively start and finish the versatile conduct (self-efficacy).

(c) A gauge of the expenses related to a specific game-plan (reaction costs).

1.2 <u>AN ACCOUNT OF PMT AND COST OF CYBER CRIME</u>

The principles describe how people are motivated to react on perceived threats in manner of self-protection. The safety incentive principle is used here to improve cyber threats associated with the aviation industry and “to develop public policy to minimize the risks involved” (Gopalakrishnan et al,2015). PMT further demonstrates the security policy enforcement of the research and information system. The role of PMT in Information Security, Cyber-Crime and threats is growing and needs to be understood in a correct framework to be applied in Aviation Cyber Security framework. In today's world, cyber threats are directed at the country's organizations, governments, and people. Report of Accenture 2019 on the costs of Cyber-Crime by industries and countries are tabulated and attached as **Appendix 'A'**. It is interesting to note that ***Air travel does not features independently*** and **so the cost of *Cyber Crime in India***. In this report and it is these two aspects which a researcher wants to highlight in his study. Worldwide estimated budget for Cyber-Crime in 2014 is approximately $445 billion (source: Economic effects of Cyber-Crime, Center for Strategic and International Studies, 2018). Range of steps to combat the crime and the threat have been taken by multiple organisations. Threats are growing and need for security and the defense of the global cyberspace aviation infrastructure increases day by day (Frei, 2015). Cyber threats are data theft and integrated loss, cyber-attacks, which are versatile and extensive in nature. "Integrated Information and Communications Technology (ICT) systems, wireless technologies to include global aviation systems remain high potential targets of large-scale cyber-attacks in the times to come primarily by script kiddies, white/black-hat hackers and the Anonymous." (Martin et al,2016)

As innovations advance rapidly, so too are risks. Aviation industry are at significant risk if it does not have the appropriate IT security systems in place to address this growing threat. Lot of meaningful work and design are under incorporation to build robust internal aviation security processes. Few organisations internationally are International organization of standardization (ISO), Federal Information Processing Standards (FIPS), National Institute of Standards and Technology (NIST) having its own validated framework, European Union Agency for Cyber Security (ENISA) apart from Federal Aviation Administration (FAA) and International Civil Aviation Organisation (ICAO) as regulatory bodies.

1.3 BUSINESS PROBLEM

1.3.1 Neglecting Cyber Vulnerabilities Causes Huge Loss in Indian Civil Aviation Industry

Cyber Attacks on the critical Infrastructure or any business cannot be predicted for its range and depth. The time taken to respond, mitigate and recover from the situation would estimate the losses. Thus, the criticality of Cyber-attack would determine its range and depth. In Aviation business, few of these may lead to:

(a) Shutting down Airport Terminal for few minutes to time taken to respond and recover.

(b) Delay in boarding, take-off.

(c) Delay in ticketing.

(d) Shutting down runway lights.

(e) In flight emergency.

(f) Baggage/Cargo management

(g) Fraudulent booking

(h) Fraudulent Credit/Debit card payments etc.

(j) Data theft

Although, Aviation economics is highly challenging to understand because of its too many complexities on Lease rent, Taxes & Insurance; strategy for cyber threat mitigation would be by educating People, Process and Technology associated with Aviation Cyber Security. An Illustration is made and given down below. Two examples have been taken to identify the cost of business of Airport and an Aviation from Indian Civil Aviation.

ILLUSTRATION 1

Table-1.1 Delhi International Airport Limited (DIAL)

Estimated Earnings (EBITDA)	1886.34 Crs
Profit after taxation	508.86 Crs
Total Passengers Handled	48.92 Million
Total Cargo Ferried	7,87,168 Metric tonnes
*Profit per ton of Cargo ferried	Rs 3232 per metric tonne
*Profit per passenger Handled	Rs 53 per passenger
Assuming only 50%profit for passengers handled and 50% profit from Cargo) *	
Profit per hour of operation	Rs 5,80,890/- per hour@ 5585 passengers per hour

(Source: Annual Financial Report of DIAL of year 2015-16 as on 31 Mar 2017)

ILLUSTRATION 2

Table-1.2 Indigo Airlines

(Rupees in Million, Except Earnings Per Share)

Particulars	2017-2018
Revenue from operations	230,208.86
Other Income *	9,468.57
Total Income	239,677.42
Profit before tax	31,266.76
Current Tax	(6,689.83)
Deferred tax credit / (charge)	(2,153.22)
Profit after Tax (PAT)	22,423.75
Other Comprehensive Income net of Tax	2.52
Total Comprehensive Income	22,426.26
Earnings per equity shares of the face value of Rs. 10 each	-
Basic (Rs.)	60.04
Diluted (Rs.)	59.91

(Source: Annual Financial Report of Indigo Aviation of year 2018 as on 31 Mar 2018)

1.3.2 Analysis

The analysis of above is that if DIAL closes for an hour the accumulated loss is not only for Rs 5.80 Lakhs as above but also loss of one flight carrier of Rs 19 Lakhs and other Aviation and other business partners.

Table 1.3 Airport costs per hour of operation

Airport	Revenue 2017-18 (in crores)	Per hour cost (in crores) *
DELHI	9,2740.25	10.58
MUMBAI	35,452.24	4.047
HYDERABAD	8,721.21	0.99
KOLKATA	12,976.96	1.481
BENGALURU	1,551.70	0.177

(Source: Annual Financial Statements 2017-18)

1.4 PROTECTION MOTIVATION THEORY IN ASPECT OF CIVIL AVIATION

The study deems protection motivation principle as a platform for its applicability to Aviation cyber security in Indian Civil Aviation focusing on human processes as they always remain centric to technology evolution and practices. Travel, leisure, safety and fear doesn’t co-exist however in current scenario of threats across all sectors, a conscious perceptive mind can evade maximum possible threats:

(a) **Perception Management:** The action of people is conditioned by its perceptual nature. Passengers being the biggest and main stakeholders in any travel industry need to contribute maximum through their cognitive domain in safety of the processes. Air-accidents and fatality are closer than any other form of travel.

(b) **Cyber Threats:** Cyber threats today co-exists whether attacks on financial institutions or the Internet of Things (IoT) devices & web, Cloud and Cyber-Physical systems (CPs) or to any functioning network that can be violated regardless of the physical presence of the threat.

(c) **Cyber Security Behavior**: This refers to a conscious behavior of people to enhance digital data protection in today's environment.

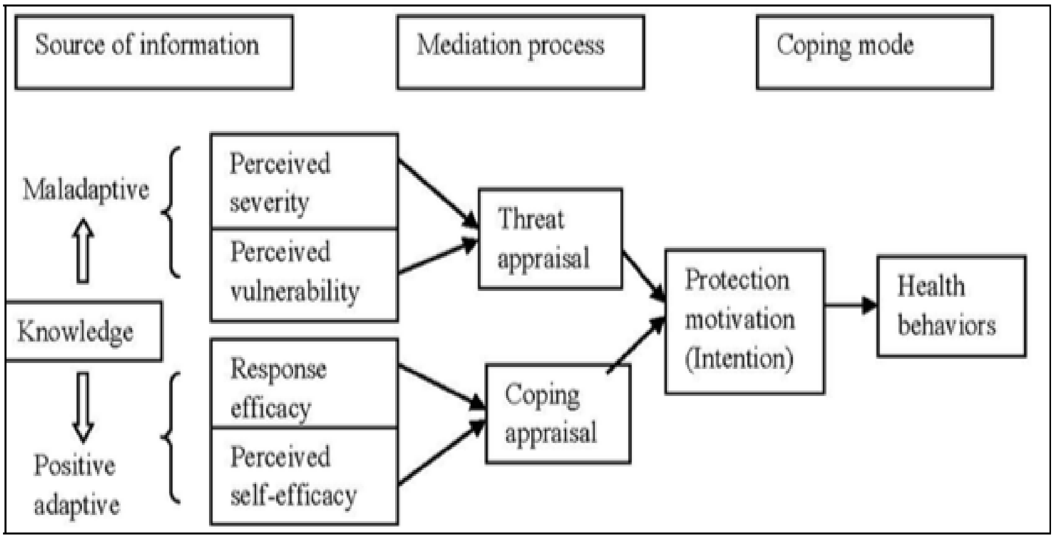
Threat assessments and online protection behaviors based on the PMT "involve threat assessments through online security protections" (Tsai et al,2016). However, previous studies on subject have given conflicting results. In few studies, the *severity of the threat* was an influential factor in predicting security-related protection, while another few deduced that the severity of the perceived threat is not an essential factor in predicting the intention to implement online cyber -protection. Recent researches have extended threat scope, adding variables, multiple variables combined to measure threat determination. The level of threat has also been determined to be influenced by the severity and vulnerable to attack. Online safety amid commercial aviation began a decade back, till then the redundancy factor of safety was considered as a fail-safe measure for industry systems. Use of ICT in aircraft systems and its vulnerability can disrupt the sector heavily. It has not happened in past primarily due to lack of awareness among the black hat community (Martin et al,2016) however past three to four years there has been a lot of interest developed among the hackers, grey hat and techhies due to centrally organized competition and games like capture the Flag (CTF) and bounties associated with identifying vulnerabilities.

The cloud and the aviation systems have layers of protective measures still it is the man behind the machine playing the key role in security and safety. The effort in developing a comprehensive strategy world over for the aviation sector is under progress and constantly evolving still the universal guidelines and protocol is waiting to emerge. The aviation sector still is one of the biggest contributors to the country's economy to the range of 2%-5% globally (NCAER,2012). Further, not only government and the business players it becomes imperative for all people to ensure safety of this sector and this can be done by creating awareness at a massive scale and improving the behaviour of people by getting the concepts of safety and security into their sub-conscious minds.

1.5 ORIGIN OF PROTECTION MOTIVATION THEORY

The PMT was formulated in 1975 and it developed on the emotional, attitudinal and behavioral improvement focus of the perception paradigm to provide understanding the interests of threat vis a vis well-being of individuals. In 1983, "PMT" was revised; the theory comprises of three cognitive processes: *knowledge processing, cognitive training and ways of coping*. 'Boer and Seydel' (1996) explained the primary structure of the theory and the factors associated with it: *strength, vulnerability, effectiveness of reactions, self-efficiency, safety motivation (expectation) and defensive behaviour*. Ronald Rogers has designed it to make it easier to understand why people are reacting to possible threats to their well-being and health. The theory suggests that both human and environmental factors are engaged together in defensive activities and that the impacts of these factors are managed through a specific cognitive procedure.

Such cognitive techniques are suggested to identify from the predicted direct relation of a passionate threat to defensive reactions. To this point, this hypothesis has to a large degree, been related to the disclosure of protective behaviors found in the field of medical services, such as wearing sunscreen to prevent malignant skin growth from obtaining empiric help. In "PMT," Rogers portrays the danger as a "private group," with obedience to both action and response (1975). Thread may be seen as an extension between the expectation of danger and the defensive operation needed to respond to the circumstances. The word thread intrigue is used to represent this relation or to illustrate the use of a person's apprehension about an event or subject to a precautionary reaction. A comparative interpretation indicates that the threat intrigue attempts to communicate a possible threat to the well-being of an individual, both by describing the danger in detail and by suggesting a strategic distance from or minimizing the effect of the danger.



(Source: Rogers (1983)

Figure 1.1: Model of Protection Motivation Theory

Figure 1.1 shows the segments of the PMT as shown in Rogers (1983). The first part involves environmental and intra-personal determinants that make proposals to the individual in relation to potential exploitation threats, potential defensive choices and triggers why the individual should or should not engage in a defensive response. Data from the environmental factors include discussions with or on behalf of others, such as relatives, neighbours, the media or the police, on threats to exploitation and possible defensive reactions (spoken opinion). These information may also include the use of defensive reactions (observatory learning). Author distinguishes between two intra-personal sources of information: identity factors, including related factors. These "intra-personal sources" of information suggest that such related participation in the use or use of defensive activities, as well as their identification, may lead to the awareness of possible threats and the interpretation of defensive reactions. Commonly, the information given above provides an individual with the normal learning of possible defensive reactions. In the light of the information provided, the individual is informed of potential threats and this intrigues defensive reactions due to the threat presented. Rogers was aware of the two subjective intervention structures by which this assessment is carried out by the individual. In the maladaptive response process, which is more generally referred to as the hazard assessment process, an individual chooses the potential favorable circumstances of proceeding along the current path despite monitoring the potential risk.

Cognitive reactions to potential threats may be reinforced by objective considerations. Although the risk assessment process helps the individual to determine the hazards of the potential threat, an adaptable response plan or an extension of the assessment process empowers the individual to recognize possible solutions that might protect the individual from hazards.

According to Rogers, the individual initially considers whether a prudent response would more likely control a specific danger (reaction viability) and whether a defensive response is likely to be used in such a way as to convince them to thwart a potential hazard (self-adequacy). The person considers the typical cost of using the defense response [response costs]. This includes both 'monetary and social expenses' related to the acquisition or use of defensive reactions. In the light of the assessment of these variables, the person must determine whether the proposed defensive response will be both physical and realistic in order to protect them from the threat. "A person may identify a potential threat but a slight defensive activity at the expense of a defensive response. This prevents individuals from taking an active part in a defensive response. Rogers recommends that" protection motivation "ultimately arise in at least one coping mode.

1.5.1 Theoretical Premise

There have been various security theories such as the Expectation Confirmation Theory (ECT), Technology Threat Avoidance Theory (TTAT), Social Learning Theory on the application of behavioral sciences to counter technology change and the risks it has identified. The aviation sector is facing numerous Cyber Security challenges due to multiple layers of Cyber-Physical networks and related risks due to high vulnerability (Krishna,2013) being a very complex industry with multiple stakeholders. Other research has also shown that most cyberspace threats come from insiders, and risk mitigation can be successful through clear protocols and a high level of awareness. This research uses the PMT as its theoretical basis. The PMT was developed by Rogers (1975) to define the mechanism of fear appeals. Moreover, the theory has been revised over the years to clarify general persuasive communications (Boer and Seydel, 1996). PMT suggests that fear-inducing communication can affect perception, behaviors and intentions.

Scholars in the past have used PMT as a tool for health-related problems such as reducing drug consumption, increasing disease prevention in healthier lifestyles (Boer and Seydel, 1996) and anti-smoking initiatives. PMT has recently been used to tackle information security concerns. PMT is one of the most predictive theories to forecast intentions to participate in protective behavior (Anderson and Agarwal, 2010; Safa et al. 2015). Major studies using PMT are summarized in the table given at **Appendix 'B'**.

1.6 THREAT APPRAISAL PROCESS

The accompanying factors might be useful in estimating the threat assessment procedure of the PMT that applies to criminal exploitation and protective practices.

(a) **Intrinsic Rewards and Extrinsic Rewards:** Natural and external rewards suggest that the benefits of an individual can be understood by continuing to participate in rehearsals to a potential hazard. The two advantages in general health mean that one should appreciate the benefits of not engaging in the defensive leadership for example, "decide not to quit the pretense of smoking because they feel that it is an attractive social feature". In any case, it is difficult to envision a situation in which one might have a desired place to deliberately engage in criminal violence. Effects of both incentives are likely to be limited and focus on particular settings that may be of benefit.

(b) **Severity and Vulnerability:** "Severity" tests enable individuals to decide their actual probability and probable nature of "crime victimization". Possible measures to measure the severity of criminal victimization depend on individual attributes. Criminal victimization "reveals the effects that involve physical and emotional disabilities, financial misfortunes. As a result of therapeutic administrations and missed work, social damage associated with injured individual markings, and damage to personal satisfaction, the threat of severity is likely to change significantly across the board, as indicated by their conditions and experiences.

(c) **Fear-Arousal:** Fear-arousal in the PMT has a comparative relationship with the severity and vulnerability section of the risk assessment process. Singular evaluations of vulnerability and severity can contribute to an increased response to fear, which can fuel vulnerability speculation. The mental feeling of fear is a fragment of the "PMT" after the use of defensive reactions. Proportions of fear arousal should be linked to the inclination of the person to 'stress' or to 'troubled' reactions identified with concern about a particular danger of criminal exploitation.

1.7 COPING APPRAISAL PROCESS

This procedure gives a cost viable investigation of "explicit hazard from criminal threats, the adapting appraisal process," it gives a financially savvy examination of prescribed, ensuring steps to foresee or mitigate unlawful dangers. In the cost- effective inquiry, the person considers the apparent capacity of the provision and it's first of its kind limitations to eliminate or reduce a possible unlawful risk, while also considering the financial and social costs of the use of that protective mechanism. "Self-adequacy" points at a person's conclusion that the consequences of a given criminal danger are turned away or reduced. Many protective effects require a person to ensure that they are used consistently or that require exceptional expertise (for example, using a weapon).

1.8 THE ONLINE SAFETY QUESTION

The supposed theory of PMT has been chosen to explain how and why individuals began to behave defensively. The PMT recommends that threat and coping assessments be carried out in order to protect them. Assessments are regulated by obvious vulnerabilities and potential loss as for risky behaviours. The internet security work can be interpreted from a PMT perspective. 'Liang and Xue' (2016) suggested a technology hazard evasion theory based on the safety incentive principle, a health convection model, and a risk analysis. It was found that both threat assessments were seen as helplessness, severity, and coping (protecting adequacy, defending costs, and self-efficiency) were noteworthy indicators of computing.

Some studies have shown that “trust in security behavior (coupling self-efficacy) is associated with security threats and threatening helplessness.” (Alan, 2015). According to ‘Johnston and Warkentin (2012)’, that “expresses social impacts as social norms, alluding to the expectation of how others behave”. Moreover, a large amount of such investigations has been undertaken in an authoritative setting. "In this case, we accept that theoretical concepts are better suited to dealing with social influences on defensive behaviour. Various examinations have resulted in distinctions between components that influence the security protection. In this review, we look at these 5 variables in a standardized PMT model to explain what individual safety goals for personal computer usage. Studies have shown how a PMT bound together can be used to decide on the means taken by individual to the security they need and prepare for them. In a digitalized world, where data is everything, not following guidelines, being security consciousness avoids business loss, notoriety and other safety issues. Analysts used PMT, together with other models of social theory, and recommended rules to improve the consistency of Internet service Providers (ISPs), (Liang and Xue). There is an extension for further research in the area. Research may lead to the discovery of a change in the Protection Motivation Behaviour (PMB) with a change in societies.

1.9 THREAT APPRAISALS AND SECURITY BEHAVIOURS OF PROTECTION MOTIVATION THEORY

Threat assessment has been adopted in PMT to maintain online security. However, previous research has found a mixed investigation that acknowledges the impact of threat assessment on protective behavior. Intensity of threat in specific investigations is a security measure. It was an important indicator. Studies have shown that the severity of the threat is not an important indicator of the goal of implementing infection protection. To test the impact of threat assessment, threat intensity testing includes the fact that a special review of internet usage and securities associated will induce the intensity threat and the secured protection of protocols and devices will lead to critical response. Past experience (with contamination in this situation) was excluded from the original PMT model. Although Rogers (1983) proposed this variable in the PMT model, some tests have been omitted. In a study of graduates, past experiences with infectious infections are expected to be used primarily to protect against targeted infections. In this study, past experiences imply a person's experience in online threat management; thus, it is associated with an important aspect of risk determination.

1.10 IMPLEMENTATION OF PROTECTION MOTIVATION THEORY

As per "PMT," an individual has a protection expectation which is persuaded in light of apparent threats or risks (Rogers 1975). As indicated by Rogers, such motivation to react is a result of a progression of "cognitive meditational forms" that include cognizance of threats and assessment of the efficacy of coping reaction factors. Explicitly, these procedures "assess the information accessible on observed severity of the threat (coping reaction efficacy), and the individual's apparent capacity to cope." The theory proposes that an individual is better equipped to judge when s/he trusts "a prescribed coping reaction can adequately avoid a threat that appears to be hazardous and liable in occurrence. One prerequisite for this procedure to work is that a subject must almost certainly grasp an occasion, and whether it is a threat. Perceiving the significant job of those "cognitive meditational forms" in the fear offer communication that "had been observed to be commonly viable in delivering frame of mind change" in points, for example, "cigarette smoking, dental cleanliness. This methodology would enable us to comprehend whether "PMT" keeps up its utility in supporting information security preparation as it had been utilized and approved in different fields.

As per "PMT", subjects would not be significantly spurred to learn and put vital standards and practices if they see the probability of a threat against their current practices. In this manner, subjects learn to be mindful of their current convictions and discernments about possible security threats. As indicated by the “PMT”, subjects are significantly persuaded to learn secret phrase points than they originally were after they have experienced this activity since they presently ought to have acknowledged the threat and its probability to occur. Additionally, it is expected that subjects are better persuaded to learn other security mindfulness subjects too. This is because when a subject is tested on the part that they believe they have the most experience and certainty to manage. One ought to be persuaded to gain proficiency with the suggested methodologies and standards for those parts that they even have less experience and certainty to adapt to adequately. Since motivation to learn is frequently remarkably corresponded with the learning results, subjects would be expected to show better learning results better the individuals who are instructed with a “PMT” driven methodology.

1.11 ALTERNATE THEORIES STUDIED TO ASCERTAIN THE SUITABILITY

This section deals with various other psychological theories such as perception theory, psychometric studies, integration, and behavioral change theory.

(a) **Theory of Perception**: It focuses on the point of view of the individual at the end of the reaction to the situation and conditions. Analysis of personal conduct towards the dominant circumstance or situation in which an individual responds or behaves. There are two types of perception theories (Nordfjærn & Rundmo, 2015):

(i) **Theory of Self-Perception**: The individual learns to understand their behaviors, feelings, and other personal states better by often assuming that they are witnessing their actions and the circumstances in which that actions happens.

(ii) **Theory of Cognitive Perceptions**: This happens when a person holds more than two opposing beliefs, values and ideas that may contradict values, beliefs and behavior. This theory states that stress or psychological disorder is the result of conflict between actions or ideas. The process of accepting reality is an important part of coping with the problem.

(b) **The Psychometric Paradigm:** analyzes the psychological stressors- problems encountered. Cognitive stress can be contextualized with the situation of aviation personnel or employees, such as 'Pilots, Engineers, Cabin Crew and ATC. 'Psychometric research concentrates on human attitudes, acts, cognitive processing and emotional processes in the diverse world of aviation systems. One's effectiveness is generally seen in a personalised way of self- expression of communicating with others, and in one’s values. Thus, being successful adheres to a healthy state of mind capable of being decisive and yet comfortable. Soft skills related to executive functions; ability to lead a team, ability to prepare and coordinate, ability to make decisions particularly in difficult circumstances, emotional maturity, communication skills interpersonal skills. Psychological paradigms of professionals-pilots, safety personnel and Aviation human capital considered to be of the utmost importance. Behavioral change theories clearly discuss the "individual behavioral change" of the situation; the situation may be "environmental, personal and behavioral characteristics." Activity models are more comprehensive and oriented towards the recognition of psychological causes that describe or predict a particular action. The transition explanations are mostly process-oriented and are usually aimed at improving actions. Each theory or paradigm of behavioral modification relies on different aspects in trying to describe behavioral changes. The proposed integration involves the combination or linkage of proposals from one or more hypotheses to a large, coherent and cohesive set of propositions. In certain instances, the principle of commonality is focused on propositional incorporation, and in others, it requires the convergence of competing theories. The most popular method of integration consists of the combination of social regulation and social learning theories. They also argue that there is an increase in the level of explanatory strength proportional to that of every principle together and that their greater representation in clarified the forms of illegal behavior. The selection of above theories and their effectiveness into our proposed study remained shallow vis a vis PMT which covered larger scope in assessing threat identification and cognitive processes. Further all propounded by these theories can be seen from the perspective of PMT. The aim of this study is to discuss how PMT can be used and extended to educate larger masses in developing a cognitive aviation cyber security behaviour in identifying and averting a cyber security related aviation incident. This leads to the research problem and questions for the study.

1.12 RESEARCH PROBLEM

Protection Motivation Theory framework has not been applied in the Aviation Cyber Security.

1.13 RESEARCH QUESTIONS

1. What are the factors affecting perception management of Aviation Cyber Security?
2. How Aviation Cyber Security studies can be linked with Protection Motivation Theory framework?

1.14 RESEARCH OBJECTIVES

Based on the need and scope of the research, the following are the precise objectives of the study:

RO1- To ascertain the identified factors of Protection Motivation Theory applicable for Aviation Cyber Security. This can be explored through various questions given as under:

(i) Does perceived threat severity affect Aviation Cyber Security?

(ii) Can perceived susceptibility affect Aviation Cyber Security?

(iii) Will prior experience with online safety hazards affect Aviation Cyber Security?

(iv) Do self attributes affect Aviation Cyber Security?

(v) Will demographics (gender, age, education) of the passengers affect their Aviation Cyber Security behavior?

(vi) Does frequency of flying affect Aviation Cyber Security?

RO2- To develop a framework using Protection Motivation theory for Aviation Cyber Security.

1.15 CHAPTER SCHEME

Chapter 1, Introduction: This covers Protection Motivation theory, its origin and development and use in various fields and applicability in Aviation cyber security comparison with other theories such as Perception Theory, Psychometric paradigm, Theories of behavioural change.

Chapter 2, Literature Review: This includes detailed literature on selected issues related to aviation cyber security, various protocols around the world, threat perception and behavioral changes to mitigate technological challenges through perception management.

Chapter 3, Overview of global Aviation industry and vulnerabilities in Cyber Space including Delhi Airport: This chapter has been provided with an analysis of primary market players, the profiles of their companies, key comments on recent developments and market strategies. This chapter discusses the global perspective of Civil Aviation sectors, the Aviation industries issues, the Indian Civil Aviation and the effects of cyber vulnerabilities in the sector.

Chapter 4, Cyber Security and Challenges: International Protocols and Studies on Aviation Cyber Physical Systems: This chapter has been presented with methods, procedures, regulations, protection initiatives, safety protocols, risk reduction approaches, protection assurance and recent developments, including details of unfavorable cyber-attacks. In this we discuss the concept of cyber securities in the aviation industries, cyber resilience in the aviation sectors, the reality and challenge of next generation air traffic managements: the ADS-B scenario, Cyber Security challenge for the Aviation industries, Cyber threat to internal operation of Airports, the study of global pilots, etc.

Chapter 5, Research Methodology: This chapter has been provided with the Research Methodology, Instrument Creation, Questionnaire, Statistical Inference Techniques adopted in the context of this study.

Chapter 6, Data Analysis & Interpretations: Covers data analysis and application of techniques such as the reliability check, multiple regressions, and dimension reduction factor analysis to render a structured equation model as per given context or variables under cyber security in the aviation perspective.

Chapter 7, Findings, Conclusion and Suggestion: This chapter summarize the finding; recommendations and conclusions of the research project.

CHAPTER 2

LITERATURE REVIEW

2.1 LITERATURE REVIEW

Literature review based on selected four themes on subject was carried out in relevance to the study. The themes concentrate on Cyber Security, Aviation/Airport Cyber Security, Airport security and online behaviour and perception management. A total of 98 research papers and reports have been studied and in addition large number of web portals and news on subject. The details of literature surveyed are tabulated below:

Table-2.1 Total Paper/Article Reviewed

Theme	Research Papers	Articles	Other Supporting Documents	Total
Airport/aviation security	05	5	9	24
Cyber security	7	12	4	23
Cyber security in Aviation sector	14	7	18	39
Online behavior	10	-	2	12
Total	36	24	33	98

(Source: Researcher Own)

Previous studies have shown that looking after only technical aspects of cyber security cannot solely be relied upon for a secure cyber environment, and it is human perceptions, their intentions to remain secure promulgated into their attitude and their behavior and the measures it adopts should also be taken into Consideration. Protection Motivation Theory is one of the most insightful theories for predicting intention to participate in defensive behavior (Safa et al., 2015). The theory sets out a great deal of detail in stimulating human minds and awareness for an overall secure environment by recognizing the fear appeal for attitudinal or behavioral change. However, the threat, spread of cyber security and its consequences also have a detrimental impact on human minds to perceive it as a danger.

As we study this aspect, we are witnessing a global pandemic of the CORONA virus that has unsettled the world economy in 2020 and, most importantly, the airline industry. It is therefore necessary to identify and resolve the threat vectors by involving the largest stakeholder, making people more aware of their consequences, and ensuring that people change their attitudes and actions to integrate security awareness into their cognitive minds and daily activities. These are shown in above table.

2.2 DETAILED LITERATURE REVIEW FROM VARIOUS SOURCES

Research Paper on Cyber Security in Civil Aviation by Joint Coordination Group (JCG) of the United Kingdom Center for National Infrastructure Protection (CPNI), 2012 emphasized on:

(a) Building awareness of the general vulnerability to Cyber Security.

(b) Address the overall Cyber Security problem of the 'Aviation System' beyond the boundaries of civil, military and space systems.

(c) Consider the degree to which their efforts can lead to the development of the global information security strategy.

(d) Address the issue of 'Worldwide' versus 'Nation State' regulation, at least in terms of network implementation guidance, information security and internet issues., Fails to give any framework for creating awareness for Cyber Security threat.

(e) Recognize any inconsistencies between the plan established and the research being performed.

Daniel P. Johnson, Honeywell, (2012). The paper stresses upon

(a) Lists various methods of Cyber-attacks.

(b) Talks of inflight entertainment system and how it was crashed by a novice accidently.

(c) Presents various tech uses wherein-

  (i) Navigation charts are uploaded using portable computing systems

  (ii) Auto diagnostic computing devices used by technicians

  (iii) Text messages over radio & satellite

  (iv) Spoofing, Exploitation, Denial of Service etc.

(d) Regulations world Over aviation by ICAO, FAR, NIST 800-53 Rev3 list 337, Little research for organizational controls and Network Intrusion Detection.

Mike Pierides, Brian E. Finch, Rafi Azim-Khan and Steven P., (2015) studied and presented in their paper **"**Cyber Security and the Aviation Sector: Recent incidents illustrate specific danger" through Pillsbury Global Source makes a mention that "Aviation authorities and company leaders are encouraging closer collaboration between government and airlines to defend the sector from cyber breaches and there are no current standard frameworks".

Rebecca C. Leng, (2009) studied **"**Security review of web applications and detection of intrusion in Air traffic control systems", of Federal Aviation Regulations Administration of Department of Transportation of the United States. In its Audit report by KPMG, on "Vulnerabilities in ATC networks" Presents the findings: 'Web apps that are used to facilitate activities on ATC networks are not sufficiently protected to deter attacks or unwanted entry. In fact, the FAA has not developed an appropriate intrusion mitigation system at ATC facilities to track and identify possible information security incidents.

Organization of Civil Air Navigation Services (CANSO), Guide to Information Protection and Risk Management, (2014) presents a paper on

(a) Air navigation service providers (ANSPs) introduced Cyber Security in Air Traffic managements.

(b) ANSP Cyber resources template methodology of risk assessment. ISO 27001-27006, Cyber Security Framework for NIST.

Randall J. Murphy's et al., (2015) studied the FAA Sponsored Airport Community Research Programme,140 (ACRP) and presented Airport Cyber Security Best Practices Guide

(a) The importance of Cyber Security is often not emphasized “outside the IT department of the airport”; Frequently struggle to properly understand the value of information protection while making financial decisions; and staff are still untrained, contributing to bad vulnerability-exposing practices.

(b) Cyber network is an important and growing component of airport infrastructure.

Air Traffic Control Association, United States Government Accountability Office, (2015) carried out research and presented that “The FAA is responsible for managing the national airspace network, which includes ATC systems, policies, facilities and aircraft, and the people who run them. FAA is introducing Next Gen to transform the existing satellite navigation and automation-based ATC-based radar network into one. It is important that the FAA ensures that successful information-security controls are implemented in the design of the Next Gen programs to protect them from threats”.

ATCA by T.Holt et al., (2016) studied and brought out White Paper Executive Summary on “Aircraft Cyber Security and Information Exchange Safety Analysis” for Department of Commerce.

(a) Joining a global plan to combat emerging Information Security threats, In the past 20 years Cyber Security has put itself in the world of operations as an autonomous group.

(b) Incident response today using different awareness tools, procedures and policies may have an effect on Aviation as a whole on a larger scale than the actual Cyber-Attack.

(c) NextGen provides reliable, secure, and reliable flight capabilities for both users and operators who work with volume assurance, disconnection, and safety. This study obtains the highest security risk (SRA)-related technology related to NextGen, direct Aviation Communications and Reporting System (ACARS) and Aviation Access Information Network (SWIM) network.

Case Study by Arctic Wolf networks on Stevens Aviation, a premier US Aviation Services Company highlighted the difficult discovery of Cybercrime while announcing the IT budget and workload, the study emphasizes:

(a) Sophisticated Mission programs require strong protection from cybercriminals.

(b) Young IT employees did not have the resources to focus on cybersecurity.

(c) A cheap solution is needed to protect 100 employees in most areas.

(d) Detecting past offenders in the private security system is difficult and requires an in-depth interview. The only way to find out if this is a violation is to analyze logs carefully and accurately from fire walls, network equipment, servers, and other infrastructure. Data from logs should be connected to users, usually by analyzing Active Directory logs. It is a tedious task to be done daily.

Gopalakrishnan et al., (2013) studied and brought out in a paper on "Cyber Protection for Airports", published in United States International Journal of Traffic and Transport Technologies mentions "criticality of aviation infrastructure which is very vulnerable to physical threats of Bring Your Own Device (BYOD)" and stresses on that there is actually no information protection. Airport requirements in the United States, as the proposed guidelines primarily focus on air control networks. It cites study of Airtight Networks IT professionals identifying major protection issues for correlated personal computers, i.e BYOD (Airtight, 2012).

Cyrille Rosey,(2015) studied for European Aviation Safety Agency (EASA) on its research paper Aviation Cyber Security Roadmap stresses upon:

(a) Four Objectives: Situational Awareness, Readiness, Reactiveness & Cyber Security Promotion.

(b) Four enablers: Aviation CERT, Cooperation, Regulatory Materials & Research and Studies.

(c) Three Research areas: Risk assessment, Difficulty of attack, Security of controls, Gives an outline however lack in detail.

The Boeing (2013) on developing a framework to improve cyber security critical infrastructure stresses upon enabling critical infrastructure cyber security. "Cyber security risks have not affected commercial aviation as frequently as other industries have. There is still a shortage of threats and threat awareness, which needs further cyber education across commercial aviation services (airlines, airports, suppliers and regulators)". Tools for "public protection, Cyber Risk Management Assessment System (CRMAP) and Cyber Risk Management Analysis Tool (CRMAT), to overcome the communication challenge between industry sectors". International Federation of Airline Pilot Associations (IFALPA) (2013); World Body for Airline Pilots, The IFALPA Security Committee has established the risk of a cyber-attack on an aircraft, ground facility or other sensitive aircraft. Infrastructure is to be a major and emerging threat. This paper articulates the threat and suggests ways in which it could be addressed.

Ruwantissa Abeyratne, (2011) studied on "Cyber-terrorism and aviation national and international reactions" in her paper stresses upon the facts that:

(a) Cyber-crimes and cyber- terrorism are constantly being targeted and recognized as a distinct danger that demands focus.

(b) The 21st ICAO Aviation Protection Panel Meeting (AVSECP/21, 22 to 26 March 2010) suggested the adoption by the Council of a new Approved Protocol on Cyber Bill

(c) Threats as part of Amendment No 12 to Annex 17 (Safety) to the Convention on international Civil Aviation (Chicago). It was introduced on November 17,2010 and came into effect on March 26,2011 and will begin on July I ,2011.

Vikram Kunchala and Edward W. Powers, (2015) studied and presented in their paper on **"**Please fasten your seat belts: handling digital aviation support risk" by LLP, Deloitte & Hold; brings out that it is clear that cyber risks are not long for all about protecting corporate data and preserving confidentialities, honesty & quality of data. Cyber threat is a business concern, and used for existing organizations, and cannot be used especially for IT. Cyber accidents can interrupt day-to-day activities, inflict irreparable harm to reputation, and even place lives at risk for the aviation industry.

This sector carries millions of transporting millions of generation security through 100,000 flights a day at 37,000 feet – have a very high stake". The United States contribute $1.5 trillion to total economic activities, and support 11.8 million job in 2012.

Jeff Schmidt, (2015) CEO, JAS Global Advisors; "Cyber-Risk Management in the Aviation Industry" in his interview (www.complianceweek.com), "The aviation industry needs to realize that the approach they took to solving security issues in the past is no longer going forward.

Yeah et al., (2016) studied on "Aviation and Cybersecurity: opportunities Applied Analysis", "The International Civil Aviation Organization's Special Task Force on Cyber Security and the proposed FAA Cyber AIR Act were designed to bridge the gaps in cyber security in aviation". The objectives include the identification of vulnerabilities in cyber security, the assessment of threats and the identification standards of mitigations measure to manage risk to the systems.

Airlines International by IATA Security/Global, (2017) brought out Cyber Crime threat demands robust defense:

(a) If passengers want to maintain trust in the aviation system, it is important for the industry to defend itself from cyber-attacks.

(b) The various entry points and interfaces make it vulnerable to cyber security threats.

(c) Without the benefits of safety-by-design, aviation has a number of critical decisions to make.

(d) Whether to make cyber-attacks mandatory is perhaps the most critical of all.

(e) Reporting and communication is one of the three pillars of IATA's cyber security strategy, along with risk management and advocacy.

Yoann Viaouet, (2017) from Aerospace and Security Research studied and brought out Association of Europe in its “Position Paper of the ASD Civil Aviation Cyber Security Task Force” mentions that “ICAO should coordinate and aggressively pursue a comprehensive Cyber Security, Cyber-Safety and Cyber-Resilience work plan through a new dedicated group with all relevant stakeholders”.

The need for international alignment makes it necessary for cyber securities in civil aviation to be placed at the top of the EU diplomatic agenda and unbalanced rules and regulations for the developments in different regions must clearly be avoided. It is not necessary to prescribe any technical solutions but rather mandate the stakeholders to demonstrate compliance with appropriate security objectives. There should be a ‘ring fenced’ budget for civil aviation cyber security research for both cost efficiency and effective implementation to improve the safe operation of the civil aviation transport system. Emphasized on need for Aviation product security experts, which are very different from IT Security experts. It proposed top objectives:

(a) Identify critical assets (systems, operations, businesses etc.)

(b) Define roles, responsibilities, and processes regarding cyber security risk management.

(c) Define administration and maintenance policies of cyber protections.

(d) Deploy training programs and awareness sessions.

(e) Protect Network and Information Systems.

(f) Regularly assess residual risks through audits of operational procedures, penetration testing and code reviews.

(g) Ensure COTS vulnerabilities management and mitigation.

(h) Deploy Cyber Security monitoring capabilities and Cyber incident management.

(j) Prepare Cyber Security crisis management and data recovery.

(k) Secure external networks and remote sites connection.

(l) Maintain cryptography of systems and networks.

(m) Secure software deliveries and supply chain (e.g., through the use of digital signature).

(n) Establish risk-based development processes for software & hardware.

A report on Aviation Perspectives by Price Water Coopers, (2016) on Cyber Security and the Airline Industry through its four volumes (Vol I-IV) emphasized on:

(a) Introduction- Prevention - Detection-Action**,** Enhanced communication and integration are essential for improving financial and operational performance.

(b) Collecting Forensic data to identify security weakness

(c) Notifying consumers and other stake holders on priority and managing press stories

Juan Lopez Jr. & Deanne W. Otto, (2014) studied and presented in their paper on "Cyber Security Analysis Contents in the Air Traffic Controllers Training Initiatives (AT-CTI) Programme" (www.twoculturalsjournal.org) makes a mention of steps:

(a) To assess the existence and level of integration of cyber security content of Air Traffic University Technical Project (ATUTP) educational programmers.

(b) Results suggest that information security material is almost completely inexistent in the curriculum of institutions participating in the software awareness and emphasized on Study of Cyber Security in school curriculum.

American Institute of Aeronautics and Astronautics, (2013) in an Aerospace Leadership World Forum while giving Framework of cyber security states that: -

(a) This robust, stable and effective network of transport handles more than 2.6 billion of passenger and 48 million ton of cargo in year.

(b) This most efficient transport network carries more than 2.6 billion travellers a year and 48 million ton of freights. The global economic effect of aviation in all is estimates at $2.2 trillion or 3.5 per cent of GDP.

(c) Global economic effect (direct, secondary, mediated, and catalytic tourist valued 3.5 percent of GDP.

(d) Currently, cyberspace is a growing threat: security of the global air traffic system. There is no shared concept or popular policy, priorities, guidelines, delivery frameworks or foreign policies that characterize commercial aviation's cyber protection.

Gil Mulin, (2014) studied on “Guidance for Digital Security in Commercial Aviation-ATA Spec 42 stresses upon that “Public Key Infrastructure set of tools, policies, and practices for Digital Assets. Electronic Logbook Protection Team (ELPT) is taking a phased implementation approach to overcome challenges of PKI”. Spec 42-Guidance for use of Digital Security in commercial Aviation list technical guidelines and policies and misses the social angle on Aviation Digital practices.

Muhammed Abdul, (2016) attempts to give theories and suggest exploring gaps through role of technology and emerging research.

Bernard Lim, (2014) of Singapore in a speech and on his research paper in "Emerging Information Security Risks in Aviation Issues and Mitigations published in Journal of Aviation Management". The initiatives were undertaken by ICAO. The ICAO AVSEC Panel addressed a variety of topics related to cyber security threats and these were:

(a) Evaluation issued by the ICAO AVSEC risk and threat group on cyber-attack across IT based Air Traffic Managements (ATM) system.

(b) Discussion with other relevant organizations on the cyber security challenges, such as the Civil Air Navigation Services Organization.

(c) Encourage States to develop cyber security management plan for aviation safety.

Andrew Munro, (2016) studied in his paper on "How Cyber (in)secure is air travel?" A 'successful' cyber-attack could cause financial loss, harm to reputation and endanger the safety of passengers. The industry must face the challenge of highly professional hackers trying to exploit a range of weaknesses cyber security. In 2014, the Center for Internet Security recorded 75 cyber-attacks on US airports lone. Current research and development programs have shown that potential penetration of air traffic control, communications navigation surveillance (ATM I CNS) networks by skilled hackers is feasible. This can impact flight activities in a very specific way: halting those scheduled to leave and presenting a possible mid-flight crisis.

National Critical Infrastructure Information Protection Centre, (2017) in its July newsletter mentions of Sectoral CERTs for Power, Finance & Banking sector and Cyber Security Capability Maturity Model (C2M2), however lacks on developing an exclusive CERT for aviation model unlike developed countries. The study, aimed at airport cybersecurity (2016), took place in the context of the CESAR project and was led by CESAR member Eurocontrol in collaboration with Helio, Group ADP and Professor Chris Johansson from the University of Glasgow. Other professors include Oliver Delaine, Oliver Ruhlman and Eric Watier (ADP Group), Matt Shreve and Piotr Circo (Helios) and Veronica Progerin (Eurocontrol) who specialize in APOC (Airport Operations and TAM (Overall Airport Management) on Quality or Assessment of Quality Systems reliability can have a significant impact on CDM (collaborative decision making), even major factors such as two hours of APOC idle time (or Airport Operation Planning (AOP)) can delay or cancel flights, or the Local Area Network (LAN). For example, according to ACL Europe, (2015), the Charles de Gaulle Airport in Paris contributes directly to France's GDP of $ 5.5.5 million per day, which requires Cyber-exercises to assess the organizational strength of existing systems of 26 million and above. Our term used to classify APOC is APOC access due to cyber-attacks at the airport There is a possibility of losing. This time is also chosen because it detects and corrects an event at a reasonable interval.

Maryruth Belsey Priebe, (2016) of International Quality and Productivity Centre (*IQPC)* from Berlin Germany in his paper on “Cyber Security and System Safety in the Aviation Industry” focusses that “Aviation remain a crucial industry in the global economy. Important as a means of travel, tourism, and shipping, aviation is estimated to *Annual $2.2 trillion impact or 3.5% of worlds GDP*”. Embry Riddle Aeronautical University in Daytona Beach has developed a Cyber Security engineering laboratory, which is designed to develop instructional and research emerging needs in the area of cyber security, offering an excellent infrastructure techniques to attack data and show information about existing attacks awareness and perception management.

Christian Beckner, (2015) of the Center for Cyber and Homeland Security studied and presented the ‘Risk Based Security and Aviation System.’ In 2012, some airports had 120 airports and millions of passengers. Basically, it shows an overview of Risk Security Development and Pre-Check Concept in TSA over the last four years and gives many benefits to this program. Beyond one-sizefits-all approaches to aviation security, TSA's mission is to make public awareness on the passenger screening system more efficient and without compromising overall safety. The increase in pre-checks allowed the TSA to save at least $ 100 million in fiscal year to reduce labor and other office costs.

Rafal Leszczyna, (2013) in Cost Assessment of Computer Security Activities and Computer Fraud & Security on its Cost Benefit Analysis-SQUARE model, I-CAMP, I-CAMP II are the basic framework models as per NIST standards for calculating cost of cyber-crimes however the model doesn't fit in for Aviation Model.

Hamid Salim, (2014) studied on Cyber Safety and highlighted: "A systems thinking and Systems Theory approach to Managing Cyber Security Risk calls for new way of thinking to approach Cyber Security risks. Symantec's 2014 Internet security report shows more than 10 million data of Names, Mobile numbers, date of birth lost in a single breach. Proposes STAMP model- System Theoretic Accident Model and Process.

Aviation Security, Center for Strategy and Evaluation Services United Kingdom, (2011) through a Case Study on Aviation Security and Detection Systems, the European Union's leading research fundraising project for the 7th Framework Program for Research and Technology Development (FP7) 2007-2017. FP7 budgeted for 50.5 bn US dollars.

Civil Air Navigation Services Organization, (2014) in their paper **"**The Global Air Traffic Management Operational Concept (ICAO Doc 9854)" speaks and sets the security expectations of an integrated, inter-operable and global integrated ATM system: "Protect against intentional attacks activities involving air, personal or land facilities (such as terrorism) or accidental activities (such as human negligence, natural disasters)". Adequate security is an important responsibility ATM group and the people. Therefore, the ATM network should lead to protection and the ATM device as well as the details relevant to ATM, should be secured from security threats. Security risk control will align the interests of the ATM group participants of network entry.

Randall, J. Murphy, Michel Sukareeh, John Hass Paul, (2015), **through** their Guidebook on Best Practices for Airport Cybersecurity and cooperative research program (ACRP) addresses threats to cyber or machines, are growing in amount and complexity. Although this phenomenon is well known in the newspapers, the airport was not attacked and some cyber information, operational disruptions, expensive Recoveries, and damaged credibility. These attacks are likely to increase as airports are increasingly relying on computer technology and cyber criminals are becoming more advanced. Most flaws have to do with human behavior. Bad treatment of usernames and passwords, opening links from hidden websites, installing malicious apps and revealing personal details has contributed to several successful assaults. Comprehensive European Approaches to the Protection of Civil Aviation (COPRA), 2013 Recommendations on future research and Developments. They collected categorized, and 70 existing, evolving, and future threats to airports, aircraft and auxiliary infrastructure were evaluated. The team than complied 350 security measures to counter these threats.

Miake Pierdes et al.,(2015) from Cyber Security task force of Pillsbury Winthop Shawn Pitmaan LLP studied and highlighted , “Cyber Security and the Aviation Sector: Recent Incident Highlight Unique Risks, If an airline is subjected to a cyber-security attack, this may not result solely in data loss, be it customer records, customer financial details or sensitive company revenue details; it may impact the core operations of an airline with cyber-attacks potentially seriously disrupting and endangering the safety of flights”.

Press release No 29 of IATA, (2016) on closer collaboration with governments to tackle threat of terrorism. Terrorists have alleged claims including Metro jet 9268, Daallo 159 and at Brussels Airport over the last twelve months. These are grim reminders of a vulnerable aviation. IATA is working with Airports Council International to broaden the securities; This would offer the “triple advantage of shortened landside waits, more reliable scanning and an enhanced customer experience”. IATA works with companies around the supply chain to introduce quick Travel that can improve self-service passenger transport. Internet check-in home printed baggage tags enable the passenger to arrive ready to travel at the airport, thereby reducing passengers dwelling time in airports landside areas.

Mariaa Badaa and Angeola Sases, (2014) presented Global Cyber Securities Capacity Centre in their paper on ‘Security perception and online behavior’ trying to understand those factors which leads to failure of data security behavior. The study was limited to experiment in United States and Australia.

Yan Chen and Fatemeh Mariam Zahedi, (2016) examined in their study context exposure of online security perception & behaviours of users’ characteristics is barely found, and there is in proper research into the continuum of behaviour of users when discussing online security threats. The is paper builds upon complementary theoretical grounds in resolving the gap: “Contextualization online security behavior through Protection motivation theory while applying contextual lens for cross-national user safety comparison behaviors in United States Studies people’s behaviour across US and China moderating role of nation and Indian Context is not studied. Indian Culture with segmented knowledge base and diverse economic segments needs to be studied on same prospects”**.**

Tsai et al., (2016) studied on ‘Understanding online security behavior: A protection, motivation theory: Internet user experiences.’ This paper combines a commonly ignored PMT variable to contributes researches on computer and securities: Previous experience with security risks, and other new police assessments variable means standard into the PMT model

Indian Brand Equity Foundation, (2017) captures Indian Aviation Industry details, 30% of the country’s income comes from the Aviation and associated industries. The government has supported the Civil Aviation Safety Bureau with $9.71 million in its expenditure.

Ronald W. Rogers, (1975) from University of South California in his paper of "A Protection Motivation Fear Appeal and Attitude Change Theory" published in Journal of Psychology published in 2010, postulates three crucial elements of the appeal of fear: -

(a) The magnitude of occurrence of that event.

(b) The degree to which a recorded case becomes noxious

(c) A defensive response's efficacy. Variables mediate attitude change.

Posey et al., (2015) findings revealed that praising PMT on Cyber Security behavior. Practical **Aviation Security Book** on Aviation: "Protecting Critical Infrastructure & Role of Government". Chapters 4 and 6 stresses on the fact that

(a) A 2010 report by the Ponemon Institute that found a single company the estimated total expense of cybercrime ranged from $1 million to $52 million. (The Snow,2011).

(b) The aviation system consists of thousands of entry points and is vast. This consists of two primary elements in the United States:

    (i) Airports, planes, and staff resources and assets; and

    (ii) Aviation command, control, correspondence, and IT services to enable and suite in secure usage of airspace.

    (iii) There are more than 19,800 airports, 211,000 registered aircraft and 550,000 trained pilots and navigators in general and commercial aviation.

L. Rn, H. Liaos, M. Castillon-Effenc, B. Beckmane, T.Citrieiti, (2015) in their book 'Applications in Aviation Cyber-Physical Systems', vide Chap 22 on transformation of mission-critical applications transformation of Mission-Critical Patterns Survey (SITA, 2015). Showed that 38% service and 57% use tech as a service. Both figures are forecast to grow and are expected to increase to 73% and 87% in 2018. Analysis qualify and quantify the physical layers by its computational and network requirements on the one hand and the cyber layer through its computational and network capacities application has safety consequences:

(a) Class 1: Public Security. Improper usage of the program has implications for health.

(b) Class 2: Extensive impact. The application operation itself may not be a direct security consequence but it does rely on many more applications including potential protection-critical activity (Although the impact on these applications has diminished), resulting in a wider impact on operation.

(c) Class 3: Large Effect critical deliverables seriously impacted and tipping point but aggregated effects over time may bring seriously impact system.

(d) Class 4: critically nonoperational and does not have any impact on the current procedure and productions. It also accentuates on New failure mode and system validations and verifications heterogeneous network and air-ground systems architecture. Degraded system operation, Security & privacy, Current and planned Next Gen modernization. investment cycle, Stakeholder interests and sustainable business models.

Florent Frederik, (2015) of 'Online Trust and Cyber Security unit European Commission' states the following:

(a) FBI claims to hack into planes. Computer Expert hacked into the aircraft and made it fly sideways.

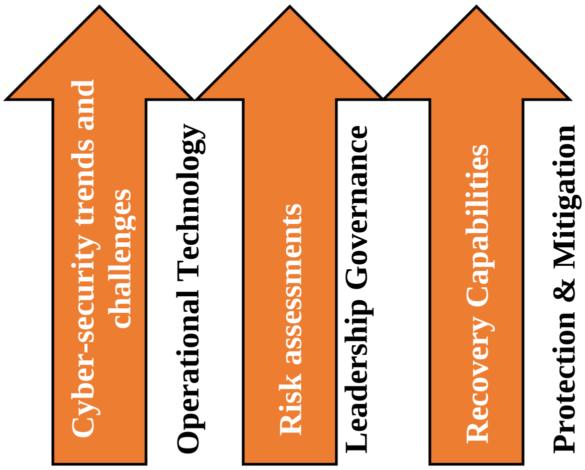
(b) Air traffic challenges.

(c) GAO warns that aircraft are vulnerable to hacking vis in flight Wi-Fi Networks; singles out Boeing Dreamliner, Airbus 350, Airbus 380 because cockpits sharing same Wi-Fi Networks as passengers.

(d) In Europe digital market: Commission sets out 16 initiatives.

Kim-Kwang and Raymond Choo, (2011) from University of South Australia, discusses in his paper routine activity theory and mitigating cyber risk by reducing the opportunity for cyber threat to occur and make these crimes complex by easier detection and harsher punishments. Increase the effort needed to make offence increasing the probability of captures. Enhance research and synergy between Government, Industry, and research Institutions.

PA Consulting, **UK, (2018**) in its paper on “Overcome the Silent Threat: Building Cyber Resilience in Airport”: Evolving from Physical Security to Cyber Security stresses upon “An averaging 1000 attack every month”. It carries out in-depth analysis of four Airports and highlights the following six parameters:



(Source: PA Consulting, UK, (2018)

Figure 2.1: Six parameters of Cyber Security

Franacis et al., (2012) has compiled in its paper "Theory of Behavior Change in the Theoretical Group" that the Theoretical Domain Framework (TDF) has been successful in transforming psychological behavior from a variety of disciplinary contexts to useful ones. Various health care settings. It describes the full range of potential mediators of behavior in relation to clinical action, ignoring social science approach and technological adaptations”.

Roberte W. Poolae Jr., (2015) highlights Policy failure occurred at FAA after 9/11 attacks. It also addresses lack of good governance and transparency principles by TSA vis a vis Airport security. Criticize governments Federal Air Marshalls (FAMs) policy. Stresses upon finding aspects of Airport Security, In Europe it is being by Airlines, Airports and Passengers.

Pollni et al., (2014) in Cyber Security & Privacy forum of Deep Blue- Italy, Airport as Critical Transportations Infrastructure become highly threatened by Cyber-Attack: “A case report covering hypothetical situations”.

Martin et al., (2016) vide its NATO Publications: “Accessing the impacts of air safety on cyber power”, Discusses in detail in threat model in Aviation with respect to Cyber electromagnetic Activities and recent advances in wireless communication and vulnerabilities in the Aviation communication and navigation systems.

Phillip et al., (2017) vide Journal of Management Information System on User motivations on Security Protection: “Managers who want to protect information systems in order to understand how to motivate users to engage in safe behaviour”.

Schmitt et al.,(2019) on Simulations support Aviation Cyber- securities risk analysis. Addresses simulation-based practices for enhancing better Cyber resilience, Calls for human interaction models.

ICAO in its working Paper, (2018) during 13th Air Navigation Conference in Montreal presents Cyber Resilience and Airport preparedness and stresses upon increasing Cyber-Attacks around the world and in Aviation Sector**.**

Georgia Lyko, (2018) studied Cyber security at airports to improve cyber stability. Technical Organizational and Policies and Standards in Cyber Security.

Georgia et al.,(2019) studied Sensors, Mitigation in threat and Cyber Resilience controls for smart Airport Security: Divides Airports into Agile, Smart, and basic Airports and carries out study of European and few American airports. Defines, Good practices for Policies and Standards.

Robert W. Poole, (2015) highlighted the 2011 TSA Pre check Program in his paper on "Fresh Thinking on Aviation Security". Airlines provide premium flyers to their customers along with customers satisfaction. TSA's standard used customers identity before flying. For the same officers also provide training for the same.

N. Anderson, (1971) studies and investigated various model and tested theories for attitudinal change of passengers and officers of Aviation industries. "Integration theory has been found to be reasonably successful in areas such as learning, understanding, judgment, decision making and personality traits, as well as attitudinal change. This is the beginning of a unified general theory. "

M.Strohmeier, M.Schäfer, R.Pinheiro,(2016) studied an indicated findings in their paper Security in Aviation Industries is very important issue and linked with various technologies such as IOT and AI. They further surveyed that knowledge must be codified in 242 international professional and also analyze various security issues in aviation communities.

B. Lim, (2014) highlights in his study report that cyber-attack more complex and sophisticated manageable issue and it relies on ICT on day-to-day operations. Today global aviation industries need to make more paces to protect awareness and recognition for dealing Cyber Security. The paper also explores some of the challenges and possible ways to address the issue of Cyber Security threats facing the global civil aviation community against Cyber threats that severely damage and weaken the global Civil Aviation system.

T.Ormerod and C.Dando,(2015) studied that there is no strong psychological basis or empirical affirmation in their paper. They demonstrate a new method of testing the integrity of passenger accounts. In the Vivo Double Blind Randomized-Control Trial conducted at international airports, security agents identified 66% of fraudulent passengers using the Variety Test method, which was less than 5% using behavioral index identification. In addition to revealing the benefits of accuracy testing on behavioral index identification, this study provides a fraud identification date up to the actual context in which the known rate of fraudulent individuals is low.

Kirschenbaum et al.,(2015) studied and defined individual design and transportation processes have transformed airports into mass production companies, where the human behavior of employees and passengers is defined in a rational and logical framework. However, recent empirical evidence raises some complex issues based on this complex hula. Ethnographic, field survey questionnaires, interviews and analyzes of data obtained from a coordination panel study from 8 airports in Europe make it clear that the use, bending and violation of regulations are very common; Most threats are assessed as false alarms; Security decisions are primarily group decisions; Coworkers and friends influence regulations and are actively involved in passenger safety decisions. These behaviors do not fit exactly into the scientific model of airport design and operations. We therefore argue based on data generated from these methods - the classical aviation security model should be expanded to take into account the reality of human behavior of passengers and employees in the security process. This approach emphasizes the social dimension of security decision-making, i.e. airports, as well as complex social institutions, with formal administrative and informal social network structures. Institutional behaviors in these social contexts are how security decisions are made and they are subject to regulations. He therefore proposes to expand the basic security model, but to increase value by reflecting the reality of human behavior in the institutional context of airport. Based on above literature there exists research gaps to study the Aviation Cyber security from a different perspective.

Research Gaps

The above study based on themes of Aviation Cyber Security, Aviation Security Cyber security and Online behaviour brings out the facts that very limited studies has been carried out by Indian researchers and so very limited data is available in the Indian context. Further, India being one of the diverse nations and one of the most promising developing one it is pertinent to study the human minds and perceptions to understand behavioural pattern and security awareness cum consciousness. It is also important to see the developmental pattern of research in this sector in past few years. There is phenomenal growth in published literature on subject however data sharing on Indian Airport security will take more time to come out among the interested fraternity. Thus, the research gap which emerges from the literature review is:

The gap which emerges from the literature review is:

(a) Very minimal studies on Aviation Cyber Security behaviour in Indian context and there is need to address Aviation Cyber Security threat by changing Perception, Attitude and behaviour of passengers.

(b) Addressing Aviation Cyber Security challenges through an established theory of fear and cognitive studies.

CHAPTER 3

GLOBAL AVIATION INDUSTRY AND CYBER VULNERABILITIES

3.1 OVERVIEW OF GLOBAL AVIATION INDUSTRY (GAI)

The GAI is made a profit of $28 billion in 2019 (Business today, 2019 June 02) much lower than previous revenues of $35.5 billion. "As per IATA, fuel prices are increasing. Global trade is having a negative impact on the airline business. IATA, a group of approximately 290 aircraft, also reports that total costs are projected to grow by 7.4 per cent, exceeding a 6.5 per cent increase in revenues" (NCAER, 2017). The previous fall of 2018 was caused by oversupply of crude oil, partially due to the production of bituminous shale oil in the United States. However, sanctions on Iran's oil exports and restricted overcapacity at OPEC have driven oil prices down to $70 a barrel and when fuel prices have been negatively affected, there is no permission/restricted to travel in the middle of the world tightened under Corona pandemic. Lately, there has been major intangible casualties in the cyber-attacks on the sector. The current slowdown in COVID-2019 will make the few aviation companies bankrupt by June 2020.

For its landside and Airside activities, the aviation sector depends highly on Information Technology. The safety of air transport systems has a major effect on operational safety, services and financial health. The survey questionnaire on study covers feedback on safe cyber practices and awareness of people travelling ranging from aviation management to control and airport management through solutions and applications. The analysis associates it to existing theory covering passenger safety to create higher awareness among all stakeholders. The objective is to estimate the size of the market and its potential for growth in different segments, such as the security solution, the end-user, the form of investment and the area. The study also includes analysis of primary market participants, the profiles of their firms, key insights into recent developments and business strategies.

3.1.1 The Aviation Cyber Security Market - Growth, Trend and Forecasts (2019 to 2024)

"Aviation industry is expected to increase cyber security market to 11% from 2019 to 2024 (Aviation cyber security market- growth, trends and forecast, 2020). The airline industry has profiteered from the emerging technologies, cloud; automation and safety however threats too have emerged significantly. The technological effort has undoubtedly improved customer service, safety, aircraft efficiency, ground and air passenger handling and experience. “In contrast to advances in technology and connectivity, the aviation systems faces a risk of cyber-attacks in the marketplace,” Hobbit said. In December 2017, for example, a large amount of confidential security information was stolen from Perth Airport with regards to flight plan and passengers data. Pacific Airways Limited, the world’s largest airline had a data loss when hackers obtained personal information from 9.4 million customers. Breach of such data needs to be prevented.

The sector has boomed and on way of accomplishing new standards, billions of investment made into this sector especially in India for the regional hub, the need to protect this critical infrastructure has become imperative. “The market is driven by several factors, such as the increasing number of passengers, the replacement of obsolete security control equipment, and the development of new airports. According to security solutions, the IT security solutions market is estimated to represent most of the market for passenger safety in 2019 due to the increase in cyber threats and attempts to hack airport and aviation operations. European Union Aviation safety agency (EASA) and Federal Aviation Authority (FAA) reported that there is an average of 1,000 attack every month in air transport networks (ACRP 140, 2015). Increased use of data analytical tools, artificial intelligence and video monitoring for security operations allows these systems to be theft-proof, which also drives the IT security solutions market. According to the end-user, the commercial airport segment is projected to have a large market share in 2019 (Gopal krishnan et al.

2013). Commercial airports have the highest market share due to the amount of systems built at each airport in 2019. In order to cope with the growing number of passengers, airport terminals need to be expanded, requiring investment to increase safety lanes. The replacement of outdated equipment with modern technologies helps to identify passengers more easily and accurately, increasing the efficiency of the safety operation.

"Asia Pacific is estimated to have accounted for the majority of the passenger safety market in 2019, which increases the movement of passengers in Asia Pacific due to increasing demand for air travel." This contributes significantly to the growth of the passenger safety industry Countries such as China and India are investing heavily in airport infrastructure. For example, according to Business Television India, China is expected to build 74 new airports by 2020 (Aviation Cyber Security Market – Growth, Trends and Forwarding, 2020). Some emerging market trends includes the growing demand for cloud-based secured security solution.

3.2 GROWTH OF INTERNATIONAL AVIATION INDUSTRY

The international aviation industry has grown in past as an indispensable component of the global marketplace. The amount of investments into this sector was phenomenal and has been a major contributor to global economy. Major challenges into this sector with airlines are the problems of priority routes ‘passenger per miles’, operating profitability and the fuel costs.

Global aviation transport shows the development of approximately 5 % in recent years. Usually, the development in this field is twice the yearly development in GDP. In fact, over the last 10-15 years there has been a consistent annual growth of 4-5% worldwide. In United States (US) alone, transport aircraft have recorded over “$ 160 billion in absolute income, and more than 8,000 aircrafts on an average 31,000 flights for each day.” Commercial Aviation accounts for 8 % of the United States’ total national output. (Impact et al, 2014)

3.2.1 Evolution of the Recent Industry

After the 9/11 attack, the industry had a major impact on aviation economy, it had already begun to show virulent repercussion. All of these factors have led to a decline in labor / management relations and poor service in general. Significant changes were noted in passenger choice behavior, particularly for business travelers. Further, economic recession and reduced budgets for business travel had a revenue impact by more than 20% in US alone. Aviation's legacy has aimed to increase aircraft profitability.

3.2.2 Current Structure of the Global Aviation Industry

The report – Global Aviation Industry 2010-2019 analyzed the global aviation sector in terms of value growth, passenger volume, industry profitability, sector segmentations and fleet developments. Global trends in the aviation industry are further analyzed in terms of industry prices and revenue, lower fuel price, regional performance margins, network operators, sector deregulation & the emergence of low-cost operators, among others. Interestingly, none of the studies mention the amount spent on aviation security or even the cost spent on improving the network structure in the region.

3.2.3 Global Aviation Cyber Security Market

The global demand for cyber security in aviation accounted for $2,794.63 million in 2017, which is projected to rise to $6,482.54 million by 2026 (NCAER, 2017). Increased cyber-attacks and a growing number of air travelers have provided impetus to the growth of the information security sector. The aviation industry relies heavily on IT infrastructure, as the world revolves around ATC and flight operations, Air side and side of operations include airline ticketing.

Aviation cyber-protection systems are integrated cyber-physical structures, networked and protected at various safety and security levels. The technology used in the Aviation Management segment has resulted in improved financial performance, customer satisfaction and operational efficiency.

3.3 GLOBAL PERSPECTIVE OF INDIAN CIVIL AVIATION INDUSTRY

We reviewed a variety of important studies and articles approved to compile this collection of key developments in the aviation industry specific to the Indian civil aviation market, vulnerability in cyberspace. "According to the IATA, the India will beat U.K. and will rise to third by 2025. (IATA, October 24, 2018). IATA expects a rise in net global income to $38.4 billion in the 2018 aviation industry review, compared to a previous year of $34.5 billion in 2017.The figures and estimations change post COVID-19.

The performance forecast for 2019 shows that the operating margin will decline to 8.1%, but that sustainable profits will also be expected for 2019. The net profit is predicted to increase by 4.7 per cent. General sales are projected to be $824 billion, while passengers are projected to be $4.3 billion. Some of the modern infrastructure technology incorporated in aviation is discussed as follows:

(a) **Digital Security System:** Implementation of technologies such as safety and biometrics has greatly shortened waiting times for travelers and shortened the pressure on staff members. Security systems have found their way into the airport security system. "There has been an increasing demand for the integration of cyber security services into IT solutions. Suppliers are actively growing security solutions to foresee competition and boost their market presence.

(b) **Robot Helpers in Airports:** In 2017, “Seoul Incheon International Airport teamed up with the electronics company LG to test two robots at the airport. One was capable of communicating with passengers in several different languages, while the other was programmed to keep the airport clean.”

(c) **Biometric Entertainment:** Biometrics are not only capable of improving protection, but are also designed to potentially enhance passenger travel experience across the air to include biometric payment and the choice of entertainment based on personal preferences. In partnership with Tascent Inc Panasonic, the aim is to infuse the biometric identification of passengers at every stage of the journey.

(d) **Book a Taxi in the Sky:** The 3D Flight Path Mobile Map is testing a way for passengers to book taxis via the IFE flight route on the backup screen. When landing, passengers can receive an SMS about the specifics of the journey.

(e) **The Growth of Low-Cost Aviation:** If 2017-2018 proved to be an excellent year for low-cost Aviation, and 2019 is expected to be yet another eventful year of rapid growth in aviation trends. Traditionally, LCCs were considered only for short-range distances. LCCs have over the years have considered flying long-distance routes, which has been profitable.

(f) **Green Airports:** Airports are constantly engaging with renewable sources of energy for improving energy management solutions for issues like limiting noise, and air pollution Suppliers such as Honeywell and Siemens have a solid portfolio of building management services. The integration of these systems with their existing airport solutions will complement airport management and other related services.

(g) **Cancellations and Complaints:** The overall cancellation rate for the domestic Aviation scheduled for December 2019 is 0.66 percent. Air India recorded the highest number of cancellations of 2.40 percent, followed by Trujet (1.07 percent) and the low-cost Aviation Spicejet (0.70). In December 2018, the national scheduled Aviation received a total of 803 passenger complaints. The industry paid over Rs 2.61 million to over 2.01 lakh passengers. "Domestic and International airfares increased by 7% and 11% respectively. However, despite the marginal increase in airfares and localized and seasonal problems such as bank strikes and fog cancellations, the domestic passenger market recorded strong annual growth of 18.6 percent.

3.4 AVIATION INDUSTRY CHALLENGES

A continuous process of restructuring and development of the aviation industry has taken place. However, even after recurring cycles of achievement and collapse, unsafe features required more attention.

3.4.1 Indian Civil Aviation Industry and Impact

Passenger traffic in India increased from 16.52 per cent each year in a row to 308.75 million in fiscal 2018. The number of passengers worldwide rose 10.43 percent to 65.48 million in 2018. The largest stakeholder in the passenger airline industry. India's domestic and foreign air transport has increased by 7.93 % and 6.36 % respectively in 2018-19. India's passenger traffic in 2019 was 344.70 millions. For that, domestic was 275.23 millions, while international was 69.47 millions. India had 103 airports in service as of March 2019. The figures are expected to be between 190 and 200 by the fiscal year 2040. The number of operating aircraft is also expected to increase significantly from 620 operating aircraft in 2018 to 1,100 by 2027(NCAER, 2017).

(a) **Investment**

Major projects and development of Indian flight department included:

(i) AAI is expected to contribute $2.33 billion in 2018-19 to expand existing terminal and build 15 new one.

(ii) In June 2018, India agreed to an outdoor agreement with Australia that would allow aircraft from both sides to give wide seats to six Indian metropolitan urban communities and a few Australian urban communities.

(iii) AAI plans development as an inter-regional focus as an inter-regional focus in Guwahati and Agartala, Imphal and Debrugarh as an inter-regional focus.

(iv) Indian Air Workshop, Repair and Improvement (MRO) Professional Co-operative and Complete Exemption from Counter-Responsibility.

(b) **Government Initiatives**

The significant activities attempted by the administration are:

(i) In February 2019, “the Indian government authorized the advancement of another Greenfield Air terminal in Dholera, Gujarat, with an expected venture of 1.440 million rupees”.

(ii) As of January 2019, the Indian government is dealing with an arrangement to advance the creation and financing of a household airplane in the nation.

(iii) In January 2019, “the Government of India propelled the 2019 national Airship cargo strategy program, which intends to make the coordination of Indian flying cargoes most effective, continuous, and beneficial worldwide.”

(iv) In November 2018, “the Indian government affirmed a proposition for the administration of six AAI air terminals in an open private organization (PPP)”.

(v) In February 2018, “The Prime Minister of India began the development of Navi Mumbai Air terminal, which is relied upon to be worked for USD 2.58 billion. The first period of the air terminal will be finished in late 2019.”

(v) The Andhra Pradesh government plans to create Greenfield air terminals in six urban communities.

(c) **Vulnerabilities in Cyber Space**

The civil aviation industry cannot be separated from the cyber-crime risk. The risks involved in civil aviation safety include: 'illegal capture of aircraft, destruction of aircraft in operation, taking hostages on board aircraft or airfields, forced intrusion into aircraft, airport or aircraft installations, use of aircraft in operation. An appropriate governance structure for the implementation of sound information protection will be a prerequisite for addressing the challenge of information protection. Cyber security involves the collection of technologies, policies, security controls, the IT environment, programs, data and organizations from attacks, damages or unauthorized access.

Cyber Security not only provides technical control, but also presents a wider goal of protecting confidentiality, dignity and availability on the basis of the organization's security standards and compliance. The use of electronic systems and technology is applicable in ISMAC (IT, software, automation, research and cloud) for critical business operations, including security. This aims to defend information systems against any cyber threats and mitigates any unforeseen circumstances that pose a threat to the CIA: confidentiality, credibility and availability of data. In an effort to recognize the urgent need to protect critical civil aviation infrastructures, information and communication systems from cyber threats. In order to achieve the objectives set out above, 'ICAO' has set up a 'Secretariat for Information Security' (SSGC) study group made up of expert from Member State and industries. 'SSGC's initiative aims to support all 'ICAO' cyber security research, identify appropriate areas for consideration and consolidation of existing 'cyber security standards and recommended practices' (SARPS) and enhance cyber security knowledge across the aviation community.

Article A39-19 of ICAO takes into account the increasing dependence on technologies and emerging issues with regard to the availability of information and communication technology systems for business continuity, privacy and confidentiality of data based on requirements in the field, the implementation of safety management systems and risk management. ICAO thus emerges as an organization that promotes a mutual awareness between member States of emerging cyber threats and the resources needed to mitigate the risks. It also facilitates cooperation between government and industry on cyber security initiatives.

3.4.2 Emerging Cyber Threats and Cognitive Vulnerabilities

Emerging threats and cognitive vulnerabilities have identified the “crucial role of human behavior” plays in IT security and provides information on how human decision-making can help cope with increasing volumes of computer threats. Apply psychological factors such as bias, group dynamics, and heuristic decision-making that can lead people to understand risk.

The objective of this understanding is to identify threats more quickly and to develop prevention and education strategies. There are many and increasingly potential cyber weaknesses in aviation. Technological advances have developed an automated phenomenon that marginalizes the role of human activity. Automated systems are responsible for handling more and more situation, which mean people have to intervene when something unusual and unexpected happen. This compromised human capacity to respond quickly and appropriately in the event of a crisis. The point of interaction between automated procedures and human interaction is considered to be the most vulnerable, according to researchers.

The Aviation industry always remain a high-value target for sufficient reasons. There is a lot of media attention to aviation-related incidents. With its ability to cause fear and uncertainty, it is likely to be an attractive target for attackers. Even a marginal disruption in the air services tends to sway away the faith of people and the market declines. The leisure and pleasure of travel takes one incident for drop in business and hence it’s critical business in terms of faith and people expectations.

This research covers a variety of topics and also faced a variety of challenges and seeks to change the response in the areas of decision-making, action, artificial intelligence and human interaction with information security:

(a) Explain the psychological factors inherent in machine learning and artificial intelligence.

(b) Examine the social dynamics of online radicalism and the recruitment of terrorists.

(c) Review the motivation and decision-making of hackers and hacktivists.

(d) Investigate the use of personality psychology to extract information from individuals that is secure.

3.4.3 Cyber Security Initiatives Launched by the Government of India

India has taken significant steps to strengthen its cyber space. This includes awareness programmers; create a strong political environment and strengthen security monitoring capabilities and international cooperation; and research and development to improve cyber security. Here are some important initiatives:”

(a) **National Cyber Security Policy:** Launched in 2013, the policy aims to provide strategic vision and direction to protect national cyberspace.

(b) **National Cyber Security Coordination Center:** The NCC will evaluate a real-time threat from the CCC and raise awareness about the potential cyber threat to the country. It has been launched since August 2017.

(c) **National Center for Critical Information:** Infrastructure Protection: (NCPC) is designated as a national nodal agency to protect complex information infrastructure, formed under Article 70A of THE IT Act. Its goal is to protect and protect complex information infrastructure (IIC) from cyber terrorism, cyber warfare and other threats.

(d) **Cyber Swachhta Kendra**: Launched early in 2017, cyber transparency centers" are used as a platform for analyzing and cleaning systems from various viruses, robots/malware, Trojans

(e) **International Cooperation:** India has signed nine new bilateral agreements with developed countries like the United States, Singapore and Japan to research and exchange information on cyber security.

(f) **Promoting Research and Development:** Companies responsible for ensuring cyber security across the country, have received an impetus with a public grant worth Rs 5 million.

(g) **Security Testing:** There are plans to set up 10 additional facilities for standardization testing, quality insurance and certification (STQC) across the country for IT product evaluation and certification." The efforts and replicating methods are taking place by the other developing nations in the direction of mitigating challenges of cyber-crimes.

3.5 CONTEMPORARY STATUS OF DELHI AIRPORT

IGI was the twelfth busiest airport in the world in 2019 and the largest and busiest in India (Please see table 3.1 below for busiest Airports across the world). It has risen four rankings have risen from 16th position in 2008. According to the 2018 World Airport Traffic Preliminary rankings published by the International Airports Council (ACI), some of the major airports such as Frankfurt, Dallas e.t.c. In the year of 2018-19, Delhi's Indira Gandhi International Airport (IGI) was declared the country's busiest airport. However, it has witnessed the lowest passenger growth rate since last year. The airport has national, regional and international passenger and freight services from more than 40 aircraft. According to the HT report and data collected from the Indian Airport Authority (AAI), IGI Airport served 69.23 million passengers in the 2018-19 period, up 5.4% from the previous year. Prior to the last financial year, the airport had a steady double-digit growth rate. Passenger traffic handled by the airport increased by 13.8% in fiscal year 2017-18, 19.2% in fiscal year 2016-17, 18.1% in fiscal year 2015-16 and 11.1% in fiscal year 2014-15.

Data published by DGCA reveals that the industry has had the lowest rate of passenger growth since June 2019 in March 2020. There are 103 airports operating in India as of March 2019. As of July 2018, 620 aircraft had been serving in the fleet of Scheduled Indian Administrators. The numbers are planning to reach 1,100 aircraft by 2027. In 2018-19, AAI invested Rs 15,000 million ($2.32 billion) in terminal expansion and assembled 15 new terminals. The airport area has been opened up to private interest; with the PPP model, six airports in central urban areas have been built. The Indian Airport Authority (AAI) is proposing to run around 250 airports throughout the country by 2020. Investments in airport infrastructure in India for Rs 420-450 billion ($5.99-4.41

billion) is expected between 2018 and 23 of the fiscal year (NCAER, 2017). There are five Territorial Aviation Protection force i.e. Delhi, Mumbai, Chennai, Calcutta, and Hyderabad. None of the Airport mention airport security expenditure and therefore the revenues generated by the airport are less significant. According to an airport official, it has been very weak since June 2019; this is a result of many factors affecting the aviation market. The closing of Jet Airways is also the result of losses in the Jet Airways industry.

Table No 3.1 Total Passenger Traffic 2018

Rank 2018	**Rank 2017**	**Airport CITY/COUNTRY/CODE**	**Passengers (Enplaning & Deplaning)**	**Percentage rise in no of Passengers**
1	1	ATLANTA GA, US(ATL)	107394029	3.3
2	2	BEIJING, CN(PEK)	100983290	5.3
3	3	DUBAI. AE(DXB)	89149387	1.1
4	5	LOS ANGELES CA, US(LAX)	87534384	3.4
5	4	TOKYO, JP(HND)	87131973	2.0
6	6	CHICAGO IL, US (ORD)	83339186	4.4
7	7	LONDON, GB(LHR)	80126320	2.8
8	8	HONG KONG, HK (HKG)	74517402	2.6
9	9	SHANGAI, CN(PVG)	74006331	5.6
10	10	PARIS, FR (CDG)	72229723	4.1
11	11	AMSTERDAM, NL (AMS)	71053147	3.6
12	16	NEW DELHI, IN (DEL)	69900938	10.2
13	13	GUANGZHOU, CN (CAN)	69769497	6.1
14	14	FRANKFURT,DE (FRA)	69510269	7.8

Rank 2018	Rank 2017	Airport CITY/COUNTRY/CODE	Passengers (Enplaning & Deplaning)	Percentage rise in no of Passengers
15	12	DALLAS/FORT WORTH TX, US (DFW)	69112607	3.0
16	19	INCHEON,KR (ICN)	68350784	10.0
17	15	INSTANBUL,TR(IST)	68192683	6.3
18	17	JAKARTA, ID (CGK)	66908159	6.1
19	18	SINGAPORE, SG(SIN)	65628000	5.5
20	20	DENVER CO, US (DEN)	64494613	5.1
Top 20 for 2018			**1539332722**	**4.7**

(Source: Airport Council International 2018)

Airport Authority of India (AAI) formed in 1972 for the administration of national-international airports with Bureau of civil Aviation Security (BCAS) came as an independent body in 1978 to look into Airport security. Airport Economic Regulatory Authority (AERA) was established in 1998. Further, Director General of Civil Aviation (DGCA) comes up as a statutory body with an amendment bill in 2020 as a central regulatory body in India for all aviation related matters. AAI operates a total of 126 airports, including 11 international, 11 traditional,89 national and 26 civilian enclaves in military airports.

3.5.1 Traffic Forecasts

The passenger traffic has been consistently growing in both domestic and international arena with regional connectivity coming in during 2018-19 Delhi airport generated an Average Annual Growth Rate (AAGR) of cargo by 11.6 percent in contrast to 8.2% of Mumbai during the comparative period.

Until 2008-09, Mumbai was the leading airport of India encompassing largest numbers of passengers. Shortly, however Delhi airport activities had grown faster than Mumbai with about 30 million passengers a year in excess as compared to Mumbai’s 29 million passengers. Below are the tables projecting and forecasting the growth of passengers across world vis-à-vis Delhi Airport by Airbus (Table 3.2). The tabulated data of Delhi Airport is in Tables 3.3.

(a) **Delhi Airport, Passenger forecasts:**

Table 3.2 Passenger Traffic Forecast (Million)

	Global market forecast, Airbus Industries, 2012 for All India*				**AER Projection for All India****		**NCAERP**
	Domestic	**Intern -ational**	**Total**	**Domestic**	**Intern -ational**	**Total**	**Domestic**
2012- 13	27.23	45.12	172.35	128.5	44.8	173.5	27.6
2013- 14	143.14	49.41	192.55	141.3	48.9	189.9	30.3
2014- 15	161.03	54.10	215.13	154.2	53.3	207.9	33.2
2015- 16	177.94	58.43	236.37	169.6	58.1	227.5	36.4
2016- 17	196.62	63.10	259.72	184.3	63.3	247.6	39.6
2017- 18	217.27	68.15	285.42	200.6	67.7	268.3	43.1
2018-19	240.08	73.60	313.68	218.2	72.5	290.7	46.9
2019-20	265.29	79.49	344.78	237.4	77.5	315.0	51.0
2020-21	-	-	-	258.3	83.0	341.3	55.5

(Source: Mott MacDonald for Delhi airport)

Table 3.3 Delhi Airport Master Plan

	Domestic	**Intl’**	**Total**	**Domestic**	**Intl’**	**Total**
2015	31.0	15.1	46.1	8.0	7.0	7.7
2016	33.4	16.1	49.5	7.5	7.0	7.3
2017	35.9	17.1	53.0	7.5	6.0	7.0
2018	38.5	18.1	56.7	7.5	6.0	7.0
2019	40.9	19.0	59.9	6.0	5.0	5.7
2020	43.3	20.0	63.3	6.0	5.0	5.7

(Source: Mott MacDonald for Delhi airport)

(b) **Revenue Forecast**

The revenues generated from Airport comprises of different sections and thus there hasn’t been an impact study on disruptions in each factor alone.

Revenue generators from an Airport includes Aviation revenues from Airlines, Passengers, and cargo both. Non-aviation comes from Maintenance services, Airport services such as shopping and food joints plus income from goods. The projection of aviation revenues depends on the general revenue per traveller for the last two years. For 2012-2013, we recognized the growth of 341 percent (334 percent + 7 percent of the CPI), and for the period 2013-2014. Moreover, it has considered "the impact of tourist development on revenue in over two years. In the event of a non-aviation event occurring, the projections are similarly established on the scope of non-aircraft revenue per passenger in the last two years. In the case of Cargo, a 2% growth rate was expected from 2016-17 onwards. The total income of DIAL is tabulated below in table 3.4 into three primary sections air, non-air and cargo for the past 9-10 years.

Table 3.4 Projection of Revenue for DIAL from 2011-12 to 2020-21

(In Millions)

	Aero	Non-Aero	Cargo	Operating	Other	Total
				Income	income*	Income
2012-13**	26481	7812	1301	35594	900	36494
2013-14	32210	8600	1326	42136	960	43096
2014-15	20908	9312	1353	31572	1008	32580
2015-16	24210	10189	1380	35779	1058	36837
2016-17	29106	11092	1407	41605	1111	42716
2017-18	34706	12009	1435	48150	1167	49317
2018-19	42026	13003	1464	56493	1225	57718
2019-20	46229	14080	1493	61802	1286	63089
2020-21	50851	15247	1523	67622	1351	68973

(Source: DIAL report 2012- 2021)

3.6 Growth Strategy

The Internet of Things (IoT) and Operational Technology (OT) have provided a smooth process and enhanced systems for the networking of aviation systems. The creation of 'smarter-aircraft, airports' has given rise to a great deal of passenger satisfaction and experience. After steady growth at the end of the 1990s, the industry withered a sharp turnaround following a global economic recession in 2001. The horrific episode of 9/11 did not deter the growth in long term. However, the loss was exacerbated by the Iraq war and the SARS outbreak. Full-Service Carriers (FSC) adopted different restructuring models to survive and remain profitable in the business. Large number of Airlines had to implement aggressive cost-cutting and fleet rationalization initiatives that are struggling to keep afloat. The circumstances of the FSCs have changed even further with the arrival of budget couriers in the United States and Europe. However, lowering of fuel costs and significant increase in traffic and increased charges made a significant contribution to aircraft revenue.

Subsequent sustainability, however, has not yet been achieved due to fluctuating fuel prices. IATA reported a cumulative loss of $36 billion over the previous four years. It was projected to be a 5% rise in global air traffic worldwide before outbreak of Corona. Growth is expected to be more apparent in emerging economies such as India and China. According to one study, there has been only 2-3 per cent of annual sales growth since 1970. Such slow revenue growth is of serious concern under the burden of growing aviation.

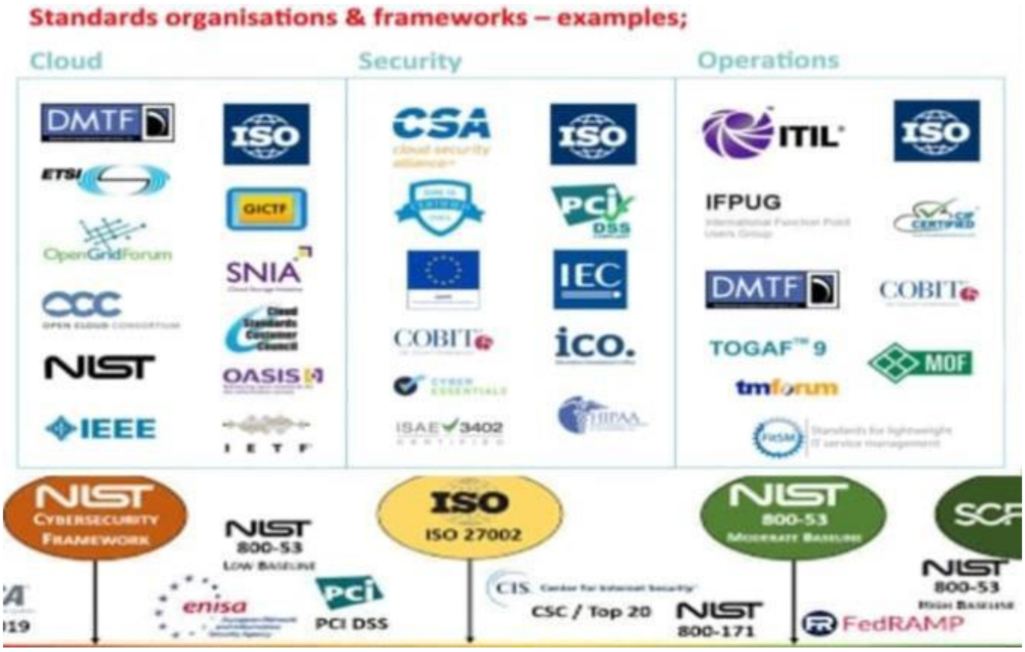
However, there is room for industrial integration to reduce distribution costs and adjustment costs. In general, restructuring is the only way to fix business overcapacity and low finance levels. From terrorist threats to strategic positions, if there is a sector that appears to be at the forefront of global security and cyber risk, it is aviation. While considered to be the safest means due to its large international regulatory structure, incidents of aircraft accidents have been very frequent and have drawn a great deal of media attention. Among the recent attacks on Malaysian Aviation, separatists have targeted Ukraine from Amsterdam to Kuala-Lumpur. Emerging technologies, "the evolving nature of the war, the position of the actors and the reliance on cybernetics are evolving the nature of the risks, putting pressure on the sector to ensure that it retains its level of security."

In order to protect the aviation industry all States must necessarily undertake a risk assessment in accordance with the relevant national authorities. All countries will have to ensure that Airline companies comes up with secure Airplanes. Recently there was a case of Boeing Max series 7000 which had to be grounded later for deeper investigation into its inbuilt algorithms for attack angle of wings which could be changed. Continuous training and development of employees to implement various aspects of the national airport security program to identify their simple information in the communication and data systems. Includes risks and disadvantages in their comparison with nature and safety system, which may include, but are not limited to, safety net, supply storage, network allocation and remote access management, as required. "The threat of cybercrime cannot be ignored, particularly with regard to the fully automated and digital civil aviation sector. Government agencies and other administrative bodies have a certain obligation to address these risks. There is requirement to focus security efforts on consistency with existing guidelines. In any event, as guidance must set aside some effort to represent knowledge on new threats, this may lead to an end to the development of hazards that are being negotiated. Every single node of the network whether small businesses, ticketing, baggage handling operations, entry-exit, Wi-Fi systems, BYODs should be monitored to prevent and encourage people like script kiddies/ gamers to infuse and malign the vulnerable connection into the system. By and large the networks are secured, still being aware of the need to share their findings on previously unknown vulnerabilities and best practices for managing them, particularly in the IT sector, better mechanisms are needed to facilitate this collaboration and thus employee engagement becomes a supreme important factor. Much more could be done to mitigate risks and, at the same time to create a smoother travel experience by promoting what some have termed a global network of trusted travelers to speed up secure cross-border movements, by establishing guidelines for the exchange of 'data usage' which may involve notification of missing travel documents. These initiatives could theoretically address the current challenges.

CHAPTER 4

AVIATION CYBER PHYSICAL SYSTEMS AND INTERNATIONAL PROTOCOLS

4.1 **CYBER SECURITY FRAMEWORK** There are many significant Cyber security frameworks used across world in many domains. Aviation cyber security is one of the most complex and secured system systems and divided into three major architectures and these are: Cloud, Security, and operations. The figure below shows various Cyber Security frameworks and the companies involved in the domain globally.

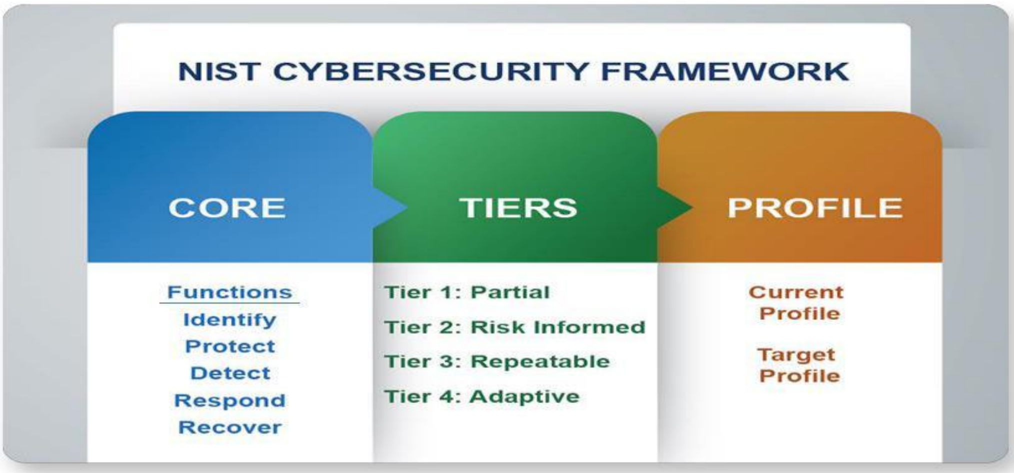


(Source: Stanford Center for Professional Development)

Figure: 4.1 Standards organisations & frameworks

It must also be impressed that the aviation sector, which is one of the most powerful and sensitive sectors, is part of the government's critical infrastructure.

United States Post-September 2011 attacks on the World Trade enter notified empty Presidential Directives Order (PDP) 21 in Feb 2012 and Executive Order (EO) 13636 for Homeland Security Enhanced Cyber Security Services (ECS). The plan is to be applied to all key infrastructure sectors. Through ECS, DHS will help critical infrastructure entities reduce their cyber risk and ensure more effective security for sensitive data and critical systems.



(Source: VTE, DHS on Critical Infrastructure Security)

Fig 4.2 NIST Cyber Security Framework

The framework shall consist of three parts:

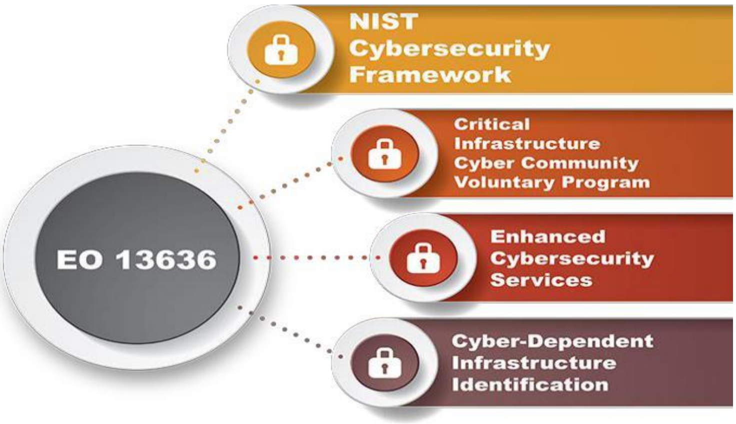
(a) Core Framework

(b) Tiers of framework implementation

(c) Frame Profile

System Core is a collection of information security standards, reports and detailed references that are common across critical infrastructure sectors and provide thorough guidance on the production of individual organizational profiles. Translation: The center discusses best practices and what you are expected to do. Tiers provide a framework for companies to view and assess the characteristics of their approach to managing information security risks. The Councils help you determine how well you are doing.

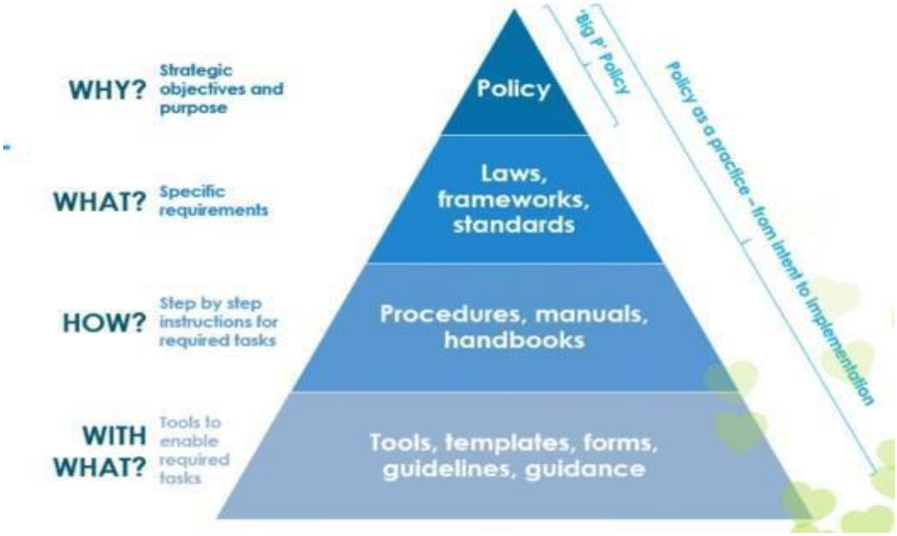
Executive Order (EO) 13636 was signed by President Obama on the same day that PDP 21 was signed. While PPD 21 generally discusses critical infrastructure security, EO 13636 focuses explicitly on cyber security. To this end, EO 13636 guided four major Cyber Security initiatives:


EO 13636
NIST Cybersecurity Framework
Critical Infrastructure Cyber Community Voluntary Program
Enhanced Cybersecurity Services
Cyber-Dependent Infrastructure Identification

(Source: VTE, DHS on Critical Infrastructure Security)

Figure: 4.3 Critical Infrastructure Security

Cyber Security covers the risks of ransom ware, mass theft and hacking, licensed software interference, denial of government attacks, surveillance, and nation-state war demonstrations. Any policy developed must address the following five policy and practice implementation issues:


WHY? Strategic objectives and purpose
WHAT? Specific requirements
HOW? Step by step instructions for required tasks
WITH WHAT? Tools to enable required tasks
Policy
Laws, frameworks, standards
Procedures, manuals, handbooks
Tools, templates, forms, guidelines, guidance
'Big P' Policy
Policy as a practice – from intent to implementation

(Source: Stanford Center for Professional Development)

Figure: 4.4 Five Policy & Practice

4.2 <u>OTHER PROTOCOLS USED IN THE AVIATION INDUSTRY</u>

Protocol has been in use since 1978 for communications within the Aircraft. Furthermore, the use of radio frequencies such as VHF, HF and SATCOM continues to be used for directional navigation. Currently, ACARS Messaging Security (AMS) has a vulnerability where details of flight, flight code, landing and take-off timings can be identified and identified. ACARS also transmits extensive data on aircraft system failure. The benefits of the ACARS analyzer are real-time connections to Sky spy, Air Nav, JACARS, etc. It also has the option of recording empty data messages; it also has the advantages of customizable airline / aircraft / route / flight lists. It provides the benefits of data alerts for registration, flight numbers, etc. However, some of the drawbacks recognised by the program were that warnings were only available in online mode. The online mode is not compatible with the data analyser mode.

A large amount of data made it possible to collect data only up to one month in real time. Absence of detailed geographical reports, the incoming data filter is a system problem coaxed. The dynamics of Cyber Security have increased to multiple dimensions.

System Wide Information Management (SWIM) has redefined security issues in a variety of ways by improving network dynamics and building a robust system (SoS) effectively. It successfully addressed the emerging security risks facing the aviation industry. In any case, information sharing quantifies the management of security threats, and attacks and techniques are still accessible across such a SoS network. It recognizes the perspectives and requirements of national security operations. The aim of this research is primarily to increase and initiate a cognitive domain outside the scope of technology in order to understand the overall travel system as a dynamic element that can still be penetrated to cause a major catastrophe. It is this consciously enhanced and conscious mind that can determine the attitude and actions of either detecting or avoiding any such incident that may cause imperfections or the eventual destruction of an aircraft.

4.2.1 Defining the Cyber-Physical System (CPS)

CPS monitors the involved physical processes and actuates actions accordingly to restructure or change the physical environment for better. The ‘physical’ and the ‘Cyber System’ constitute two of its major components. This system involves the supervision of multiple processes in a network system. The devices installed is used to monitor sensing, computing, and communication.

The U.S. Federal Aviation Administration, has several times in recent years, have reported incidence of breach. Incidences of breaches have been further confirmed by Central Intelligence agency (CIA) report, which affirms to intrusion of hackers interrupting the power system in several regions. This tool can stop the car engine remotely, and meantime, it makes the car working. It is true the black hat guys have started venturing into this domain for a significant result and the fame associated with the risk involved.

4.2.2 Vulnerabilities of CPS

CPS is still evolving, encompassing new domains like sensor networking, Wi-Fi routers and its vulnerabilities, Operational technology, IoT, software integration and much more. There persists vulnerability with regard to the networking operations capability with CPS. The technical know exists however it is the man behind the machine who matters in successful implementation of safety measures. Thus, ensuring secured interaction between the systems remains a concern for cyber-physical systems. New security issues have surfaced, with the advancement in technology, which requires identification of the possible vulnerabilities and approach with an attacking model. Ciholas (2016) in the paper entitled “Composite vulnerabilities in Cyber Physical Systems” has emphasized on assessing composite vulnerabilities within CPS. With its increasing applicability in cross-cutting domains, the complexity of CPS vulnerability is expected to further aggravate.

The paper suggests identifying single vulnerabilities and its interaction, to assess the possible composite vulnerabilities. This methodology can possibly evaluate the severity, impact and possible countermeasures in response to composite Vulnerability. The method can essentially be also implicated in the aviation segment as well. The evident property of CPSs constitutes functionality, performance, dependability, and security cost. Further, the pattern of its uses, management and adaptability determines its dependability. The physical environment also constitutes an important feature for securing the communication channels.

4.2.3 The Application Domain of CPS

CPS provides to be an efficient means of safety in multiple domains. CPS could be applicable in multiple aspects “like infrastructure control, safe and efficient transport, networking, manufacturing and agriculture.

(a) **Generic Architectures for CPSs:** This "CPS Architecture" will provide for a clear structure Aviation industries. The software offers an initial approach to the relevant related definition, but it should be supported by the CPS. The intertwining of cyber-physical elements warrants analysis of the behavior of the system. It further enlightens the cyber world through the representation of events and information as abstracts of the real physical world.

Following are the components for the Generic Architecture:

(i) **Global Reference Time** - “The next generation network provides the Global Reference Time which should be accepted by all CPS components”

(ii) **Event/Information Driven** - “The events/information are the “raw facts”, processed as a form of abstraction of the physical world through controlled systems like the CPS.

(iii) **Quantified Confidence** - It involves a standard procedure of validating the events/information at a given specific time

(iv) **Publish/Subscribe Scheme** - Each CPS control unit subscribes interesting events / information based on its system targets and publishes necessary events / information.”

(v) **Semantic Control Laws** - “The specific law regulates system behavior in the environmental context of CPS.

(vi) **New Networking Techniques** – “It makes the delivery of technologies like global reference time, new event/information routing and data management schemes a simple wave. In a study titled West End Palmer (2006), "A software architecture application for the next generation of cyber- physical systems proposes a CPS development based on specific service collection. The way to communicate and disconnect between services is well recognized.”

(a) **CPSs Design Principles:** The aim of Lee (2008) and Baheti (2011) is to define certain principles of CPS design, to analyze addressed consists of three main disciplines: control, systems and software engineering. It also indicates that the interdependence of CPS materials limits the structure of the design process.

(b) **CPSs Modeling:** CPS modeling epitomizes the key to the system’s application. CPS modeling, in recent years has evolved acquiring new tools like meta-modeling and meta-programmable techniques and were chosen for the following reasons:”

(i) "Enables interaction between material and observation.”

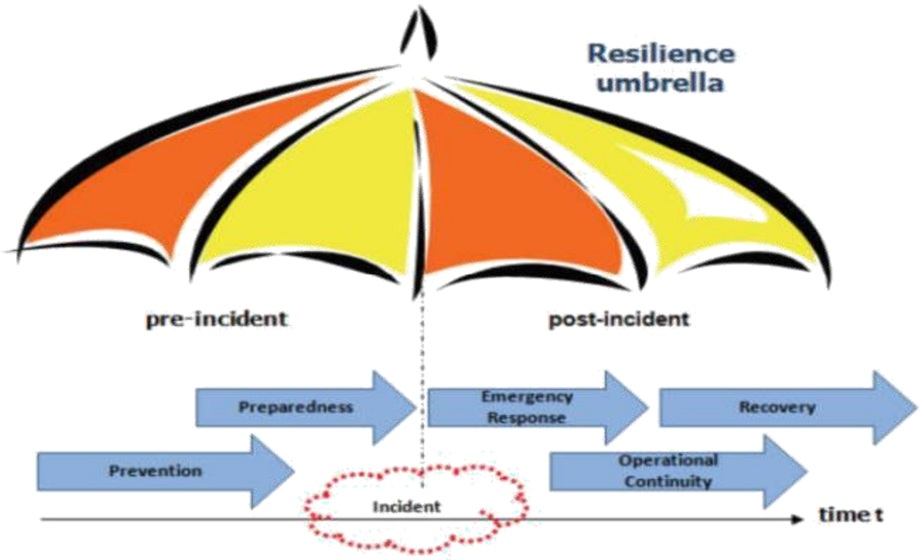
(ii) "Events are based on the concept of partial discipline that reflects physical reality.”

Therefore, autonomous agents and interactive agents form two compositional models, which require a cumulative approach for its understanding.

(c) **CPSs Dependability:** The definition is based on the criterion for deciding the dependability of the provided services. The attributes of dependability are contingent upon the safety, confidentiality, and integrity of its services. Fault prevention, tolerance, removal, and forecasting constitute the means to achieve dependability.

4.3 CYBER RESILIENCE IN THE AVIATION CONTEXT

It is evident that resilience eludes more from risk management than from its elimination. Being resilient indicates a reduction in attack protection. It adheres to several levels of action taken to protect against attacks. These methods are aimed at rightful solutions against the attacks.



(Source: Aviation Cyber-Security and Cyber-Resilience: Lykou Georgia-2019)

Figure 4.5: Cyber Resilience

The above-mentioned figure illustrates the resilience umbrella; it addresses the adequate measures applied throughout an attack. The development of services, tools or the concerned system accentuates the flow of cyber resilience actions. As preventive measures, it regulates the threats emanating from SOS. Improving the standards of staffs with adequate training facilities can be decisive in anticipating possibility of attacks. To ensure "Preparedness" the activities need to be conducted in organized manner, while also being aware of latest software tools to ensure security. It is essential to respond under the attack, and it did under the point of Emergency response. It primarily concentrates on recognizing the concern prevailing and remove it. This step includes limitations of service. Furthermore, the recovery phase must ensure the necessary tools to recover from a possible cyber-attack. The application of resilience engineering has not yet been expanded significantly with respect to Air traffic management. However, the aerial project for Air

Traffic was aimed at analyzing and evaluating a comprehensive risk assessment of the complex infrastructure of air traffic. Stability is seen as a system power to maintain strategic distance from damage and to protect, reduce and restore. It proposes a digital risk investigation process to develop digital stability, sustainable capabilities of the extraordinary all-round transportation system. The recommendations in the project report are identified as fundamental to the use of stability in air transport, recorded and explained below. A new structural process must ensure the combination of old-fashioned data security and new improved cyber operational stability systems. This can help air traffic agencies meet the growing cyber threat and meet information security rules and standards.

The currently applied adhoc ways of threat regulation needs to be replaced with utilization of systemized process. Means of controlling Air space Cyber threat scenarios need to adopt similar approach. Collaborative meta-models for data exchange need to be further standardized. Further tool-based analysis is required for the integration cyber based findings. The dynamic risk analysis techniques depict the semi-computerized analysis. This strategy empowers to dynamically demonstrate and break down cyber risks in complex systems or organizations.

The remarkable capability of “this methodology permits a wide, powerful Cyber risk assessment in the air transport sector. Ensures security and security continuity and empower cooperative strategies. Cyber-attacks can directly affect safety-basic system capacities, subsequently, the extension of an exhaustive risk the board approach is recommended.” The rebuilding of designs of sociotechnical systems could support cyber versatility notwithstanding defensive measures.

The new methodologies center on complex systems must be stretched out in a specialized sense towards strengthening the cyber capacities. The Significant parts for consideration are Development of infrastructure for continuous change; Ideas for reducing system design and recovery techniques and expanding system capabilities to support cyber-attack detection. Simulation methods help to analyze the risks of complex threats and cyber security. Moreover, using human-in-the-loop simulations is crucial to identify potential human factors responsible for possible cyber-attacks. There is a fundamental difference between the recommendations of stability from cyber security discipline, which in most cases manages a solitary level. Stability, in all respects, seems to be a combination of the community, integrated efforts and the development of the current cyber security system. The institutional level is regularly associated with the work of communication staff and interdisciplinary procedures for all recommendations to ensure a collective and efficient business balance. To advance a common cyber stability system in the air transport sector, the long-term process should strengthen the level of technical, institutional, social and economic stability. This cyber stability system can guarantee improved preparation, system-oriented and effective.

4.4 REALITIES AND CHALLENGES OF NEXT GEN AIR TRAFFIC MANAGEMENT: THE CASE OF AUTOMATIC DEPENDENT SURVEILLANCE-BROADCAST (ADS-B).

Contemporary times has seen the rise in Air traffic and is further progressively increasing across the world. The next generation Air traffic navigation system has proved to be modern and away from conventional guidance systems. ADS-B, the current technology has been the most secured so far in the field of navigation however challenged in the digital age.

The improvements recommended are pivotal to address those worries as they represent a significant problem for the future across the board deployment of the protocol. There are vulnerabilities in ADS-B, which are inalienable to the communicated idea of unbound RF communication. With the approach of modest and available software-defined radios and a set of nominal hardware for gathering Air traffic communication leading to following assessments:

(a) **Vulnerabilities of the ADS-B Data Link**: Any disabled opponent decoders can search for ADS-B messages. Nevertheless, an attacker who can effectively disrupt at the ATC correspondence represents a more dangerous security. The results show that an attacker has full control over the remote correspondence channel and can voluntarily infuse, delete, and change any ADS-B message. Some dynamic attacks can be controlled, standard off-the-rack hardware: such as ground station flooding: Continuous jamming attacks on 1090MHz channels will encourage high luck and message deletion. This will lead air traffic controllers to change more experienced, less accurate surveillance systems with potentially fatal consequences, especially in high-altitude airspace around the notable public air terminals.

(b) **The Ghost Aircraft Injection/Flooding**: 1090-Megahertz channel can be used to infuse fake ADS-B messages with an existing aircraft (supposed ghost) guarantee. Any actual ADS-B recipient would consider these fake messages as obscure from the original aircraft, which would cause risky confusion for both the pilot and airport control, especially under the weak mark when the device is most dependent.

(c) **An Aircraft Disappearance**: Deleting all ADS-B messages sent by a specific aircraft will completely disappear from the ADS-B application. Attacks are more subtle and sophisticated than simple; However, regulators need to rely on less accurate surveillance systems, such as PSR, to defeat the first objective of ADS-B. Any attack that requires a message to be deleted or changed is increasingly unexpected over time. On the other hand, ADS-B messages can be easily changed. ADS-B messages are changed to create false alarms.

(d) **Aircraft Spoofing**: Each aircraft is identified by a 24-piece detector by ICAO, which can be changed with the message deleted and the infusion attack mixture. In the case of transportation framework, the utilization of COTS advancements increases in aviation and thus situations found in ICS become increasingly irregular. It introduces a resistance inside and out approach and stretches out to route and surveillance at a calculated level yet does not manage explicit systems.

4.5 CYBER INCIDENTS IN AVIATION SECTOR

The history of Cyber-attacks into the aviation industry and major cyber-attacks across the world in last 20 years is attached in **Appendix 'C'.**

4.6 CYBER THREAT: AVIATION CONTEXT

Current trends do not spare any Industry from cyber-crimes and so there is on this Aviation industry too as well however the main issue revolves around its nature of operation and the scale of disruptions. An aircraft of the likes of make Boeing had to be put down because of the error in technology settings and prone to the hack. It is challenging to hack all operations under ACARS, however there exists a vulnerability as on today. As a consequence, an intruder with a broad knowledge and intelligence of the operation of the aircraft could cause disruption.

In another similar case, integrity of SATCOM devices is still to be established in the current threat scenario. There is a need to resolve the need for the sector to be digitized. The objective of reducing labor costs, for example. Compared to other sectors, two examples of information security breaches are likely to be seen:

(a) **Opportunistic:** The aim is to reduce errors made by inner employees handling the IT systems to create a nuisance to an entity associated with the flying ecosystem.

(b) **Calculated and Premeditated:** It involves a malicious attack to obstruct operations or endanger lives. It is form of terrorism using the cyber platform.

In addition, the platform will offer realistic solutions and digital access to workers and travelers. As a result, this progression the increasing complexity of software in all industries. Ten times the number of flight software codes has increased in the last 10 years. From 1960 to 2000, the functionality of pilot software increased from 8 per cent to 80 per cent. Thus, complexity of the system is always at a high risk of breach. The significant efforts made by these stakeholders to safeguard the system are the following.

(i) ICAO encourages better and stronger collaboration among all the stakeholders to recognize the possible threats.

(ii) ICAO likes to encourage countries to implement a strong cyber security strategy and management. The goal is to implement more policies and measures to prevent any cyber-attacks, which includes aviation resilience and crisis management. Many nations have started to work on cyber security in recent years. Several airports have invented to implement measures for cyber security problems for future projects.

4.7 CYBER SECURITY CHALLENGES FOR THE AVIATION INDUSTRY

Airports as a critical infrastructure faces threat from all sides whether physical in forms of sabotage but also cyber threats. The threat vectors now have shifted from physical security and intelligence gathering to Anonymous and all types of computing devices including mobiles that too have become hazardous if exposed to malicious traffic.

Security strategies focus primarily on aircraft control systems. Independent agencies that look deeper into aviation cyber security issues are given as under:

(a) Aircraft Electronic Engineering Committee (AEEC),

(b) Subcommittee on the health of aircraft details

(c) Radio Technical Aviation Commission (RTCA),

(d) Aviation Radio Incorporated (ARINC)

(e) The European Civil Aviation Equipment Organization (EUROCAE).

The DHS Transport ICS Cyber Security Policy Strategy has recognized cyber security at ICS Airport as a modern concept. The Airports Council has proposed to cooperate with the International-North America (ACI-NA) Business Information Technology (BIT) Committee to strengthen the cyber security standards of ICS Airport. ACI-NA Bit Committee is a forum of stakeholders with airport-related IT obligations in line with networking, connectivity, information sharing, research management and most advanced technological advancements.

The US Airports Co-operative Research Program (ACRP) is unveiling a plan to help the airport develop a cyber-security program. Its multimedia content will highlight various cyber security alerts and indicate risk awareness.

4.8 CYBER THREATS TO INTERNAL AIRPORT OPERATIONS

There are around 450 business air terminals, including 19,000 new air terminals all through the United States. Business air terminals have varied fluctuating degrees of security identified into various zones. It is possible to have vulnerabilities among these zones. The very nature of IoT systems does make it vulnerable to cyber-attacks however robust are to be policies and routine audit check. Apart from the conventional IT framework, the potential for digital attacks in an air terminal persist among the following:

(a) E- Enabled aircraft systems

(b) Credentialing and document management systems (CAD, blueprints)

(b) Radar systems

(c) Ground radar

(d) Network-enabled baggage systems.

(e) Wireless and wired network systems.

(f) Heating, Ventilation and Air conditioning Systems HVAC

(g) Supervisory control and data acquisition (SCADA) type ICSs

The future intelligent terminal will improve communication infrastructure that will help the next generation of e-active aircraft in the air transport system.

That plays an essential role in every level of government, private and government. Therefore, the airport can help local, state, and federal law enforcement agencies ensure proper response and analysis of their existing relationships."

4.9 THE REVIEW OF WORLDWIDE PILOTS ON CYBER THREAT WITH REFERENCE TO INTERNATIONAL FEDERATION OF AIR LINE PILOTS' ASSOCIATIONS

The IFALPA Security Committee saw the event of a digital assault on an aircraft a ground office or any other basic framework as a noteworthy and developing hazard. The purpose of this section is to express this threat and to suggest quantifies in which it can be used. This information is used, not just for the standard activity of the aircraft. However, it can be used in a similar way to provide sustenance and support energy. Co-operative operators and Air traffic specialists gather a lot of dangerous and even classified information about their workers and travellers.

This security system is expected to provide protection for a long term. Programming Providers (counting firmware) and working frameworks ought to have the option to communicate adequate safety efforts that can shield from both internal and external threats. Additionally, applications ought to be exhibited to work just in their proposed way. The broadening of working frameworks may diminish vulnerability.

4.10 NATIONAL STRATEGY FOR AVIATION SECURITY: UNITED STATES

(a) **Strategic Objectives:** It adheres to the principles of values embodied in the law applicable to National Security Presidential Directive 47 / Homeland Security Presidential Directive 16 (NSPD-47 / HSPD16) and other national strategies. It outlines a strategic vision for aviation security while identifying ongoing efforts and directs the production of the National Strategy for Aviation Security and Support Plans. Support plans cover the following areas: aviation transport system security; Aviation operational threat response; Aviation system recovery; Air Domain Surveillance and Intelligence Integration; Domestic and international air Traffic. The following four goals guide the country's aviation security operations:

(i) To protect the United States and its global interests in the air climate, the country's global interests must be protected by terrorism, crime and violent activity, crime and violent activity, crime and violent activity, physical, spectrum-based or cyber-transport.

(ii) "The increase in the safety of the air transport infrastructure and the economic impact of the United States are effectively required to implement significantly higher security in the internal system".

(iii) Improve stability, reduce damage and improve recovery.

(iv) "The United States must take steps to reduce damage and recover from the attack on the air base. Training and national reduction and recovery plans can maximize coordination in aircraft infrastructure. These are the key to active recovery. It creates measurable feedback choices to ensure a flexible and fast recovery transport infrastructure that reduces conflicting safety and financial outcomes (for example, the separation of the Aviation Transport System (AS) to a certain section. When a disturbance occurs, federal-state-local-sub-national and regional (FSLTT) departments and private sector agencies must be prepared to take urgent action to ensure the continuation of operations, the potential national security impact of essential public services. The Federal Emergency Management Agency (FEMA) controls the role of the federal government, including prevention, response, response and recovery from all internal disasters, including natural or humanitarian activities. The National Cyber Accident Response Plan and another appropriate policy will respond to cyber incidents, Strategic operations to maintain a safe, safe, efficient and efficient air transport infrastructure.

(b) **Maximize Domain Awareness:** It decided to prevent counter-terrorism attacks, protect the United States and its global interests in aviation ecosystems, and reduce the consequences of attacks. It has incorporated air surveillance data, intelligence from all sources, law enforcement information and is deeply subject to sophisticated data collection review and sharing.

(c) **Threat vectors and Vulnerabilities Aviation Eco-system:** The lack of expected intelligence and process inconsistencies has led to various reactions such as the Aviation-related printer Cartridge Bomb Plot (2010), Indoor Bomb (2009 and 2012), Sept 2011, WTC attack and The Dalo Aviation (2016) internal attacks. The advance countries like US have faced such attacks in past and threat looms over the global aviation industry.

CHAPTER 5

RESEARCH METHODOLOGY

The research approach adopted in this chapter was deduced mixed survey from the participants in classroom and online survey through snowballing of the passengers flying through Delhi Airport. Aviation involves all stakeholders from the Airline to the Airport Authority to the Government, the Security Force, the Central Industrial Security Force (CISF) in our country, and the largest are travellers or passengers. Despite all the technical policies and frameworks in place, it is the people who manage this process, and these people must remain technically and ethically integrated into the process. In addition, it is important to know and understand the travellers perception travellers must be made aware of the cyber risks associated with this transport model. We saw the recent COVID-19, when the worlds over Airlines were stopped simply because of a virus that was becoming contagious even from a third-party touch. Since, it was a rare and first-time occurrence, a global pandemic has been declared and approaches to deal with are still being discussed rather than being aware of it.

The survey was conducted to understand the opinion of passengers on the adequacy of cyber security measures at Airport at the present time. The format of this survey and other details, including the questionnaire, are provided in the Appendix. The data received from the survey shall be treated with confidentiality. In this chapter, we present the current methodologies adopted as necessary in the context of this research to begin with the problem statement, research design, research hypothesis, validation of the survey instrument, questionnaire items used for constructs, development of the structured equation model, data analysis, validity and reliability, statistical techniques for systematic analysis of data.

5.1 PROBLEM STATEMENT

To appreciate Business Loss in Indian Aviation Industry due to Cyber disruptions.

5.2 RESEARCH DESIGN AND ITS STRATEGY

According to BT Basavanthappa, “The design of the research is the method, layout and strategy of the research to solve the research question, which is the overall plan or blueprint chosen by the researcher to conduct the analysis”. The choice of research design is a very crucial step because it provides the basis for the study. Research design is a type of statistical analysis used by researchers to select topics, manipulate independent variables, control, data collection and describe data. In this section, we describe the methods used for Gaussian testing and evaluation and which model is most effective to predict the motivation of users to remain alert and conscious while travelling and developing cyber secure behavior.

5.2.1 Research Problem:

Protection Motivation Theory framework has not been applied in the Aviation Cyber Security.

5.2.2 Research Questions

(a) What are the factors affecting perception management of Aviation Cyber Security?

(b) How Aviation Cyber Security studies can be linked with Protection Motivation Theory framework?

5.2.3 Research Objectives

Based on the need and scope of the research, the following are the precise objectives of the study:

RO1- To ascertain the identified factors of Protection Motivation Theory applicable for Aviation Cyber Security. This can be explored through various questions given as under:

(i) Does perceived threat severity affect Aviation Cyber Securi

(ii) Can perceived susceptibility affect Aviation Cyber Security?

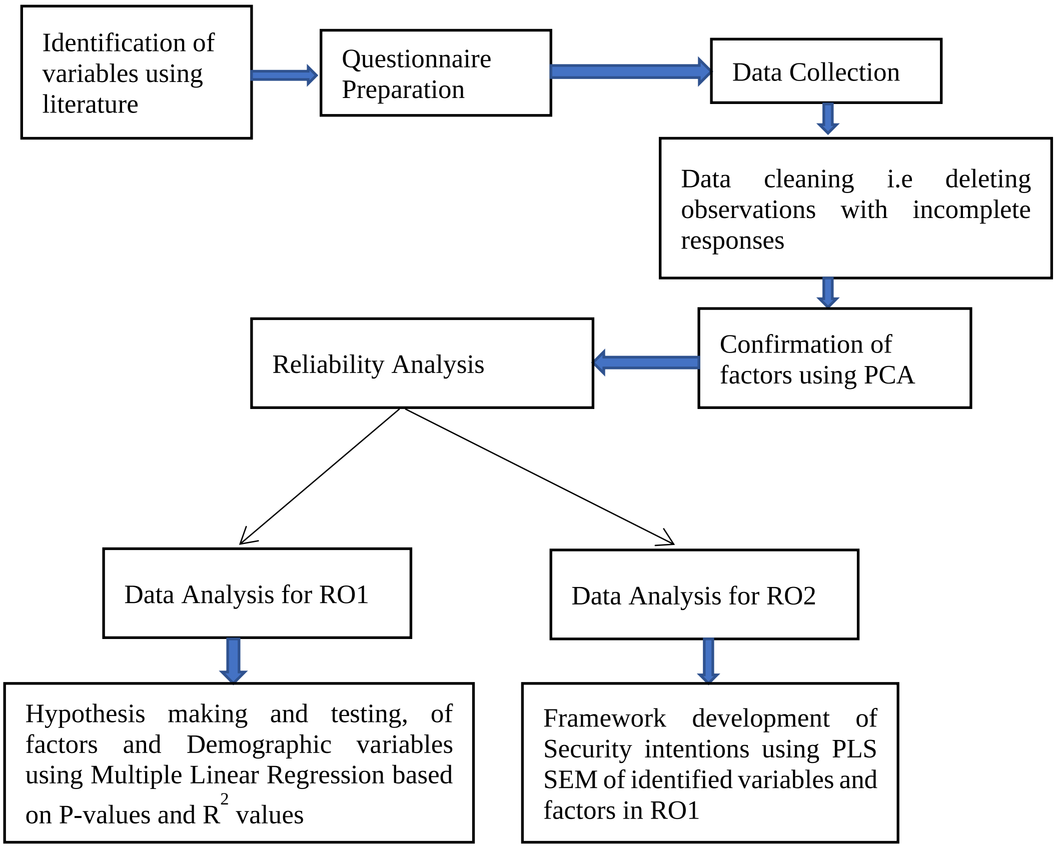
(iii) Will prior experience with online safety hazards affect Aviation Cyber security?

(iv) Do self attributes affect Aviation Cyber Security?

(v) Will demographics (gender, age, education) of the passengers affect their Aviation Cyber Security behavior?

(vi) Does frequency of flying affect Aviation Cyber Security?

RO2- To develop a framework using Protection Motivation theory for Aviation Cyber Security.


Identification of variables using literature
Questionnaire Preparation
Data Collection
Data cleaning i.e deleting observations with incomplete responses
Confirmation of factors using PCA
Reliability Analysis
Data Analysis for RO1
Data Analysis for RO2
Hypothesis making and testing, of factors and Demographic variables using Multiple Linear Regression based on P-values and R2 values
Framework development of Security intentions using PLS SEM of identified variables and factors in RO1

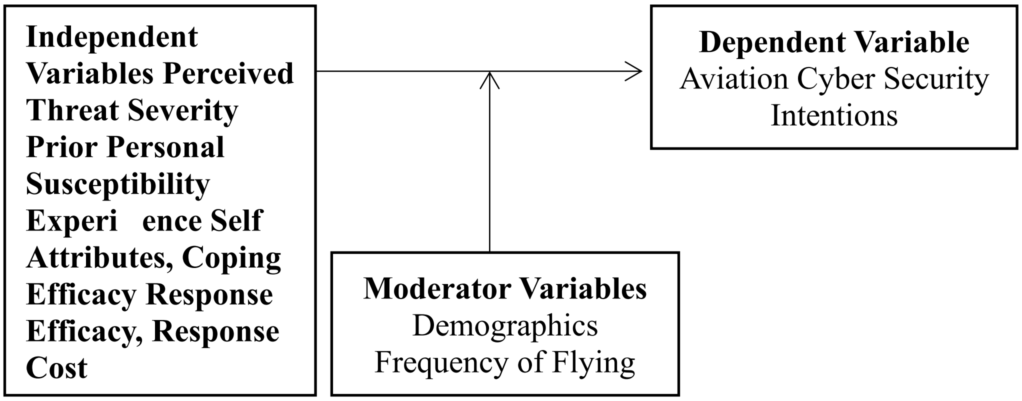
(Sources: Researcher own)

Figure 5.1: Research Design and its Strategy

5.3 RESEARCH METHODOLOGY FOR RO1

Table 5.1 Procedure Used for Research Methodology RO1

Philosophical Assumption	Protection Motivation Theory
Type Research study	Qualitative & Quantitative
Role of researcher	To interact with air travelers flying through NCR, data collection, and compilation and deeper study of subject.
Sampling framework	Age gp 20-50 yrs; three months' time frame (Oct-Dec 2017); Random Sampling. Sample size will be 384 as population is more than 01 lakh. (Daryle, 1970)
Data collection procedures	Through Structured Questionnaires.
Tools	Hypothesis Testing through Regression (Mean, SD)
Research Design	Descriptive Design, Structural Equational Modelling using PLS SEM tool.


Independent Variables Perceived Threat Severity Prior Personal Susceptibility Experi ence Self Attributes, Coping Efficacy Response Efficacy, Response Cost
Dependent Variable
Aviation Cyber Security Intentions
Moderator Variables
Demographics
Frequency of Flying

(Source: Researcher Own)

Figure 5.2: Hypothesized Model, Sources: Researcher Own

5.3.1 Data Collection

Data Collection about the steps are available at the request of the authors. We have created survey questionnaires, methods and questionnaires of participants based on a literary study using the International Database. This information is collected on previous experiences such as security measures, perceived threat intensity, perceived threat potential, security risks, self-attributes. This construction is measured on a 5-point Likert scale and the scale adapted from previous research. Question Paper is attached as Appendix.

5.3.2 Instrument Development: Data was collected on abstract concepts such as Security Measures, Perceived Threat severity, Perceived Threat susceptibility, Prior experience with safety hazards, Self Attributes. These constructs are measure on 5-point Likert scale and on scales adapted from previous studies. Questionnaire is attached as Appendix A

Table 5.2 Instruments Variables Details

Construct	Adapted From
Security intentions/ Measures	Tsai et al., (2016); Anderson and Agarwal (2010), Liang and Xue (2010)
Threat Severity	Tsai et al., (2016); Liang & Xue (2010)
Threat susceptibility	Liang and Xue (2010); Tsai et al., (2016)
Prior experience with safety hazards	Tsai et al., (2016)
Personal responsibility (Self Attributes)	Tsai et al., (2016), Anderson and Agarwal (2010)
Coping Efficacy	Tsai et al., (2016), Anderson and Agarwal (2010)
Response Efficacy	Tsai et al., (2016), Anderson and Agarwal (2010)
Response Cost	Tsai et al., (2016), Anderson and Agarwal (2010)

(Source: Researchers Own)

5.3.3 Sampling Method

The sampling method used was random convenience for passengers flying from Delhi Airport from an age 18-30 years given by Daryle, 1970 in small sample techniques.

When population is known and finite:

$$S = X^2 NP (1-P)$$

$$\overline{}$$
$$(d^2 (N-1) + X^2 P(1-P))$$

Where S= required sample size
X^2= 3.841 (The table value of chi-square for one degree of freedom at the desired confidence level= 3.841(1.96x1.96))

N= Population Size

P= The population proportion (assumed to be 0.05, this would provide the max sample size).

For our study—Population is 570 lakh Air Traveler's in a year from DIAL d = Degree of accuracy expressed as a proportion (.05) Thus, 570/12*3=36 lakhs for three months, S=384

Approximately 500 samples were floated offline and online and after data cleaning the sample size analysed is 298.

5.4 DATA ANALYSIS TOOLS

Data on nominal/ categorical variables such as demographic variables will be summarized through frequency tables, cross tabulations and pie charts.

(a) Data collected on interval scale measures will be summarized through mean and standard deviation.

(b) Validity of the scales used will be tested using confirmatory factor analysis. The reliability will be then tested through Cronbach’s Alpha.

(c) Hypothesis testing will be conducted by multiple regression analysis, taking Aviation Cyber Security Intention as a dependent variable and perceived Threat Intensity, perceived Threat Susceptibility, Previous Safety Risk Experience, Self-Attribute (Personal Responsibility), Coping Effectiveness, Response Efficacy, Response Costs as Independent Variables and Demographics, and Duration.

(d) The framework will be made using structural Equational Modelling using PLS tool.

5.4.1 PMT variables

The PMT variables are: Threat Severity, Threat Susceptibility, Coping Self-Efficacy, Response Efficacy, Response Cost, Prior Experience, Personal Responsibility and Security Intentions.

Table 5.3 PMT Variables /Constructs

Constructs	Definitions
Threat Severity	Compromise of own mobile device or the personal data to bring any threat to Aviation security
Threat Susceptibility	Vulnerability into the Airport Cyber-Physical systems
Coping Self-Efficacy	Adequate measures and security protocols adopted by the Airport
Response Efficacy	Adequate preventive measures taken by passengers
Response Costs	Any added costs for providing safe environment
Personal responsibility	Awareness level of passengers
Prior Threats	Personal exposure to Cyber nuisances

(Source: Researchers Own)

Based on PMT model hypothesis are as follows: Further our current study involves study of demographic variables and frequency of flying as moderating variables affecting aviation cyber security intentions.

5.4.2 Validation of the Survey Instrument

In order to measure the various identified dimensions identified using the PMT framework an email survey was conducted, since it was not possible to obtain responses from airline passengers outside any airport or inside the airports in India. So, the survey was first sent via email to few know people who travel by air and then were asked to further snowball the survey to other such people in their circles. 108 Surveys was taken online and balance by meeting people physically. In duration of four months, 297 responses were obtained from the survey.

Table 5.4 Shows the Demographic Profile of the Respondents and their Frequency of Flying: Demographic Profile

Variable	Categories	Frequency
Gender	Male	237
	Female	60
Age Groups	18-30	93
	31-40	63
	41-50	114
	51 and above	27
Education Level	Graduate	48
	Postgraduate	180
	Postgraduate+ above	69
Frequency of Flying	11 or more times in a year	24
	6 to 10 times in a year	54
	2 to 5 times in a year	84
	Once a year	135

(Source: Researcher Own)

To measure the respondents' threat severity, a 7-item scale was developed, "taking questions from measures earlier developed by Tsai et al. (2016) and Liang and Xue (2010). The items in the measure asked the respondents to agree or disagree with the statements, which are considered as cyber security threats caused by malware such as viruses, trackers.

To gauge the respondents' perception regarding threat susceptibility, a 4-item measure was developed, which was adapted from Tsai et al. (2016) and Liang and Xue (2010). Respondents' coping self-efficacy was measure using a 6-item scale, which was adapted from Anderson and Agarwal (2010) and Tsai et al. (2016). The items were modified to suit the needs of the current study. A 3-item scale measured the respondent's response efficacy, and the items were adapted from Tsai et al. (2016) and Liang and Xue (2010). The dimension of response cost was measured using a 3-item scale adapted from Liang and Xue

(2010). A 7-item scale measured the respondents' prior experience with cyber security issues. This measure was adapted from Tsai et al. (2016). Personal responsibility towards cyber security was measured using a 3-item scale adapted from Anderson and Agarwal (2010). Lastly, cyber security intentions were measured using a 7-item scale adapted from Tsai et al. (2016)." This is an order to check the dimensional validity and "the underlying factor structure, exploratory factor analysis using the principal axis factoring method with oblique rotation was performed. The exploratory factor analysis (EFA) was conducted using the psych package (Revelle, 2017)" in R version 3.4.4.

Table also summarizes the factors extracted. All the factors extracted have loadings greater than 1 Since all the 8 factors extracted from the data have SS loadings greater than 1.0, therefore, all the 8 factors are significant (Nath, 2018). The total variance captured by this 8-factor solution is 58.4%. Table 5.7 summarizes the factor structure and loadings. Since the sample size of the current study is 298, factor loadings greater than 0.40 (Nath, 2018), were considered significant. All the items in the questionnaire scored factor loading above this threshold, therefore, no items were deleted after the EFA.

Table 5.5 Questionnaire Items Used for Constructs

Construct	Questionnaire Item
Protection motivation	I "am likely to follow the organization's Information systems security policy in the future. (Strongly agree<->Strongly disagree) (Ifinedo, 2012) "
Rewards	I "would feel [a] of sense of internal Satisfaction for allowing information security threats to harm my organization. (Strongly agree<->Strongly disagree) (Posey, Roberts, Lowry, Courtney, & Bennett, 2011)
Severity	I "believe the productivity of [the] organization and its employees is threatened by security incidents. (Strongly agree<->Strongly disagree) (Herath & Rao, 2009)
Vulnerability	I "know my organization could be vulnerable to security breaches if I don't adhere to its information security policy. (Strongly agree<->Strongly disagree) (Ifinedo, 2012)

Construct	Questionnaire Item
Response efficacy	Enabling “the security measures on my work computer is an effective way to deter hacker attacks.(Strongly agree<->Strongly disagree) (Ifinedo, 2012)”.
Self-efficacy	For me, “taking information security precautions to protect my organization’s information and information systems is easy. (Strongly agree<->Strongly disagree) (Posey et al., 2011)”
Response cost	There “are too many overhead costs associated with implementing information system security. (Strongly agree<->Strongly disagree) (Ifinedo, 2012)

(Source: Researcher Own)

Table 5.6 Research Methodology Table (RO2)

Philosophical assumption	Protection Motivation Theory
Type research study	Qualitative & Quantitative
Role of researcher	To Analysis the data and develop a framework to address the aviation cyber threat by creating awareness among passengers flying through NCR.
Sampling framework	Age group 20-50(years); three months’ time frame (Dec 2017-Apr 18); convenience sampling
Data collection procedures	From the Data collected earlier through Questionnaire and if found significant; the same can be used for analysis and making a framework.
Tools	Structural Equational Modelling using PLS SEM tool.
Research Design	Descriptive Design

(Source: Researchers Own)

5.4.3 Hypothesis Building. A threat is being defined as the possibility and severity of danger (Safa et al., 2015). Threat severity or perceived severity is determined by perceived vulnerability and severity to risks/ threats (Tsai et al., 2016). In simple terms, perceived severity describes how seriously an individual believes that the threat would be their own life (Wong et la., 2016). Threat susceptibility or perceived vulnerability (PV) determines how Susceptible or vulnerable an individual feel to the communicated threat (Wong et al., 2016).

Studies in the past have reported threat appraisal (severity and susceptibility) to be positively affecting behavioural intentions in case of cyber security related threats (Laing and Xue, 2010; Tsai, 2016; Lee and Larsen, 2009; Siponen et al., 2014). Therefore, it can be hypothesized that:

5.4.4 Research Hypothesis.

H_0 is Null Hypothesis and **H_A** is Alternate Hypothesis

H_0: Perceived Threat severity has no significant relationship with Aviation Cyber Security.

H_A: Perceived Threat severity has significant relationship with Aviation Cyber Security.

H_0: Perceived Threat susceptibility has no significant relationship with Aviation Cyber Security.

H_A: Perceived Threat susceptibility has significant relationship with Aviation Cyber Security.

H_0: Prior experience with online safety hazards has no significant relation with Aviation Cyber Security.

H_A: Prior experience with online safety hazards has significant relation with Aviation Cyber Security.

H_0: Self attributes (personal responsibility) has no relation with Aviation Cyber Security.

H_A: Self attributes (personal responsibility) has significant relation with Aviation Cyber Security.

H_0: Demographics (gender, age, education) of the passengers have no significant effect on the Aviation Cyber Security intentions.

H$_A$: Demographics (gender, age, education) of the passengers have significant effect on the Aviation Cyber Security intentions.

We discussed survey questionnaires, procedures, and participants. We then discuss the analysis of data, the validity, and the reliability of the measures. Researcher used a 5-point Likert scale, ranging from completely non-agreement. PMT calculated all variables of the predictor.

5.5 DATA EXTRACTION METHOD

An information extraction form was used to collect information from research in a reliable way. It forms fields for research, sample frames, sample size, definition, and relationship or effects studied from measurement items. The following are also recovered: treatment, measured PMT variables(s), a short design description, statistical explanation, little group value, and group differences. There are some studies where PMT variables are used but are named and launched differently. For example, the PMT concept 'self-functionality' is sometimes turned on when asked if the task is under the control of the respondent. The purpose of this meta-analysis is to report average values to indicate common trends.” Once factors identified by Literature review are established, using Principal Component Analysis and the scree plot as given under, A total of seven significant factors with Eigen values more than were identified for the study.

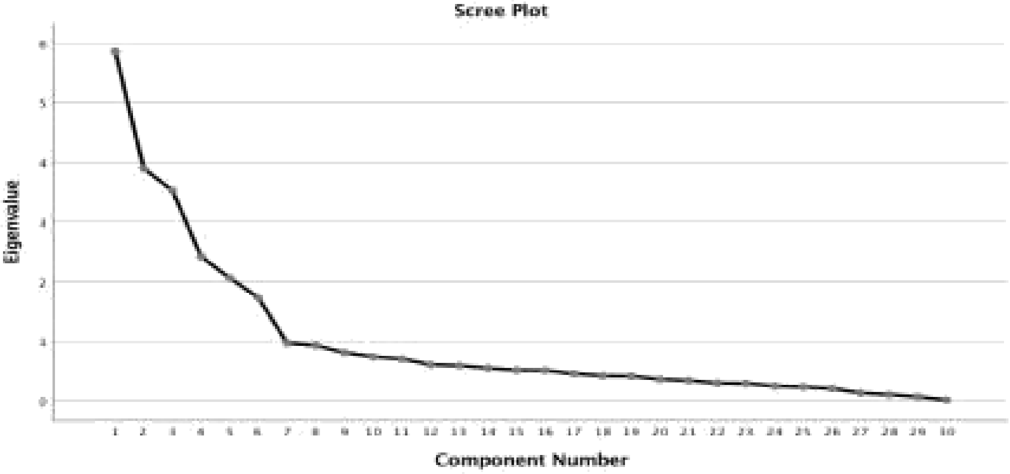


Figure 5.3 Scree Plot

Table 5. 7 Factor Analysis for the Study Variables

Construct	Items	Factor Loading	SS Loading	α	Scale Mean	Scale Std. Deviation
Threat Severity			4.378	0.920	3.355	0.843
	Using free Wi-Fi at airport makes my computer/ mobile/I-pad run more slowly.	0.624				
	There is a possibility That your personal mobile being used by others to cause disruptions.	0.667				
	You feel highly comfortable using free Wi-Fi / Hotspots at Delhi Airport compared to other Airports	0.868				
	Do you feel higher Awareness among Passengers can make one safer in rendering Cyber Security at Airports?	0.724				
	Using free Wi-Fi at Airports can Compromise your personal identity Aadhar/ ID/PAN number or credit card details.	0.963				

Construct	Items	Factor Loading	SS Loading	α	Scale Mean	Scale Std. Deviation
	Delhi Airport takes adequate precautionary measures to safeguard Airport Cyber Security.	0.581				
	I feel Airport’s IT Systems cannot be infected and we are not susceptible to any risks using internet at the Airport (R).	0.650				
Threat Susceptibility			1.905	0.752	2.932	0.733
	My personal devices are highly Safe to operate in an Airport /Aircraft as anywhere else	0.742				
	I recommend use of all mobiles and computers inside the Airport/Aircraft.	0.641				
	Delhi Airport takes Adequate precautionary Measures to Safeguard Airport Cyber Security.	0.581				
	I feel Airport’s IT Systems cannot be infected and we are not Susceptibleto any risks using internet at the Airport (R).	0.650				

Construct	Items	Factor Loading	SS Loading	α	Scale Mean	Scale Std. Deviation
Coping Self-Efficacy			3.716	0.850	4.775	0.316
	I feel comfortable taking measures to secure my devices while using public internet at the airports.	0.819				
	Taking necessary Security measures Is entirely within my control.	0.681				
	I have the expertise to take required security measures.	0.888				
	Taking the required security measures is easy.	0.516				
	I feel very paranoid when thinking about Cyber security (R).	0.643				
	In general, I am safe from any threat when Using public Wi-Fi at airports/ planes.	0.646				
Response Efficacy			1.384	0.700	4.726	0.454
	Security software would be useful for detecting and removing malware.	0.736				

Construct	Items	Factor Loading	SS Loading	α	Scale Mean	Scale Std. Deviation
	Security software will increase my level of protection.	0.655				
	Security software will help in detecting and removing threats faster.	0.577				
Response Cost			3.075	0.949	3.39	1.049
	I am ready to pay extra for safer cyber environment at Airports.	0.890				
	Security programs cause issues with other programs in my phone /computer.	0.967				
	Using security software is too much of a hassle.	0.923				
Prior Experience			4.378	0.907	3.262	0.789
	Slowing down of your IT device	0.774				
	I got a virus from opening a link.	0.650				
	I got a virus attack from visiting a website.	0.924				
	Mysterious programs appeared on my phone/computer	0.798				

Construct	Items	Factor Loading	SS Loading	α	Scale Mean	Scale Std. Deviation
	A pop-up message offering free stuff.	0.628				
	I had important information stolen.	0.713				
	I “have been a victim of cyber-crime and I have lost money.”	0.878				
Personal Responsibility			1.928	0.753	4.13	1.248
	If “I adopt security measures, I can make a difference in helping secure the cyber space.”	0.799				
	The “efforts of one Person are useless in this vast cyber space (R).”	0.473				
	Every “person can make a difference when it comes to cyber security.”	0.901				
Security Intentions			3.716	0.883	3.585	0.849
	I am likely to take security measures to protect my mobile device while using at airport.	0.878				

Construct	Items	Factor Loading	SS Loading	α	Scale Mean	Scale Std. Deviation
	I will upgrade my Security measures to protect myself better while using free Wi-Fi at Airport.	0.721				
	I will not save my Passwords	0.842				
	while Using mobile /computer at Airports.					
	I will use passwords that are harder to guess.	0.638				
	I will change my browser security settings to a higher level, and I am vigilant using my device at Airport.	0.671				
	I will learn how to be more secure online at Airports.	0.650				
	I run protective software regul-arly to remove spyware from my computer / mobile	0.621				

(Source: Researcher Own)

The analysis of variance factors above significant result as given in Table 5.8

Table 5.8: Analysis of Variance Factors

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig
1	Regression	5366.626	7	766.661	43.414	.000[b]
	Residual	5103.543	289	17.659		
	Total	10470.168	296			

a. Dependent Variable: Security intentions
b. Predictors: Threat severity, Threat susceptibility, Coping Self Efficacy, Response Efficacy, Response Cost, Prior experience, & Personal responsibility.

The value of F test of ANOVA is 43.414 with p value = 0.000 which was less than 0.05 level of significance which showed that the **model was statistically fit.** The overall model summary is given in table 5.9

Table 5.9 Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.716[a]	**.513**	.501	4.202

The value of correlation coefficient (R) between security intentions and all independent variables is 0.716 which shows there is a relation between them. The value of regression coefficient (R square) was 0.513 which showed that there is 51.3% of variation on dependent variable security intentions described by independent variables such as Perceived threat severity, Perceived threat susceptibility, prior experience, Coping efficacy, response efficacy, Prior experience and personal responsibility. The internal reliability was checked with values of Cronbach alpha as tabulated in Table 5.10

Table 5.10 Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha based on standardised items	No of items
.833	.813	37

The overall value of **Cronbach alpha for the entire set of items is higher than 0.75 and hence statistically fit**. In order to test the hypothesis for the current study, **a multiple *regression* analysis** was performed. The multiple linear regression model gives the significant variables contributing as a predictor as given in table 5.11

Table 5.11 Regression Model

Coefficients ^{a}					
Model	**Unstandardized Coefficients**		**Standardized Coefficients**	**t**	**Sig.**
	B	**Std. Error**	**Beta**		
(Constant)	6.460	5.046		1.280	.202
Threat severity	3.321	0.771	.3500	4.159	**.000***
Threat susceptibility	-.049	.085	-.024	-.584	.560
Coping Self Efficacy	-.832	.080	-.773	10.354	**.000***
Response Efficacy	.332	.130	.108	2.547	**.011***
Response Cost	-.055	.129	-.018	-.429	.669
Prior experience	.005	.181	.001	.028	.978
Personal responsibility	3.364	.206	.203	16.300	**.000***
a. Dependent Variable: Security intentions					

The above table brings out four independent variables as significant; these are Threat severity, coping self-efficacy, Response efficacy and personal responsibility. The mathematical model can be represented by:

Y (SI) = 6.460+3.321(Ts)-0.49(Tsp)-0.832(Cse)+0.332(Re)-0.055(Rc)+0.005(Ep) +3.364(Pr)

From the reliability statistics, table 5.12 we find Cronbach alpha > 0.75 and hence statistically fit and the ANOVA from table 5.13 below is showing all 7 items differs significantly. From above we reject Null hypothesis.

Further for reliability, component loading of individual items, except an item of reaction cost, which is later deleted, is loaded on to the associated material (® .70), providing evidence for the unit level of the item. However, we had to remove two self-functionality and attitude items because these items were loaded high on security sentiments. Therefore, both construction structural models are represented by a single item, a potential threat to reliability.

Table 5.12 Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on standardized Items	No of Items
.920	.919	7

Table 5.13 ANOVA with Friedman's Test

		Sum of Squares	df	Mean Square	Friedman's Chi-Square	Sig
Between People		1473.744	296	4.979		
Within People	Between Items	30.504[a]	6	5.084	73.799	**.000**
	Residual	706.067	1776	.398		
	Total	736.571	1782	.413		
Total		2210.316	2078	1.064		
Grand Mean =3.3555 a. Kendall's coefficient of concordance W = .014.						

Construction reliability is evaluated using co-efficient use of collective reliability; For all items, the cut-off point of .70 has been exceeded. The aggregate validity is evaluated by using the average variation (AVE) extracted by a construction from its index, which crosses the cut-off point of 0.70, except for control 0.64. Each structure from its index analyzes the square root of the avenue and evaluates the legality of the crime, which should be larger than its relationship with the rest of the building (Fornel-Larker-Standard, 1981). All standards have met this condition. Additional SPS analysis did not show any multi-linear problems.

5.6 STATISTICAL TECHNIQUES FOR DATA ANALYSIS

In this way researcher further analyze the data for validation and reliability through partial-minimum square path-modeling (PLS) from Smart PLS 2.0 (Ringle etc. 2005). PLS can describe the relationship between the measured variable and the Latin variable (Chul etc. 2014) as a class of multifaceted strategies. We will take after the following way of data analysis strategies, which is used in aviation sector as well as other sector as required for the further study. The next chapter have been described the more detail applicability of this chapter.

CHAPTER 6

DATA ANALYSIS AND INTERPRETATION

The IBM 24.0 SPSS is used for data analysis to apply a strategy such as reliability testing, multiple regressions, and dimension reduction factor analysis to a structured equation model.

6.1 DEMOGRAPHIC INFORMATION

6.1.1 Gender Distribution of Respondents

The table 6.1.1 doles out the gender distribution of the respondents as out of 297 respondents, 79.8% of respondent were male and 20.2% of respondent were female.

Table 6.1.1: Gender of Respondents

Gender	Frequency	Percent
Female	60	20.2
Male	237	79.8
Total	297	100.0

6.1.2 Age Distribution of Respondents

The age supply of defendant is given in table 6.1.2, out of 297 respondents, 31.3% of the respondents belonged to the age group of 18 to 30 years, 21.2% of respondents were from 31 to 40 years, 38.4% of defendants were from the age group of 41 to 50 years and 9.1% of respondents were of 51 years or more.

Table 6.1.2: Age of Respondents

Age	Frequency	Percent
18- 30 years	93	31.3
31– 40 years	63	21.2
41– 50 years	114	38.4
51 years or more	27	9.1

6.1.3 Education Level of Respondents

It can be seen in the table 6.1.3 that 16.2% of respondent were graduates and 60.6% of respondent were post graduates, 23.2% of respondents were post graduate and above.

Table 6.1.3: Education Level of Respondents

Education level	Frequency	Percent
Graduate	48	16.2
Post graduate	180	60.6
Post graduate + above	69	23.2
Total	100	100

6.1.4 Frequency of Respondents Using Aircrafts to Travel

The table 6.1.4 alludes to the frequency of the respondents of using flights to travel. It was observed that 8.1% of respondent have used the fights to travel for 11 or more times, followed by the ones who used it for 6 to 10 times (18.2%), 2 to 5 times (45.5%) and only once a year (28.3%).

Table 6.1.4: Frequency of Flying of Respondents

Frequency of aircrafts use	Frequency	Percent
11 or more times	24	8.1
6 to 10 times	54	18.2
2 to 5 times	84	45.5
Once a year	135	28.3

6.2 PARAMETERS OF PROTECTION MOTIVATION THEORY (PMT)

6.2.1 Constructs of Threat Severity

Respondents were asked to rate their threat that can be caused by malware while using their mobiles. "It can be seen in the table 6.2.1 that 5.7% of the respondents highly disagree with vulnerability of airports regarding cyber threats whereas 25.9% respondents agree and 37.7% highly agree with the same. 45.5% of respondents highly agree and 27.3% agree that their computer/mobile/i-pad run slowly when they were connected with the Wi-Fi available at the airport whereas 2.4% respondents highly disagree and 6.7% of the respondents disagree with it and 18.2% of the respondents were neutral about it. It was also found that 34% of the respondents highly agree and 27.3% people agree that they were highly comfortable using free Wi-Fi at Delhi Airport compared to other airport and 6.4% highly disagree with the same." 22.2% of the total respondents feel no difference in using the Wi-Fi at the Delhi airport comparing to the other airports. Higher awareness among passengers can make one make one safer in rendering cyber security at airports has been highly accepted by 44.4% of the respondents and 26.35 of Respondents agree, 3.7% of respondents agree highly disagree that the awareness cannot assure safety and 13.8% of the respondents believe that it won't make any difference. It was observed that 36.4% respondents highly agree that using Wi-Fi at airports could compromise their personal identity Aasdhar/ID/PAN number or credit card details and 6.1% of the respondents highly disagree and 20.2% of them didn't feel any difference in using their identity and credit card details. The 38.7% of the respondents highly agree and 31.6% that the information shared at public places such as airport/railway station can be used to commit crimes and 3.4% highly disagree and 9.4% with the same.

Table 6.2.1 Frequency of Constructs of Threat Severity

Constructs of Threat Severity		
	Frequency	**Percent**
1. Do you feel airports too are vulnerable for cyber threats?		
Neutral	58	19.5
Highly disagree	17	5.7
Highly agree	112	37.7
Disagree	33	11.1
Agree	77	25.9
2. Using free Wi-Fi at airport makes my computer/mobile/I-pad run more slowly.		
Highly disagree	7	2.4
Disagree	20	6.7
Neutral	54	18.2
Agree	81	27.3
Highly agree	135	45.5
3. There is A Possibility That Your Personal Mobile Being used by Others To Cause Disruptions.		
Highly disagree	5	1.7
Disagree	30	10.1
Neutral	51	17.2
Agree	73	24.6
Highly agree	138	46.5
4. You feel highly comfortable using free Wi-Fi / Hotspots at Delhi Airport compared to other Airports.		
Highly disagree	19	6.4
Disagree	30	10.1
Neutral	66	22.2
Agree	81	27.3
Highly agree	101	34.0
5. Do you feel higher awareness among passengers can make one safer in rendering Cyber Security at Airports?		
Highly disagree	11	3.7
Disagree	52	17.5
Neutral	41	13.8

	Frequency	Percent
Agree	61	20.5
Highly agree	132	44.4
6. Using free Wi-Fi at Airports can compromise your personal identity Aadhar/ ID/ PAN number or credit card details.		
Highly disagree	18	6.1
Disagree	33	11.1
Neutral	60	20.2
Agree	78	26.3
Highly agree	108	36.4
7. The information shared at public places such as Airport/Railway Station can be used to commit crimes.		
Highly disagree	10	3.4
Disagree	28	9.4
Neutral	50	16.8
Agree	94	31.6
Highly agree	115	38.4

6.2.2 Constructs of Threat Susceptibility

Respondents were asked to rate their safety that they feel in operating their personal IT devices at the airport/aircraft despite being its vulnerability to cyber domain. The table 6.2.2 insinuates that 28.3% of the respondents highly agree that their devices were highly safe to operate in an airport and only 4% highly disagree with it whereas 26.3% of the total respondents felt no difference of safety in using their devices anywhere. Only 8.15% of the total respondents highly disagree to recommend the use of mobiles and computers inside the airport/aircraft but 34.7% respondent highly agree to recommend. “It was found that 44.1% of the respondents highly agree and 32.7% of respondents agree that Delhi airport took adequate precautionary measures to safeguard airport cyber security but 9.1% of the respondents disagree with that. The 46.1% of the respondents highly agree and23.9% of the respondents agree that airport’s IT systems cannot be hacked and they were not susceptible to any risk using internet at the airport, whereas 4.7% of the respondents highly disagree with the same."

Table 6.2.2: Frequency of Constructs of Threat Susceptibility

Constructs of Threat susceptibility		
	Frequency	**Percent**
1. My personal devices are highly safe to operate in an Airport/Aircraft as anywhere else		
Highly Disagree	12	4.0
Disagree	15	5.1
Neutral	78	26.3
Agree	84	28.3
Highly agree	108	36.4
2. I recommend use of all mobiles and computers inside the Airport/Aircraft		
Highly disagree.	24	8.1
Disagree	6	2.0
Neutral	78	26.3
Agree	86	29.0
Highly agree	103	34.7
3. Delhi Airport takes adequate precautionary measures to safeguard Airport Cyber Security		
Disagree	29	9.4
Neutral	41	13.8
Agree	97	32.7
Highly agree	131	44.1
4. I feel Airport's IT systems cannot be hacked and we are not susceptible to any risks using internet at the Airport		
Highly disagree	14	4.7
Disagree	29	9.8
Neutral	46	15.5
Agree	71	23.9
Highly agree	137	46.1

6.2.3 Constructs of Coping Self-Efficacy

Respondents were asked to rate the adequate measures taken by the airports to secure themselves from cyber nuisances. And the table 6.2.3 gives the information that, 77.4% of the respondents highly agree that they were comfortable taking measures to secure their devices while using public internet at airports and no one disagree for the same. And 78.1% of the respondents said that the security measures that can be taken were entirely in their control. It was observed that 76.1% of the respondents have the expertise to take required security measures by themselves. "And 77.4% of the respondents highly agree and 22.6% agree that taking the required security measures was easy at airport as elsewhere. It can be seen that 78.8% of the total respondents highly agree that they felt paranoid while thinking about cyber security. It was found that 76.8% of the respondents highly agree that they were safe from any threat while using public Wi-Fi at airports/aircrafts."

Table 6.2.3: Frequency of Constructs of Coping Self-Efficacy

Constructs of Coping Self-Efficacy		
	Frequency	**Percent**
1. I feel comfortable taking measures to secure my devices while using public internet at Airports		
Agree	67	22.6
Highly agree	230	77.4
2. "Taking necessary security measures is entirely within my control."		
Agree	65	21.9
Highly agree	232	78.1
3. I have the expertise to take required security measures		
Agree	71	23.9
Highly agree	226	76.1
4. Taking the required security measures is easy at Airports as anywhere else.		
Agree	67	22.6

	Frequency	Percent
Highly agree	230	77.4
5. I feel paranoid when thinking about cyber security.		
Agree	63	21.2
Highly agree	234	78.8
6. In general, I am safe from any threat when using public Wi-Fi at Airports / Aircrafts.		
Agree	69	23.2
Highly agree	228	76.8

6.2.4 Constructs of Response-Efficacy

Respondents were asked to rate the security measures regarding "the nuisances of cyber security in the environment. From the table 6.2.4 given below, it can be seen that 75.1% of the respondents highly agree that security software would be useful for detecting and removing a malware and no one disagrees with it." whereas, 76.1% of the total respondents highly agree that security software would increase their level of protection and 4% of the respondents disagree with it. It was observed that 82.5% of respondents highly agree that security software would help in detecting and removing threats faster and no one disagree for it.

Table 6.2.4: Frequency of Constructs of Response-Efficacy

Constructs of Response Efficacy		
	Frequency	**Percent**
1. Security software would be useful for detecting and removing a malware		
Neutral	18	6.1
Agree	56	18.9
Highly agree	223	75.1
2. Security software will increase my level of protection.		
Highly disagree.	2	0.7
Disagree	12	4.0
Agree	57	19.2
Highly agree	226	76.1

Constructs of Response Efficacy		
	Frequency	**Percent**
3. Security software will help in detecting and removing threats faster.		
Agree	52	17.5
Highly agree	245	82.5

6.2.5 Constructs of Response Cost

Respondents were asked to rate the cost applied for the safety and security for cyber nuisances. “And the numbers of respondents who highly agree to pay extra for safer cyber environment was 31.3% and 9.1% of the respondents highly disagree and 14.5% of the respondents disagree for the same. 29% of the respondents highly agree” and 23.2% agree that security programs interfered with other programs in their phones and 12.5% of respondents disagree with the same, and 21.5% of respondents have no problem using security programs on their phones because it did not interfere with other programs they are using.

Table 6.2.5: Frequency of Constructs of Response Cost

Constructs of Response Cost		
	Frequency	**Percent**
1. I am ready to pay extra for safer cyber environment at Airports.		
Highly disagree.	27	9.1
Disagree	43	14.5
Neutral	51	17.2
Agree	83	27.9
Highly agree	93	31.3
2. Security programs interfere with other programs in my phone.		
Highly disagree	41	13.8
Disagree	37	12.5
Neutral	64	21.5
Agree	69	23.2
Highly agree	86	29.0

Constructs of Response Cost		
	Frequency	**Percent**
3. Using Security software is too much of a hassle.		
Highly disagree.	34	11.4
Disagree	41	13.8
Neutral	49	16.5
Agree	76	25.6
Highly agree	97	32.7

6.2.6 Constructs of Prior Experience with Safety Hazards

Respondents were asked about their prior experiences about "their usage of devices after browsing at airports and 41.1% of the respondents highly agree and 26.6% of the respondents agree that their IT devices slows down after browsing at the airports and 24.2% of the respondents didn't find any difference and 2% of the respondents highly disagree with the same. The 43.4% of the respondents highly agreed and 24.2% of the respondents agree that their devices got a virus attack from opening a link while browsing and only 8.1% of the respondents disagree for that. It was observed that 41.4% of the respondents highly agreed that they got a virus attack from just visiting a web site while browsing and 6.1% of the respondents disagree and only 1% highly disagreed with it. The 44.4% of the respondents highly agree that they got mysterious icons or programs on their phone while browsing at the airport while only 1% highly disagreed and 7.1% disagree with the same. It was found that 46.5% of the respondents highly agree that a pop-up message offering a free computer security scan appeared on their device and only 3% of the respondents highly disagreed that the message didn't appear.

Table 6.2.6: Frequency of Constructs of Prior Experience with Safety Hazards

Constructs of Prior Experience with Safety Hazards		
	Frequency	**Percent**
1. Slowing down of your IT device		
Highly disagree	6	2.0

Constructs of Prior Experience with Safety Hazards		
	Frequency	**Percent**
Disagree	18	6.1
Neutral	72	24.2
Agree	79	26.6
Highly agree	112	41.1
2. I got a virus attack from opening a link.		
Highly disagree	12	4.0
Disagree	24	8.1
Neutral	60	20.2
Agree	72	24.2
Highly agree	129	43.4
3. **Virus attack from just visiting a web site.**		
Highly disagree	3	1.0
Disagree	18	6.1
Neutral	75	25.3
Agree	78	26.3
Highly agree	123	41.4
4. **Mysterious icons or programs appeared on my phone.**		
Highly disagree	3	1.0
Disagree	21	7.1
Neutral	69	23.2
Agree	72	24.2
Highly agree	132	44.4
5. **Pop-up message offering a free computer security scans.**		
Highly disagree	9	3.0
Disagree	21	7.1
Neutral	69	23.2
Agree	72	24.2
Highly agree	132	44.4
6. Had important personal information stolen, such as your Social Security Number or credit card number?		
Highly disagree	15	5.1
Disagree	15	5.1
Neutral	77	25.9
Agree	92	31.0

Highly agree	98	33.0
7. Been the victim of an online scam and lost money.		
Highly disagree	4	1.3
Disagree	23	7.7
Neutral	67	22.6
Agree	79	26.6
Highly agree	124	41.8

6.2.7 Constructs of Personal Responsibility

Respondents were asked whether they were prepared to be more educated and aware about the actions as passengers, to make the airport IT safety systems more secure and "it was observed that 31.6% and 56.2% of the respondents highly agree and agree, respectively, that if they adopt cyber security measures then they will make a difference.

Table 6.2.7: Frequency of Constructs of Personal Responsibility

Constructs of Personal Responsibility		
	Frequency	**Percent**
1. If I adopt cyber security measures, I can make a difference in helping the Airport much safer.		
Highly disagree	5	1.7
Disagree	11	3.7
Neutral	20	6.7
Agree	167	56.2
Highly agree	94	31.6
2**. The efforts of one person are useless in securing the cyber space in Airports.**		
Highly disagree	4	1.3
Disagree	24	8.1
Neutral	21	7.1
Agree	162	54.5

Constructs of Personal Responsibility		
	Frequency	**Percent**
Highly agree	86	29.0
3. Every passenger can make a difference when it comes to cyber security.		
Disagree	3	1.0
Neutral	21	7.1
Agree	173	58.2
Highly agree	100	33.7

6.2.8 Constructs of Security Intentions

Respondents were asked about their future actions regarding “their likelihood of implementing security measures to protect themselves online while travelling at airports. And the table 6.2.8 doles out that, 39.4% of the respondents were highly agree and 32.3% of the respondents were agree and 10.1% of the respondents disagree and 18.2% were neutral for it. The 33.3% of the respondents highly agree and 27.3% of the respondents disagree that they will upgrade their security measures to protect themselves better while using free Wi-Fi at airport and 2% of the respondents highly disagree and 20.2% of the respondents disagree for the same. It was found that 39.1% of the respondents highly agree and 30.6% of the respondents agree that they won’t save their passwords while using mobile/computer at airports and only 0.7% of the respondents highly disagree for it. The 33.7% of the respondents highly agree and 41.8% of the respondents agree that they will use passwords that will be difficult to guess and only 2% of the respondents disagree for the same. It was observed that 36.4% of the respondents highly agree to change their browser security settings to a higher level, they are vigilant using their device at airport and 5.1% of the respondents highly disagree and 13.1% of the respondents disagree to it. The 35.4% of the respondents highly agree and 25.3% of the respondents agree that they will learn how to be more secure online at airports; On the other hand, 8.1% of respondents disagree also on the table, 28.3 percent of respondents agreed that they regularly run defensive software to remove spyware from their computers/mobiles at airports, while 9.1 percent of respondents disagree.

Table 6.2.8: Frequency of Constructs of Security Intention.

Constructs of Security Intentions		
	Frequency	**Percent**
1. I am likely to take security measures to protect my mobile device while using at airport.		
Disagree	30	10.1
Neutral	54	18.2
Agree	96	32.3
Highly agree	117	39.4
2. I will upgrade my security measures to protect myself better while using free Wi-Fi at Airport		
Highly disagree	6	2.0
Disagree	60	20.2
Neutral	51	17.2
Agree	81	27.3
3. I will not save my passwords while using mobile/computer at Airports.		
Highly disagree	2	0.7
Disagree	36	12.1
Neutral	52	17.5
Agree	91	30.6
Highly agree	116	39.1
4. I will use passwords that are harder to guess.		
Highly disagree	6	2.0
Disagree	26	8.8
Neutral	41	13.8
Agree	124	41.8
Highly agree	100	33.7
5. I will change my browser security settings to a higher level, and I am vigilant using my device at Airport.		
Highly disagree	15	5.1

Constructs of Security Intentions		
	Frequency	**Percent**
Disagree	39	13.1
Neutral	57	19.2
Agree	78	26.3
Highly agree	108	36.4
6. I will learn how to be more secure online at Airport.		
Highly disagree	24	8.1
Disagree	42	14.1
Neutral	51	17.2
Agree	75	25.3
Highly agree	105	35.4
7. I run protective software regularly to remove spyware from my computer/ mobile at Airport.		
Highly disagree	27	9.1
Disagree	45	15.2
Neutral	69	23.2
Agree	72	24.2
Highly agree	84	28.3

6.3 RELIABILITY MEASURES OF PARAMETERS OF PROTECTION MOTIVATION THEORY (PMT)

6.3.1 Threat Severity

The table 6.3.1.1 given below gives “the value for Cronbach’s Alpha for threat severity as 0.920, showing high internal consistency of the measuring instrument for the constructed factor. And the table 5.3.1.2 doles out the item statistics of the construct, threat severity.”

Table 6.3.1.1: Reliability of Threat Severity

Reliability Statistics	
Cronbach's Alpha	**No. of Items**
0.920	7

Table 6.3.1.2: Item Statistics of Threat Severity of Protection Motivation Theory

Items of Threat severity	Mean	Std. Deviation
Do you feel Airports too are vulnerable for cyber threats?	3.29	1.080
Using free Wi-Fi at airport makes my computer/mobile/I-pad run more slowly	3.36	0.934
There is a possibility that your personal mobile being used by others to cause disruptions	3.46	0.948
You feel highly comfortable using free Wi-Fi / Hotspots at Delhi Airport compared to other Airports	3.19	1.091
Higher awareness among passengers can make one safer in rendering Cyber Security at Airports	3.58	1.047
Using free Wi-Fi at Airports can compromise your personal identity Aadhar/ ID/ PAN number or credit card details	3.26	1.090
The information shared at public places such as Airport/Railway Station can be used to commit crimes	3.34	0.977

6.3.2 Threat Susceptibility

The table 6.3.2.1 given below gives the value for Cronbach alpha for threat susceptibility as 0.752, “showing high internal consistency of the measuring instrument for the constructed factor. And the table 6.3.2.2 doles out the item statistics of the construct, threat susceptibility.”

Table 6.3.2.1: Reliability of Threat Susceptibility

Reliability Statistics	
Cronbach's Alpha	No. of Items
0.752	4

Table 6.3.2.2: Item Statistics of Threat Susceptibility of Protection Motivation Theory

Items of Threat susceptibility	Mean	Std. Deviation
My personal devices are highly safe to operate in an Airport/Aircraft as anywhere else	2.94	1.005
I recommend use of all mobiles and computers inside the Airport/Aircraft	2.82	0.838
Delhi Airport takes adequate precautionary measures to safeguard Airport Cyber Security	3.38	0.838
I feel Airport's IT systems cannot be hacked and we are not susceptible to any risks using internet at the Airport (R).	2.59	1.016

6.3.3 Coping Self-Efficacy

The table 6.3.3.1 given below gives the value for Cronbach alpha for coping self-efficacy as 0.85, **"**showing high internal consistency of the measuring instrument for the constructed factor. And the table 6.3.3.2 doles out the item statistics of the construct, coping self-efficacy."

Table 6.3.3.1: Reliability of Coping Self-Efficacy

Reliability Statistics	
Cronbach's Alpha	No. of Items
0.850	6

Table 6.3.3.2: Item Statistics of Coping Self-Efficacy of Protection Motivation Theory

Items of Threat susceptibility	Mean	Std. Deviation
I feel comfortable taking steps to protect my device while using the public internet at the airport	4.77	0.419

Items of Threat susceptibility	Mean	Std. Deviation
Taking necessary security measures is entirely within my control	4.78	0.414
I have the expertise to take required security measures	4.76	0.427
Taking the required security measures is easy at Airports as anywhere else	4.77	0.419
I feel paranoid when thinking about cyber security	4.79	0.410
In general, I am safe from any threat when using public Wi-Fi at Airports/Aircrafts.	4.77	0.423

6.3.4 Response Efficacy

The table 6.3.4.1 given below gives the value for Cronbach alpha for response efficacy as 0.669, showing high internal consistency of the measuring instrument for the constructed factor. And the table 6.3.4.2 doles out the item statistics of the construct, response efficacy.

Table 6.3.4.1: Reliability of Response Efficacy of Protection Motivation Theory

RELIABILITY STATISTICS	
Cronbach's Alpha	**No. of Items**
0.669	3

Table 6.3.4.2: Reliability of Response Efficacy of Protection Motivation Theory

Items of Threat susceptibility	Mean	Std. Deviation
Security software will be useful for detecting and removing a malware	4.69	0.580
Security software will increase my level of protection	4.66	0.741
Security software will help in detecting and removing threats faster	4.82	0.381

6.3.5 Response Cost

The table 6.3.5.1 given below gives the value for Cronbach alpha for response cost as 0.533, showing low internal consistency (less than 0.6) of the measuring instrument for the constructed factor and the table 6.3.5.2 doles out the item statistics of the construct, response cost.

Table 6.3.5.1: Reliability of Response cost of protection Motivation theory

Reliability Statistics	
Cronbach's Alpha	**No. of Items**
0.533	3

Table 6.3.5.2: Item Statistics of Response Cost of Protection Motivation Theory

Items of Threat susceptibility	Mean	Std. Deviation
I am ready to pay extra for safer cyber environment at Airports	3.26	0.940
Security programs interfere with other programs in my phone.	4.01	0.991
Using Security software is too much of a hassle.	2.98	1.023

6.3.6 Improved Reliability of Response Cost

Now, the objective is to improve the reliability of response cost, because it is having the reliability less than 0.6, the last column (Cronbach's Alpha if Item deleted) in the table 6.3.6.1 below. This column explains the reliability of the response cost, if we delete the corresponding item from the survey. It explains that reliability of response cost will be 0.089 if we delete the first item of ready to pay extra for safer cyber environment, if we delete the second item, then reliability of response cost will be 0.818. It means that deleting the second item will increase our reliability of the instrument for response cost.

Table 6.3.6.1: Item Total Statistics of Response Cost of Protection Motivation Theory

Item Statistics	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach Alpha if Item Deleted
I am ready to pay extra for safer cyber environment at Airports	6.99	2.125	0.552	0.089
Security programs Interfere with other programs in my phone	6.24	3.265	0.076	0.818
Using Security software is too much of a hassle	7.27	2.044	0.489	0.173

After removing the second element of security programs that conflict with other programs on the computer, the value of Cronbach's alpha response cost is increased to 0.818, indicating the high reliability of the measuring instrument. This also shows a high degree of internal continuity with respect to the Sample Objects. And Table 6.3.5.4 displays the item Construction Figures, Response Costs.

Table 6.3.6.2: Reliability of Response Cost of Protection Motivation Theory

Reliability Statistics	
Cronbach's Alpha	**No. of Items**
0.818	2

Table 6.3.6.3: Item Statistics of Response Cost of Protection Motivation Theory

Items of Threat susceptibility	Mean	Std. Deviation
I am ready to pay extra for safer cyber environment at Airports	3.26	0.940
Using Security software is too much of a hassle	2.98	1.023

6.3.7 Prior Experience with Safety Hazards

The table 6.3.7.1 given below illustrates **“**the value for cronbach’s alpha for the prior experience as 0.907, showing high internal consistency of the measuring instrument for the constructed factor. And the table 6.3.7.2 shows the item statistics of the construct, prior experience.”

Table 6.3.7.1: Reliability of Prior Experience with Safety Hazards of Protection Motivation Theory

Reliability Statistics	
Cronbach's Alpha	**No. of Items**
0.907	7

Table 6.3.7.2: Item Statistics of Prior Experience with Safety Hazards of Protection Motivation Theory

Items of Threat susceptibility	Mean	Std. Deviation
Slowing down of your IT device	3.25	0.958
“I got a virus attack from opening a link. “	3.27	1.044
“Virus attack from just visiting a web site. “	3.26	0.940
“Mysterious icons or programs appeared on my phone	3.33	0.944
“A pop-up message offering a free computer security scan”	3.42	1.028
“Had important personal information stolen, such as your number Social Security Number or credit card	2.98	1.023
“Been the victim of an online scam and lost money.”	3.32	0.953

6.3.8 Personal Responsibility

The table 6.3.7.1 given below illustrates the value for Cronbach’s alpha for the personal responsibility as 0.753, showing high internal consistency of the measuring instrument for the constructed factor.

Table 6.3.8.1: Reliability of Personal Responsibility of Protection Motivation Theory

Reliability Statistics	
Cronbach's Alpha	**No. of Items**
0.753	3

Table 6.3.8.2: Item Statistics of Personal Responsibility of Protection Motivation Theory

Items of Threat susceptibility	Mean	Std. Deviation
If I adopt cyber security measures, I can make a difference in helping the Airport much safer.	4.12	0.819
The efforts of one person are useless in securing the cyber space in Airports.	0.42	0.898
Every passenger can make a difference when it comes to cyber security.	4.25	0.623

6.3.9. Security Intentions

The table 6.3.8.1 given below illustrates **“**the value for Cronbach’s Alpha for the security intentions as 0.883, showing high internal consistency of the measuring instrument for the constructed factor.

Table 6.3.9.1: Reliability of Security Intentions of Protection Motivation Theory

Reliability Statistics	
Cronbach's Alpha	**No. of Items**
0.883	7

Table 6.3.9.2: Item Statistics of Security Intention of Protection Motivation Theory

Items of Threat susceptibility	Mean	Std. Deviation
I “am likely to take security measures to protect my mobile device while using at airport”	4.01	0.991
I “will upgrade my security measures to protect myself better while using free Wi-Fi at Airport.	3.70	1.187
I “will not save my passwords while using mobile/computer at Airports. “	3.95	1.005
I “will use passwords that are harder to guess”	3.96	1.004
I “will change my browser security settings to a higher level, and I am vigilant using my device at Airport. “	3.09	1.085
I will learn how to be more secure online at Airport	3.22	1.204
I run protective software regularly to remove spyware from my computer/ mobile at Airport	2.16	1.214

6.3.10 Discriminant Validity

Discriminant Validity of “the above stated factors are given in the table below. The diagonal items in the table represented the square root of AVE’s, which was a measure of variance between the construct and its indicators, and the off-diagonal items represented the correlation between constructs. It was observed from the table that the square root of AVE was higher than the correlation, which it should be, between the constructs indicated that all the constructs exhibit discriminant validity.”

Table 6.3.10.1: Discriminant Validity

Factors Constructed For the model	CE	PR	PE	RE	SI	TSe	TSu
Coping self efficacy (CE)	**0.863**						
Personal Responsibility (PR)	-0.042	**-0.846**					
Prior Experience (PE)	-0.053	-0.085	**0.753**				
Response Efficacy (RE)	-0.051	0.219	0.114	**0.835**			
Security Intentions (SI)	-0.014	0.410	0.214	0.214	**0.257**		
Threat Severity (TSe)	0.046	0.073	0.236	0.133	0.329	**0.742**	
Threat Susceptibility (TSu)	0.064	0.439	0.048	0.020	0.311	0.236	**0.817**

6.4 FACTOR ANALYSIS WITH PRINCIPAL COMPONENT ANALYSIS

6.4.1 Security Intentions

Table 6.4.1.1 Table shows that the KMO measure was 0.693 "it suggests passing by variable." Second, The test of Bartlet's health was a p-value of <0.001 which means The relationship of variable measurements was not the Matrix Identity Matrix. Both these tests together provide minimum standards that should have been passed before a factor analysis."

Table 6.4.1.1: KMO and Bartlett's Test for Security Intentions

Kaiser-Meyer- Olkin Measure of Sampling Adequacy		.693
Bartlett's Test of Sphericity	Approx. Chi-Square	1034.997
	df	21
	Sig.	<0.001

The table 6.4.1.2 alludes to “the extracted communalities that states that the factor security intension could explain higher amount of variation with the variable security_intention1 (0.869), security_intention3 (0.828) and lower of security_intention5 (0.242).”

Table 6.4.1.2: Communalities for Security Intensions

Communalities	Initial	Extraction
security_intension1	1.000	.869
security_intension2	1.000	.624
security_intension3	1.000	.828
security_intension4	1.000	.561
security_intension5	1.000	.242
security_intension6	1.000	.664

Table 6.4.1.3: Total Variance Explained of the Factors in Security Intentions

Initial Eigenvalue				Extraction Sum of Squared Loading			Rotation Sum of Squared Loading		
Component	Total	%o f Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulativ e %
1	3.021	43.160	43.160	3.021	43.160	43.160	2.971	42.449	42.449
2	1.519	21.706	64.866	1.519	21.706	64.866	1.569	22.417	64.866
3	.917	13.095	77.961						
4	.600	8.575	86.536						
5	.472	6.744	93.280						
6	.411	5.870	99.149						
7	.060	.851	100.000						

The scree plot in Fig. 6.4.1.1 shows the first two components account for the most variance that can be seen as the big drops in the graphs and the other components that account for very low variation gives the small drops after the second component and have low eigen values.

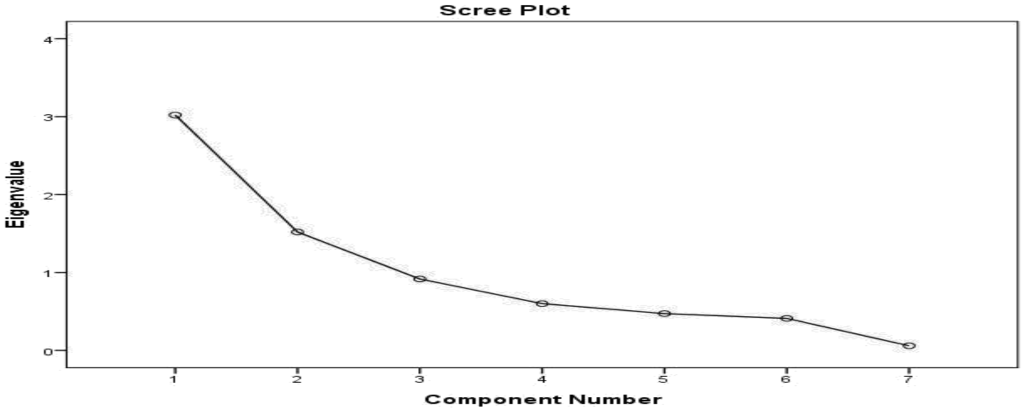


Figure 6.4.1.1: Scree Plot for the Factors in Security Intensions

The table given below shows how the variables are rotated under the factors to explain the maximum amount of variation based on their correlation with them and we can see that variables from security_intension1to security_intension4 are highly correlated to the component 1 and variables from security_intension5 to security_intension7 are highly correlated to component 2.

Table 6.4.1.4: Rotated Component Matrix for the Factors in Security Intensions

Variables for security intension	**Component**	
	1	**2**
security_intension1	0.931	0.031
security_intension2	0.790	-0.004
security_intension3	0.909	-0.053
security_intension4	0.741	-0.112
security_intension5	-0.317	0.376
security_intension6	0.061	0.813
security_intension7	-0.041	0.867

6.4.2 Threat Severity

In the table 6.4.2.1 given below, "The KMO measure was 0.836 which suggests passing through the variable. Second, the test of Bartlet's Sphericity was the p-value of <0.001 which suggests that the relationship of the threat intensity measuring variable is not the Matrix identity matrix.

Table 6.4.2.1: KMO and Bartlett Test for Threat Severity

Kaiser-Meyer-Olk in Measure of Sampling Adequacy		.836
Bartlett's Test of Sphericity	Approx. Chi-Square	1831.605
	df	21
	Sig.	<0.001

The table 6.4.2.2 given below shows Unused communality which says that factor threat threat_severity1 intensity variables (0.941) threat_severity6 s (0.931) and threat_severity4 s (0.876) can explain high volumes. Expelled communality factor threat not too low for Security intention.

Table 6.4.2.2: Communalities for Threat Severity

Communalities	**Initial**	**Extraction**
threat_severity1	1.000	.941
threat_severity2	1.000	.704
threat_severity3	1.000	.682
threat_severity4	1.000	.876
threat_severity5	1.000	.646
threat_severity6	1.000	.931

Table 6.4.2.3 below indicates the total difference is explained by the total component, which is 7 sizes, and their two own values exceed the 1 square load extract total, the first of which explains 61.086 percent and the second explains the element. The first factor explains 46,383 per cent of the variance and the second factor explains 30,268 per cent of the variance after varimax.

Table 6.4.2.3: Total Variance Explained of the Factors in Threat Severity

Component	Initial Eigenvalues			Extraction Sum of Squared Loading			Rotation Sum of Squared Loading		
	Total	% of Variance	Cumulative %	Total	%of Variance	Cumulative %	Total	%of Variance	Cumulative %
1	4.276	61.086	61.086	4.276	61.086	61.086	3.247	46.383	46.383
2	1.090	15.565	76.651	1.090	15.565	76.651	2.119	30.268	76.651
3	.588	8.398	85.049						
4	.457	6.527	91.576						
5	.405	5.780	97.356						
6	.162	2.309	99.665						
7	.023	.335	100.000						

The scree plot in fig 6.4.2.1 shows that the first component explains the most variation that gives the biggest drop from it to the second component which has the eigen value more than 1. The second element is given flat graphs after the 1 eigen is above the standard and is unable to explain much of the variation.

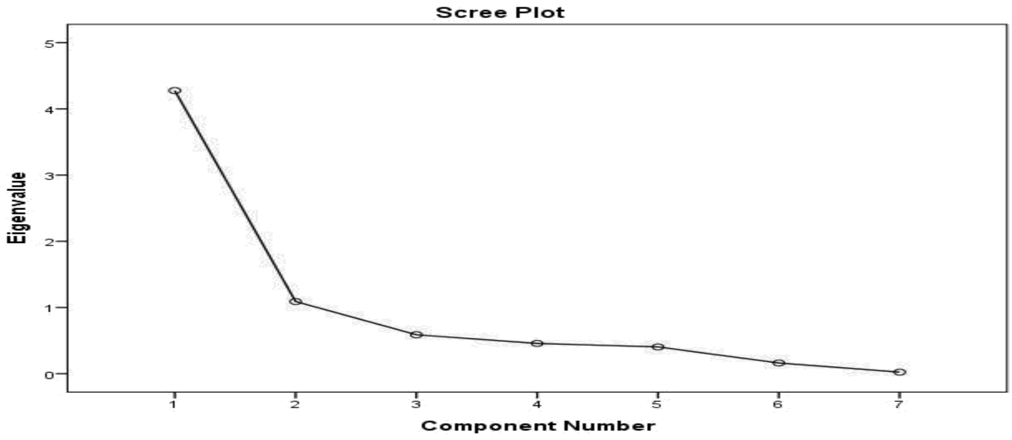


Figure 6.4.2.1: Scree Plot for the Factors in Threat Severity

The table given below shows how the variables are rotated under the factors to explain the maximum amount of variation based on their correlation with them and we can see that variables threat_severity1, threat_severity4, threat_severity5 and threat_severity6, element 1 and was highly related to the variable threat_severity2, threat_severity3 and threat_severity8 are highly correlated to component 2.

Table 6.4.2.4: Rotated Component Matrix for the Factors in Threat Severity

Variables for threat severity	**Component**	
	1	**2**
threat_severity1	0.939	0.244
threat_severity2	0.213	0.811
threat_severity3	0.250	0.787
threat_severity4	0.910	0.218
threat_severity5	0.722	0.353
threat_severity6	0.922	0.286
threat_severity7	0.240	0.726

6.4.3 Threat Susceptibility

Table 6.4.3.1 describes "The KMO measure 0.567 as it suggests to pass by variable and the p-value of the sphericity of the bartlett which means the threat-measuring variable was not the relation matrix of these two tests were given the minimum standard which should have been passed before conducting the factor analysis."

Table 6.4.3.1: KMO and Bartlett Test for Threat Susceptibility

Kaiser-Meyer-Olkin Measure of Sampling Adequacy		.567
Bartlett's Test of Sphericity	Approx. Chi-Square	86.757
	df	6
	Sig.	<0.001

The table 6.4.3.2 given below gives "Passive communality noted that factor sensitivity variables could explain higher variables from decrease_sas3 (0.868) to threat_sus 1 (0.0.665), threat_sus 2 (0.646) and threat_sus 4 (0.456). No reason for passive communality is too small for threat susceptibility.

Table 6.4.3.2: Communalities for Threat Susceptibility

Communalities	Initial	Extraction
threat_sus1	1.000	.665
threat_sus2	1.000	.646
threat_sus3	1.000	.868
threat_sus4	1.000	.456

The percentage explained variant and the second element explained 25.959 percent variant. The first factor explained 39.77 percent of the variants and the second explained 26.116 percent of the variants after the Varimax rotation.

Table 6.4.3.3: Total Variance Explained of the Factors in Threat Susceptibility

Component	Initial Eigenvalues			Extraction Sum of Squared Loading			Rotation Sum of Squared Loading		
	Total	% of Variance	Cumulative %	Total	%of Variance	Cumulative %	Total	%of Variance	Cumulative %
1	1.597	39.927	39.927	1.597	39.927	39.927	1.591	39.770	39.770
2	1.038	25.959	65.886	1.038	25.959	65.886	1.045	26.116	65.886
3	.811	20.284	86.170						
4	.553	13.830	100.000						

The scree plot is shown in fig. 6.4.3.1 as the first and second ingredients had more than 1 of their eigen value and the variation gave large drops and the third and subsequent ingredients had less than 1 of their eigen value.

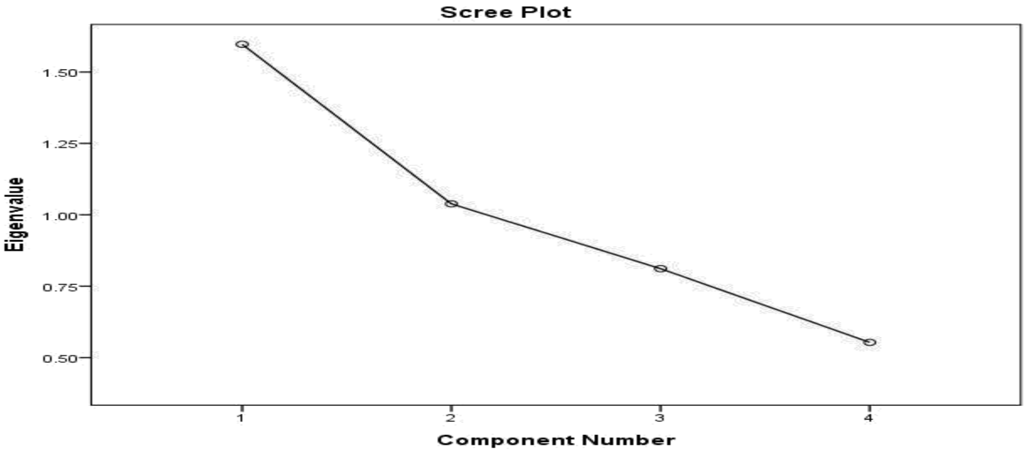


Figure 6.4.3.1: Scree Plot for The Factors in Threat Susceptibility

The table 6.4.3.4 given below shows how the variables are rotated under the factors to explain the maximum amount of variation based on their correlation with them and we can see that variables threat_sus1, threat_sus2 are Element 1 and variable threat_sus3 and highly related elements threat_sus4.

Table 6.4.3.4: Rotated Component Matrix for the factors in threat severity

Variable for threat susceptibility	**Component**	
	1	**2**
threat_sus1	0.815	
threat_sus2	0.789	
threat_sus3	0.064	0.929
threat_sus4	0.547	0.395

6.4.4 Coping Self Efficacy

Table 6.4.4.1 below explains the percentage variant and explained 57.797 percent variant after the Varimax rotation.

Table 6.4.4.1: KMO and Bartlett Test for Coping Self-Efficacy

Kaiser-Meyer-Olkin Measure of Sampling Adequacy		.678
Bartlett's Test of Sphericity	Approx. Chi-Square	951.794
	df	15
	Sig.	<0.001

The table 6.4.4.2 marks out the extracted communalities.

Table 6.4.4.2: Communalities for Coping Self-Efficacy

Communalities	Initial	Extraction
coping1	1	.708
coping2	1	.588
coping3	1	.765
coping4	1	.371
coping5	1	.532
coping6	1	.506

Table 6.4.4.3 Represents "total difference" by the number of materials extracted from the total material, which was 6 in number, and, among them, a square loading extraction sum was more than 1, where the first element was explained 57.797% because only one element was extracted.”

Table 6.4.4.3: Total Variance of the Factors in Coping Self-Efficacy

Component	Total	Initial Eigenvalue		Extraction Sum of Squared Loading		
		% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.468	57.797	57.797	3.468	57.797	57.797

2	.937	15.620	73.418			
3	.730	12.170	85.588			
4	.454	7.560	93.148			
5	.284	4.730	97.877			
6	.127	2.123	100.000			

The scree plot is given in fig. 6.4.4.1 below as the graph of eigen values with respect to their components and it can be seen here that only one component is having its eigen value greater than one and giving the biggest drop in the variance to be explained and other components were going flat after that.

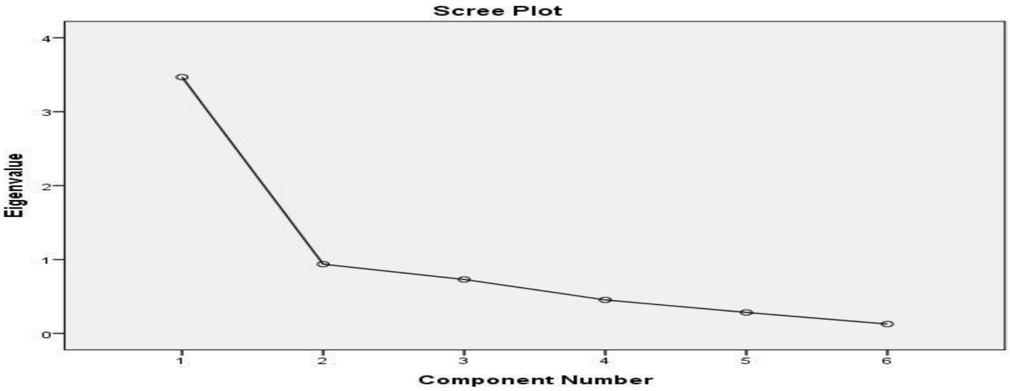


Figure 6.4.4.1: Scree Plot for The Factors in Coping Self-Efficacy

The table 6.4.4.4 describes no rotation can be performed because of the single component produced and we could see that variables coping3 followed by coping1 and coping 2 were highly correlated to the component produced.

Table 6.4.4.4: Component Matrix for the Factor in Coping Self-Efficacy

Variables for coping self-efficacy	**Component**
	1
coping1	0.841
coping2	0.767
coping3	0.875
coping4	0.609
coping5	0.729
coping6	0.711

6.4.5 Response Efficacy

The test for the applicability of factor analysis is given in table 6.4.5.1 as KMO measure was 0.669 suggesting it to be passed by the variables. And the second was Bartlett's test of sphericity that had p-value of <0.001 which meant that our correlation matrix of the variables measuring response efficacy was not an identity matrix. Together both of these tests provided the minimum standards which should be passed before the factor analysis is conducted.

Table 6.4.5.1: KMO and Bartlett's Test for Response Efficacy

Kaiser-Meyer-Olkin Measure of Sampling Adequacy		.669
Bartlett Test of Sphericity	Approx. Chi-Square	157.246
	df	3
	Sig.	<0.001

The table 6.4.5.2 gives "the extracted communalities that stated that the factor response efficacy could be explained by the higher amount of variation from the variables response_eff1 (0.664) followed by response_eff2 (0.625) and response_eff3 (0.590). None of the extracted communality was very low for the factor response efficacy."

Table 6.4.5.2: Communalities for Response Efficacy

Communalities	Initial	Extraction
Response_eff 1	1.000	.664
Response_eff 2	1.000	.625
Response_eff 3	1.000	.590

The table 6.4.5.3 below represents "the total variance explained by the extracted components from the total number of components, which were 3 in number, and only one out of them was having its eigen values greater than 1 represented in the extraction sum of squared loadings, in which the component explained 62.656% of the variation. No rotation was done because only one component was extracted out of 3."

Table 6.4.5.3: Total Variance of The Factors in Response Efficacy

Component	Total	Initial Eigenvalue		Extraction Sum of Squared Loading		
		% of Variance	Cumulative %	Total	% of Variance	Cumulative%
1	1.880	62.656	62.656	1.880	62.656	62.656
2	.606	20.185	82.841			
3	.515	17.159	100.000			

Scree plot is shown in fig. 6.4.5.1 and it was observed that only one component out of the 3 can be taken out on the basis of the eigen value criteria of being greater than 1.

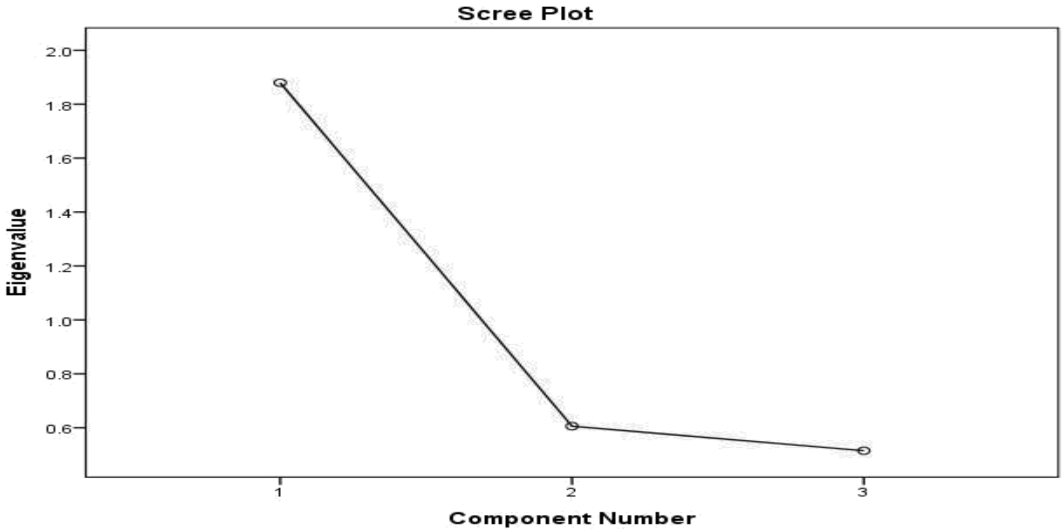


Figure 6.4.5.1: Scree Plot for The Factors in Response Efficacy

The table 6.4.5.4 given below describes how the variables were correlated within the component and no rotation could be performed because of the single component produced and it was found that variables response_eff1 followed by response_eff2 and response_eff3 were highly correlated to the component produced.

Table 6.4.5.4: Component Matrix for The Factor in Response Efficacy

Variables for response efficacy	Component
	1
Response_eff 1	0.815
Response_eff 2	0.791
Response_eff 3	0.768

6.4.6 Response Cost

The test statistics for factor analysis are given in table 6.4.6.1 as KMO measure was 0.555 suggested it will be passed by variable. And the P-Value of The Bartlett's Sphericity was 0.005 which means our reaction was not related to the cost-measuring variable.

Table 6.4.6.1: KMO and Bartlett's Test for response efficacy

Kaiser-Meyer-Olkin Measure of Sampling Adequacy		.555
Bartlett Test of Sphericity	Approx. Chi-Square	13.022
	df	3
	Sig.	.005

The table 6.4.6.2 given below shows "Passive communality which describes that the factor response cost can be traced by a higher amount of variable response_effCS1 (0.461) followed by response_effCS2 (0.414) and response_effCS3 (0.374).

Table 6.4.6.2: Communalities for Response Cost

Communalities	Initial	Extraction
res cs1	1.000	.461
res cs2	1.000	.414
res cs3	1.000	.374

The table 6.4.6.3 represents “Passive communality which describes that the factor response cost can be traced by a higher amount of variable race CS1 (0.461) followed by resCS2 (0.414) and resCS3 (0.374).

Table 6.4.6.3: Total Variance Explained of the Factors in Response Cost

Component	Initial Eigenvalue			Extraction Sum of Squared Loading		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative
1	1.249	41.634	41.634	1.249	41.634	41.634
2	.898	29.945	71.579			
3	.853	28.421	100.000			

Scree plot shown in fig. 6.4.6.1 that only one component out of the 3 could be taken out on the basis of the eigen value criteria of being greater than 1.

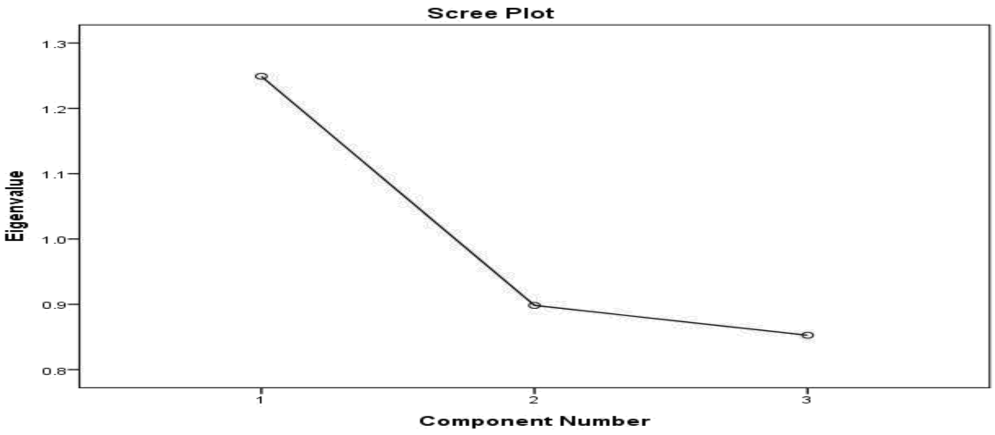


Figure 6.4.6.1: Scree Plot for the Factors in Response Cost

The table 6.4.6.4 given below illustrates no rotation could be performed because of the single component produced and we could see that variables res cs1 followed by res cs2 and res cs3 were highly correlated to the component produced."

Table 6.4.6.4: Component Matrix for the Factor in Response Cost

Variables for response cost	Component
	1
res cs1	0.679
res cs2	0.644
res cs3	0.611

6.4.7 Prior Experience with Safety Hazards

The table 6.4.7.1 The following is shown as "KMO measure 0.744 as it is a k variable and the sphericity test of The Bartlett which was the p-value of <0.001 which means that the variables relation matrix of our previous experience measurement was not a matrix. Both these tests are given a minimum standard that should be passed before the factor analysis."

Table 6.4.7.1: KMO and Bartlett's Test for Prior Experience

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.744
Bartlett Test of Sphericity	Approx. Chi-Square	997.418
	Df	21
	Sig.	<0.001

The table 6.4.7.2 gives "Passive communal data that spoke of previous experience can be explained by the variable P3 (0.830) and high amounts of P7 (0.793) and P7 (0.791).

Table 6.4.7.2: Communalities for Prior Experience

Communalities	Initial	Extraction
pe1	1.000	.680
pe2	1.000	.457
pe3	1.000	.830
pe4	1.000	.636
pe5	1.000	.316
pe6	1.000	.793
pe7	1.000	.791

The table 6.4.7.3 illustrates: In addition to the square loading extraction of the two components of the total variant described by the lifting elements obtained from the 7 elements of the total number, there is more than 1 eigen value, where the first element explained 49.381% change and the second element explained 14.943% variation.

Table 6.4.7.3: Total Variance Explained of The Factors in Prior Experience

Component	Initial Eigenvalues			Extraction Sum of Squared Loading			Rotation Sum of Squared Loading		
	Total	% of Variance	Cumulative %	Total	%of Variance	Cumulative %	Total	%of Variance	Cumulative %
1	3.457	49.381	49.381	3.457	49.381	49.381	3.248	46.398	46.398
2	1.046	14.943	64.324	1.046	14.943	64.324	1.255	17.926	64.324
3	.879	12.560	76.884						
4	.786	11.231	88.115						
5	.412	5.891	94.005						
6	.319	4.551	98.557						
7	.101	1.443	100.000						

The scree plot given in fig. 6.4.7.1 shows: the first and second factors were having their eigen values more than 1 and giving the big drops in the variance and the components.

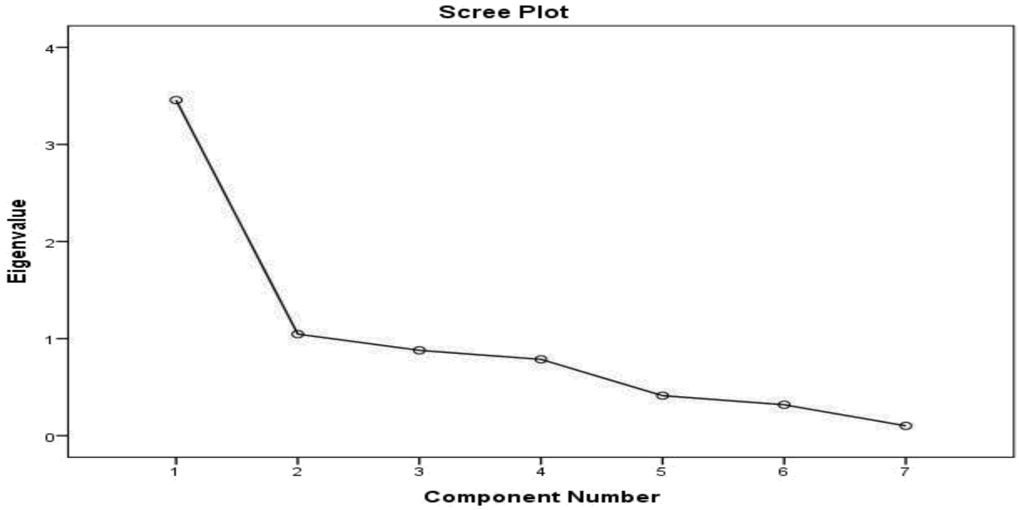


Figure 6.4.7.1: Scree Plot for the Factors in Prior Experience

The table 6.4.7.4 marks out how the variables were rotated under the factor to explain "the maximum amount of variation based on their correlation with it, and we could see that variables prior_exp1, prior_exp3, prior_exp4, prior_exp5 and prior_exp7 were highly correlated to the component 1 and variables prior_exp2 and prior_exp6 were highly correlated to component 2."

Table 6.4.7.4: Rotated Component Matrix for the Factor in Response Cost

Variables for the prior experience with safety hazard	**Component**	
	1	**2**
prior_exp1	0.797	0.211
prior_exp 2	0.306	0.603
prior_exp 3	0.899	0.146
prior_exp 4	0.792	0.090
prior_exp 5	0.561	0.031
prior_exp 6	-0.037	0.890
prior_exp 7	0.875	0.159

6.4.8 Personal Responsibility

The table 6.4.8.1 given below shows "The KMO measurement was 0.609, so it was recommended to pass the variable and Bartlett sphere test with a p-value of <0.001 which meant that our personal liability measurement did not have a relative matrix identification matrix. These two tests together provided the minimum value that should have been passed before any factor analysis."

Table 6.4.8.1: KMO and Bartlett's Test for Personal Responsibility

Kaiser-Meyer-Olkin Measure of Sampling Adequacy		0.609
Bartlett Test of Sphericity	Approx. Chi-Square	309.339
	df	3
	Sig.	<0.001

The table 6.4.8.2 alludes to "Passive communality which is the personal liability can be explained by the variables Personal_ Race 3 (0.834) followed by Personal_Rage1 and Personal_Race2. None of the communality raised for previous experience was too small."

Table 6.4.8.2: Communalities for Personal Responsibility

Communalities	Initial	Extraction
personal_res1	1.000	.718
personal_res2	1.000	.542
personal_res3	1.000	.834

The table 6.4.8.2 illustrates to "The total number of variants described by the lifting material obtained from the 3 elements, and the sum of the lifting loads of a square contains more than 1 of its eigen values, of which the element explained 69.81% of the change. No rotation was performed because one of the 3 was removed.”

Table 6.4.8.3: Total Variance Explained of the Factors in Personal Responsibility

Component	Initial Eigenvalue			Extraction Sum of Squared Loading		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative
1	2.094	69.813	69.813	2.094	69.813	69.813
2	.648	21.609	91.422			
3	.257	8.578	100.000			

Scree plot shown in fig. 6.4.8.1 that only one component out of the 3 can be taken out on the basis of the eigen value criteria of being greater than 1.

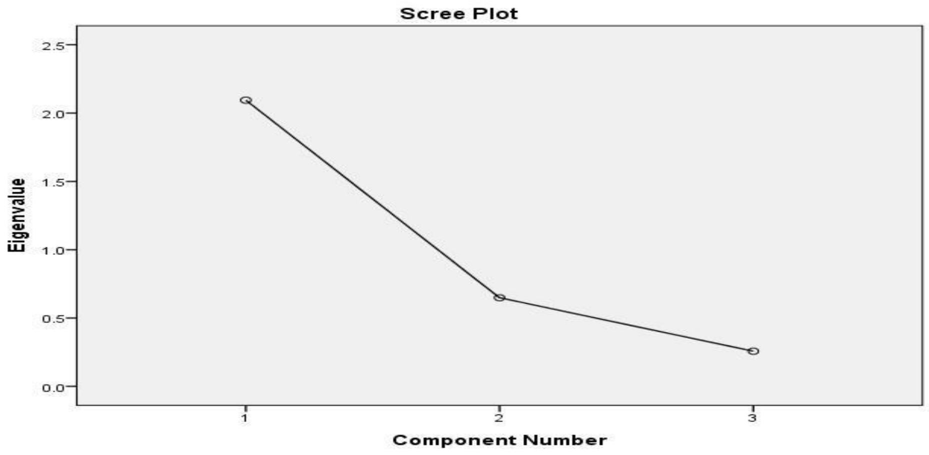


Figure 6.4.8.1: Scree Plot for the Factors in Personal Responsibility

The table 6.4.8.4 depicts how the variables were correlated within the component and no rotation could be performed because of the single component produced and we could see that variables personal_res3 followed by personal_res1 and personal_res2, were highly correlated to the component produced.

Table 6.4.8.4: Component Matrix for The Factor in Response Cost

Variables for personal responsibility	Component
	1
personal_res1	0.847
personal_res2	0.736
personal_res3	0.913

6.5 HYPOTHESIS TESTING

(a) To Find the Effect of Threat Severity and Aviation Cyber Security

H_0: Perceived Threat severity has no significant relationship with Aviation Cyber Security.

H_A: Perceived Threat severity has significant relationship with Aviation Cyber Security.

The effect of threat severity can be seen in table 6.5.2 as the R^2 value was 11% which indicates the amount of variability explained variability by threat severity from the Cyber Security. The significance of this effect can be seen in table 6.5.2 as the effect was not significant since the test statistic was having its value lower than the required critical value for the rejection of the null hypothesis.

Table 6.5.1: Model Summary Between Security Intentions and Threat Severity

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.110[a]	0.012	0.009	0.84592
a. Predictors: (Constant), threat severity				
b. Dependent Variable: intentions				

Table 6.5.2: ANOVA between Security Intentions and Threat Severity

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	2.579	1	2.579	3.604	.05
Residual	211.098	295	0.716		
Total	213.677	296			

(b) To Find the Effect of Threat Susceptibility and Aviation Cyber Security

H_0: Perceived Threat susceptibility has no significant relationship with Aviation Cyber Security.

H_A: Perceived Threat susceptibility has significant relationship with Aviation Cyber Security.

The effect of threat susceptibility can be seen in table 6.5.3 as the R^2 value was 0.1% which indicates the amount of variability explained variability by threat susceptibility from the Cyber Security. The significance of this effect can be seen in table 6.5.4 as the effect was not significant since the test statistic was having its value lower than the required critical value for the rejection of the null hypothesis.

Table 6.5.3: Model Summary Between Security Intentions and Threat Susceptibility

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.037[a]	0.001	-0.002	0.85048
a. Predictors: (Constant), threat susceptibility				
b. Dependent Variable: intentions				

Table 6.5.4: ANOVA Between Security Intentions and Threat Susceptibility

Model	Sum of Squares	df	Mean Square	F	Sig
Regression	0.297	1	0.297	0.411	.522
Residual	213.379	295	0.723		
Total	213.677	296			

(c) To Find the Effect of Respondent's Prior Experience and Aviation Cyber Security

H_0: Prior Experience with cyber threats does not significantly affects passengers' intentions towards Aviation Cyber Security.

H_A: Prior experience with online safety hazards has significant relation with Aviation Cyber Security.

The effect of respondent's prior experience with safety hazards can be seen in table 6.5.5 as the R^2 value was 4.9% which indicates the amount of variability explained variability by prior experience from the cyber security behavior. The significance of this effect can be seen in table 6.5.6 as the effect was significant since the test statistic was having its value higher than the required critical value for the rejection of the null hypothesis.

Table 6.5.5: Model Summary between Security Intentions and Prior Experience with Safety Hazards.

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.222[a]	0.049	0.046	0.82975
a. Predictors: (Constant), prior experience with online safety hazards.				
b. Dependent Variable: intentions				

Table 6.5.6: ANOVA between Security Intentions and Prior Experience with Safety Hazards

Model	Sum of Squares	df	Mean Square	F	Sig
Regression	0.297	1	0.297	0.411	.522
Residual	213.379	295	0.723		
Total	213.677	296			

(d) To find the effect of respondent's self attributes on the Aviation Cyber Security

H_0: Self Attributes (Personal responsibility) does not significantly affects passengers' intentions towards Aviation Cyber Security.

H_A: Self attributes (personal responsibility) has significant relation with Aviation Cyber Security.

The effect of respondent's personal responsibility can be seen in table 6.5.7 as the R^2 value was 0.4% which indicates the amount of variability explained variability by personal responsibility from the cyber security. The significance of this effect can be seen in table 6.5.8 as the effect was not significant since the test statistic was having its value lower than the required critical value for the rejection of the null hypothesis.

Table 6.5.7: Model Summary between Security Intentions and Self Attributes.

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.086[a]	0.007	0.004	0.84793
a. Predictors: (Constant), personal responsibility.				
b. Dependent Variable: intentions				

Table 6.5.8: ANOVA between Security Intentions and Self Attributes

Model	Sum of Squares	df	Mean Square	F	Sig
Regression	1.578	1	1.578	2.195	.140[b]
Residual	212.099	295	0.719		
Total	213.677	296			

(e) To find the effect of respondent's frequency of travelling on the Aviation Cyber Security.

H0: Frequency of flying does not significantly affect passengers' intentions towards Aviation Cyber Security

HA: Frequency of flying has significant effect on Aviation Cyber security

The effect of respondent's frequency of using flights to travel can be seen in table 6.5.11 as the R^2 value was 0.1% which indicates the amount of variability explained variability by the frequency out of the cyber security behavior. The significance of this effect can be seen in table 6.5.12 as the effect was not significant since the test statistic was having its value lower than the required critical value for the rejection of the null hypothesis.

Table 6.5.9: Model Summary between Security Intentions and Frequency of Flying of Passengers.

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.038[a]	0.001	-0.002	0.85047
a. Predictors: (Constant), frequency of flying.				
b. Dependent Variable: intentions				

Table 6.5.10: ANOVA between Security Intentions and Frequency of Flying of Passengers

Model	Sum of Squares	df	Mean Square	F	Sig
Regression	0.303	1	0.303	0.418	.518[b]
Residual	213.374	295	0.723		
Total	213.677	296			

(f) Multiple Linear Regression Model

The table 6.5.11 describes the mean, standard deviation and total sample size of the following variables, the Aviation Cyber Security Intentions, threat severity, threat susceptibility, Copying Prior experience and personal responsibility etc.

Table 6.5.11: Descriptive Statistics of the Factors Constructed by the Variables

Variables in the model	Mean	Std. Deviation	N
Security intentions	3.7874	.59206	297
Threat severity	3.8788	.91119	297
Threat susceptibility	3.9411	.67713	297
Coping Self-Efficacy	4.7744	.31657	297
Response Efficacy	4.7250	.45474	297
Response Cost	3.5107	.87206	297
Prior experience	3.9644	.71831	297
Personal responsibility	4.1291	.64505	297

The amount of variation in the table 6.5.12 as the total variation explained was 51.3%. And the significance of this model can be seen in the table 6.5.15 as the constructed model was significant with the test statistic was 43.41.

Table 6.5.12: Model Summary between Security Intentions and All Underlying Factors

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.716[a]	.513	.501	4.202

Table 6.5.13: ANOVA between Security Intentions and all factors

Model	Sum of Squares	df	Mean Square	F	Sig
Regression	5366.626	7	766.661	43.414	<0.001
Residual	5103.543	289	17.659		
Total	10470.168	296			

a. Dependent variable: security intentions

b. Predictors: Personal responsibility, Threat severity, Coping Self- Efficacy, Response Efficacy, Response Cost, Prior experience, Threa susceptibility

The table 6.5.14 mentions the parameter estimates of our threat severity, coping efficacy, response efficacy and personal responsibility are the significant contributing variables for security intention and threat susceptibility, response cost and prior experience as the non-significant contributors.

Table 6.5.14: Regression Coefficients of all the Factors under the Regression Model

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig
	B	Std Error	Beta		
(Constant)	6.460	5.046	-	1.280	.202
Threat severity	3.321	0.771	1.500	4.159	.003

Threat susceptibility	-.049-	.085	-.024	-.584	.560
Coping Self-Efficacy	-.832	.080	-.773	-10.354	.000
Response Efficacy	.332	.130	.108	2.547	0.11
Response Cost	-.055	.129	-.108	-.429	.669
Prior experience	.005	.181	.001	.028	.978
Personal responsibility	3.364	.206	1.203	16.300	.000

(g) To find the relationship between the demographic variables of the passenger's gender and Aviation Cyber Security intentions

H_{01}: Demographic variables (Gender) does not significantly affects passengers gender and aviation cyber security intentions.

H_{A1}: Demographic variables (Gender) does not significantly affects passengers gender and Aviation Cyber Security intentions.

The table 6.5.15 alludes to the cross tabulation of gender of the passenger and their aviation cyber security intention. A Fisher's Exact test was conducted to find out the relationship between them, the test statistic was 6.59 with 4 degrees of freedom and it was not significant(p-value=0.159). So, we failed to reject the null hypothesis.

Table 6.5.15: Cross-Tabulation of Passenger's Gender and Security Intentions

Security intentions	**Gender**		**Total**
	Male	**Female**	
Highly disagree	18	2	20
Disagree	19	11	30
Neutral	31	7	38
Agree	83	19	102

Highly Agree	86	21	107
Total	237	16	297

H02: Age of the passengers has no significant relationship with their Aviation Cyber Security intentions.

HA2: Age of the passengers has a significant relationship with their Aviation Cyber Security intentions.

The table 6.5.16 alludes to the cross tabulation of age of the passenger and their Aviation Cyber Security intention. A Fisher's Exact test was conducted to find out the relationship between them, the test statistic was 23.87 with 12 degrees of freedom and it was significant(p-value=0.021). So, we reject the null hypothesis to conclude that the relationship was significant.

Table 6.5.16: Cross-Tabulation of Passenger's Age and Security Intentions

Security intentions	**Age**				**Total**
	18-30	**31-40**	**41-50**	**51 and above**	
Highly disagree	4	9	4	3	20
Disagree	15	4	10	1	30
Neutral	9	10	13	6	38
Agree	35	18	37	12	102
Highly agree	30	22	50	5	107
Total	93	63	114	27	297

Chi-Square Tests

	Value	**df**	**Asymp. Sig. (2-sided)**
Pearson Chi-Square	23.871[a]	12	.021

Likelihood Ratio Linear-by-Linear	22.958	12	.028
Association	.507	1	.476
N of Valid Cases	297		

a.4 cells (20.0%) have expected count less than 5. the minimum expected count is 1.82.

H$_{03}$: Education of the passengers has no significant relationship with their Aviation cyber security intentions.

H$_{A3}$: Education of the passengers has a significant relationship with their Aviation cyber security intentions.

The table 6.5.17 alludes to the cross tabulation of education of the passenger and their aviation cyber security intention. “A Fisher’s Exact test was conducted to find out the relationship between them, the test statistic was 17.79 with 8 degrees of freedom and it was significant(p-value=0.023). So, we reject the null hypothesis to conclude that the relationship between passenger’s age and security intension was significant.”

Table 6.5.17: Cross-Tabulation of Passenger’s Education and Security Intentions

Security intentions	**Education**			**Total**
	Graduate	**Postgraduate**	**Others**	
Highly disagree	0	17	3	20
Disagree	4	21	5	30
Neutral	11	17	10	38
Agree	13	69	20	102
Highly agree	20	56	31	107
Total	0	17	3	20

Chi-Square Tests

	Value	**df**	**Asymp. Sig. (2-sided)**
Pearson Chi-Square	17.796[a]	8	.023

Likelihood Ratio Linear-by-Linear	20.344	8	.009
Association	.125	1	.724
N of Valid Cases	297		

a. 3 cells (20.0%) have expected count less than 5. The minimum expected count is 3.23.

(h) To find the effect of the demographic variables on the aviation cyber security intensions

H_0: Demographics (gender, age, education) of the passengers have no significant effect on the Aviation cyber security intentions.

H_A: Demographics (gender, age, education) of the passengers have significant effect on the Aviation cyber security intentions.

Table 6.5.18 shows that the amount of variability explained by the independent variables (gender, age and passenger education) out of the dependent variable (security intensity) is 5%. The effect can be seen in Table 6.5.19 which was not significant as the test statistical value of 0.513 was lower than the critical value. We therefore failed to reject the null hypothesis in order to conclude that the influence of demographic variables (all combined) on the safety strength of passengers was not important.

Table 6.5.18: Model Summary between Security Intentions and Demographics of the Passenger

Model	R	R Square	Adjusted R Square	Std Error of the Estimate
1	.072[a]	0.005	-0.005	0.85174
a. Predictors: (Constant), Education, Gender, Age				
b. Dependent Variable: intentions				

Table 6.5.19: ANOVA between Security Intentions and Demographics of the Passenger

Model	Sum of Squares	df	Mean Square	F	Sig
Regression	1.117	3	0.372	0.513	.674
Residual	212.560	293	0.725		
Total	213.677	296			
a. Dependent Variable: intentions					
b. Predictors: (Constant), Education, Gender, Age					

6.6 DATA ANALYSIS USING PARTIAL LEAST SQUARE-STRUCTURAL EQUATION MODELLING (PLS SEM)

The data analysis of the current study was carried our using PLS SEM (Partial least square Structural Equation Modelling) Technique. A two-stage analysis process was carried out, firstly, the measurement model was analysed to ascertain the validity and reliability of the measures used. For the Consistent PLS algorithm was used to generate factor loadings and correlations between the constructs. The results of the Consistent PLS algorithm are shown in the figure. The factor loadings are shown in Table 6.6.1. All the loadings are greater than 0.50 and were found be statistically significant during the Bootstrapping (See Figure 6.6.1, measurement model).

Table 6.6.1: Shows Factor Loadings

	Coping Self Efficacy	Personal Responsibility	Prior Experience	Response Efficacy	Security Intentions	Threat Severity	Threat Susceptibility
cs1	0.892						
cs2	0.861						
cs3	0.903						

	Coping Self Efficacy	Personal Responsibility	Prior Experience	Response Efficacy	Security Intentions	Threat Severity	Threat Susceptibility
cs4	0.800						
cs5	0.913						
cs6	0.799						
i1					0.858		
i2					0.808		
i3					0.859		
i4					0.896		
i5					0.531		
i6					0.623		
i7					0.538		
pe1			0.694				
pe2			0.823				
pe3			0.955				
pe4			0.656				
pe5			0.606				
pe6			0.609				
pe7			0.856				
pr1		0.856					
pr2		0.807					
pr3		0.875					
re1				0.827			
re2				0.770			
re3				0.903			
ts1						0.766	
ts2						0.866	
ts3						0.939	
ts4						0.805	

	Coping Self Efficacy	Personal Responsibility	Prior Experience	Response Efficacy	Security Intentions	Threat Severity	Threat Susceptibility
ts5						0.514	
ts6						0.569	
ts7						0.633	
tsp1							0.910
tsp2							0.832
tsp3							0.681
tsp4							0.826

6.6.1 DEVELOPMENT OF STRUCTURED EQUATION MODEL USING PLS SEM

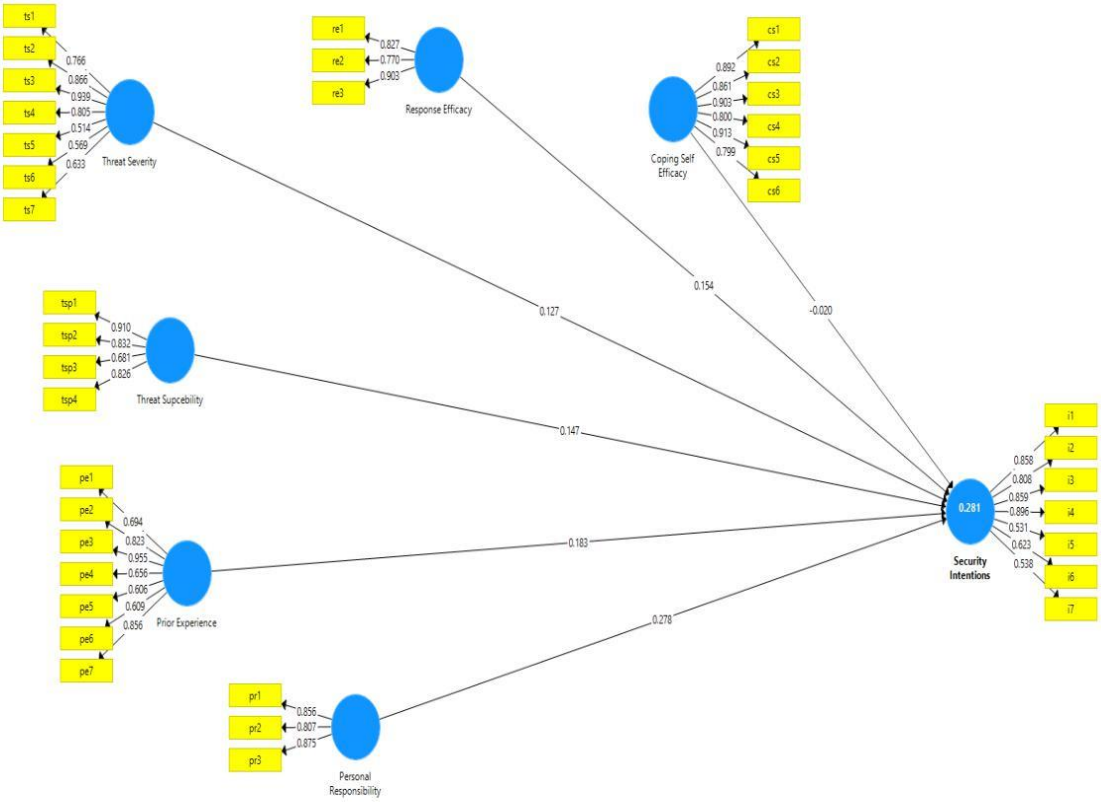


Figure 6.6.1: Structured Equation Model

The figure 6.6.1 displays the structured model was constructed out of the significant relationships and effects appeared from the previously done tests and analysis. The fitted model was a good as the GFI achieved was 0.92, CFI was 0.931 and TLI was 0.901. The method used for parameter estimation was partial least squared which produced the estimates given in table 6.6.2.

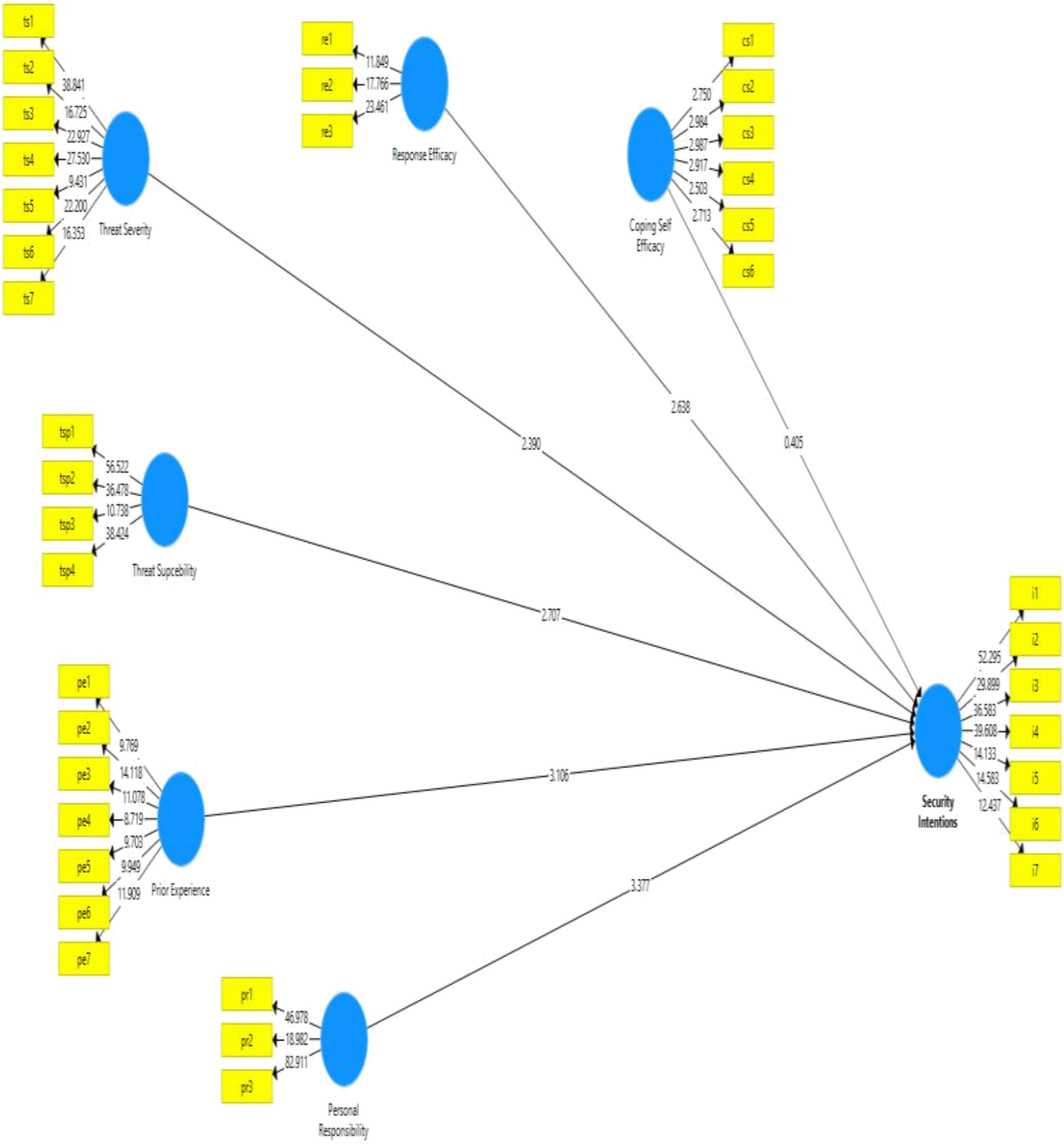


Figure 6.6.2: Structural Model estimated with Bootstrapping Method Showing values of Path Estimates

Table 6.6.2: Regression Parameter Estimates from the Structured Model

Regression Parameter Estimates	Coefficient	Standard Error	T Statistics	P-Value
Coping Self Efficacy → Security Intentions	-0.015	0.075	0.660	0.509
Personal Responsibility→ Security Intentions	0.242	0.072	3.315	0.001
Prior Experience → Security Intentions	0.170	0.055	3.002	0.003
Response Efficacy → Security Intentions	0.154	0.059	2.621	0.009
Threat Severity → Security Intentions	0.144	0.058	2.439	0.015
Threat Susceptibility → Security Intentions	0.151	0.056	2.713	0.007

6.7 PROPOSED FRAMEWORK

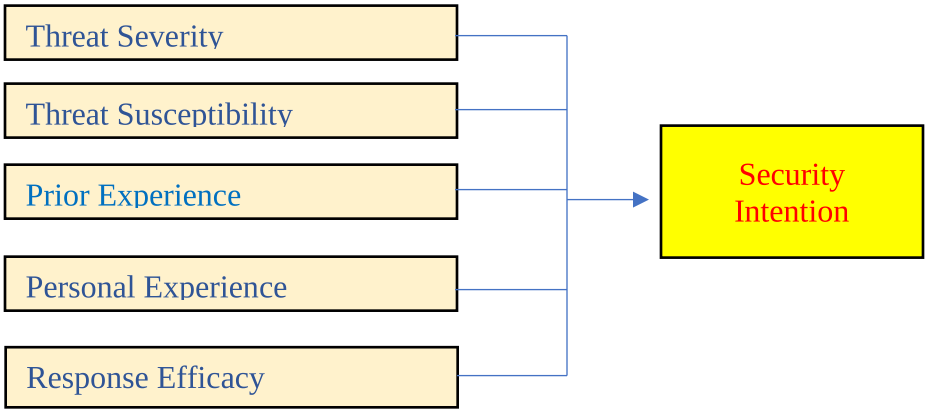


Figure 6.7.1 Proposed Framework

CHAPTER 7

FINDINGS, CONCLUSION AND SUGGESTION

This chapter outlines the findings, suggestions, and conclusions of the specific research project. This study was borrowed from the Protection Motivation Theory as a benchmark and further developed a model for its application in the fight against cyber security in aviation. The selected variables pertaining to the threat intensity, threat potential, prior experience with security risks and personal responsibility are examined for their relevance during study of the additional changes and behavior analysis. The study is based on Cyber Threat Perception in Indian Civil Aviation with respect to Delhi Airport, with 297 respondents selected for the study. The proposed research addresses some of the associated issues related to cyber security threats to the civil aviation environment through behavioral change and passenger management. The data collected for the study were grouped and analyzed in accordance with the objectives set for the study. The IBM 24.0 "Statistics Kit for Social Sciences" (SPSS) was used for data analysis to apply techniques such as the reliability test, multiple regressions, and dimension reduction factor analysis to a hierarchical equation model.

7.1 FINDINGS OF THE STUDY

7.1.1 Demographic Information

The demographic profile of the respondent has been determined from the gender distribution of the respondents; as out of 297 respondents, 79.8% of respondent were male and 20.2% of respondent were female. The age distribution of respondent indicated that out of 297 respondents, 31.3% of the respondents belonged to the age group of 18 to 30 years ,21.2% of respondents were from 31 to 40 years, 38.4% of respondents were from the age group of 41 to 50 years and 9.1% of respondents were of 51 years or more. 16.2% of respondent were graduates and 60.6% of respondent were postgraduates, 23.2% of respondents were post graduate and above. It was observed that 8.1% of respondent have used the flights to travel for 11 or more times, followed by the ones who used it for 6 to 10 times (18.2%), 2 to 5 times (45.5%) and only once a year (28.3%).

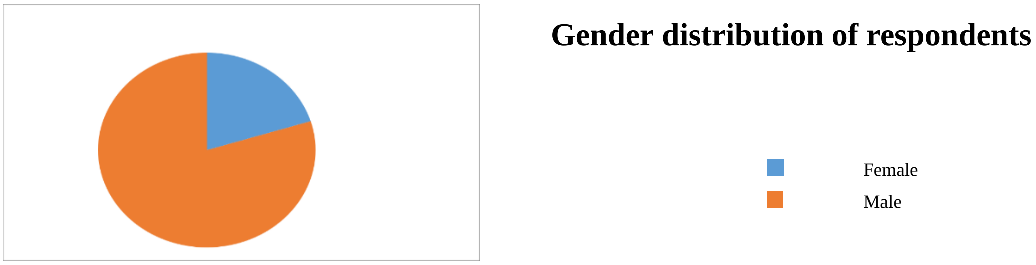


Figure 7.1 Gender Distributions of Respondents

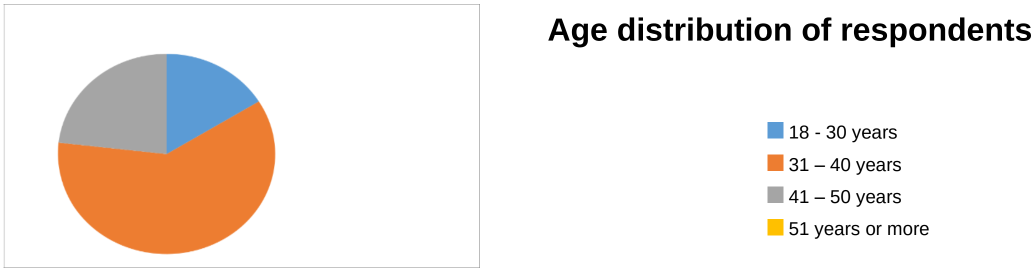


Figure 7.2 Age Distribution of Respondents

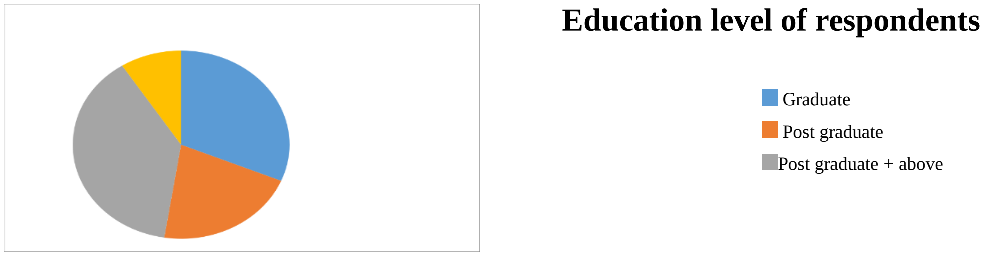


Figure 7.3 Education Level of Respondents

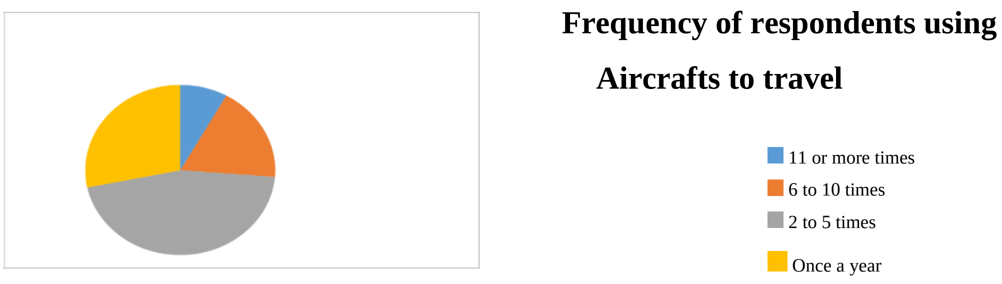


Figure 7.4 Frequency of respondents using Aircrafts to travel

7.1.2 Inference and Analysis of Data Collection: PMT aspects

(a) **Constructs of Threat Severity:** It was found that 5.7% of respondents strongly disagreed with the susceptibility of airports to cyber-attacks, while 25.9% agreed and 37.7% strongly agreed. 45.5 per cent of respondents strongly agreed and 27.3 % respondent agreed that their computer / mobile / I would run slowly when they were connected to Wi-Fi available at the airport, while 2.4 % respondent strongly disagreed and 6.7 % respondent disagreed and 18.2 % respondent were neutral.

It was found that 34 % respondent strongly agreed, and 27.3 % respondent agreed that they were very happy using free Wi-Fi at Delhi Airport compared to other airports, and 6.4 % respondent strongly disagreed. 22.2% of the total respondents believe that there is no distinction between using Wi-Fi at Delhi airport and other airports. It was noted that improved awareness among passengers by means of cyber protection at airports was widely supported by 44.4% of respondents, and 26.35 % respondent also agreed that 3.7% of respondents strongly disagreed that awareness could not ensure safety, and 13.8% of respondents claimed that it would not make any difference. It was noted that 36.4 % respondent strongly agreed that using Wi-Fi at airports could compromise their personal Aadhar/ ID/ PAN number or credit card information, and 6.1 per cent of respondents strongly disagreed and 20.2 per cent did not feel any difference in using their identity and credit card details. 38.7 per cent of respondents strongly agreed and 31.6 per cent agreed that the details exchanged in public locations, such as the airport / railway station, could be used to commit crimes and 3.4 per cent strongly disagreed and agreed.

(b) **Constructs of Threat Susceptibility:** Once asked about the risk of running personal IT devices in the cyber domain, it was found that 28.3 % respondent strongly agreed that their devices were extremely secure to use in an airport and only 4 % respondent strongly disagreed with them, while

26.3 % respondent thought that there was no difference in safety in using their devices anywhere. Only 8.15 % respondent of the total respondents strongly disagreed with the recommendation to use mobile phones and computers inside the airport / aircraft, but 34.7 % respondent strongly agreed to the recommendation. It was found that 44.1% of respondents were very much in agreement, and 32.7% of respondents agreed that Delhi Airport took adequate precautionary steps to safeguard cyber security at airports, but 9.1% disagreed. 46.1% of respondents strongly agreed, and 23.9% of respondents agreed that airport IT systems could not be hacked and that they were not susceptible to any risk from using the Internet at the airport, while 4.7% of respondents strongly disagreed with the same.

(c) **Constructs of Coping Self-Efficacy:** When asked to rate the correct steps taken by airports to protect themselves from cyber nuisance, it was found that 77.4% of respondents strongly agreed that they were comfortable taking measures to safeguard their devices when using the public internet at airports, and that no one disagreed for the same reason. And 78.1% of respondents said that the security steps that could be taken were completely beyond their power. It was noted that 76.1 per cent of respondents had the skills to take the requisite security steps and 77.4 per cent of the respondents were very much in agreement and 22.6 per cent agreed that taking the necessary security measures at the airport was as easy as elsewhere. It has been found that 78.8 % respondent agree that they are afraid to think about cyber security. It was found that 76.8% of respondents strongly agreed that they were free from any danger when using public Wi-Fi at airports / aircraft.

(d) **Constructs of Response-Efficacy:** Respondents have also been questioned about the rate and cost of cyber nuisance safety and protection. And the number of respondents who strongly agreed to pay more for a better cyber world was 31.3 % respondent and 9.1 % respondent of respondents strongly disagreed and 14.5 % respondent disagreed. 29 % respondent strongly agreed, and 23.2 % respondent agreed that security programs interfered with other programs on their phones, and 12.5 % respondent disagreed, and 21.5 % respondent did not have any problems using security programs on their phones because they did not interfere with other programs they were using.

(e) Constructs of Prior Experience with Safety Hazards: With regard to previous experience with the use of browsing devices at airports and 41.1 % respondent strongly agreed and 26.6 per cent of respondents agreed that their IT devices slow down after browsing at airports and 24.2 % respondent did not find any difference and 2 % respondent strongly disagreed with the same. 43.4% respondent strongly agreed, and 24.2 percent of respondents agreed that their computers had a virus attack from opening a connection while browsing, and just 8.1 % respondent disagreed. It was noted that 41.4 % respondent strongly agreed that they had experienced a virus attack from only visiting a web site while surfing, and 6.1 % respondent disagreed, and just 1 % respondent strongly disagreed. 44.4 % respondent strongly agreed that they had obscure icons or programs on their phone when searching the airport, while only 1 percent strongly disagreed, and 7.1% respondent disagreed. It was found that 46.5 % respondent strongly agreed that a pop-up message offering a free computer security scan appeared on their screen, and only 3 % respondent strongly disagreed that the message did not appear. Respondents were asked about their previous knowledge of the valuable personal details being compromised when searching their aircraft at the airport and 33 % respondent were very much in agreement and 33 % respondent of total respondents were in agreement, when 5.1 % respondent strongly disagreed, and 5.1 % respondent disagreed. 41.8 % respondent strongly agreed, and

26.6 % respondent agreed that they had been the victim of an online scam and had lost money while using their apps.

(f) **Constructs of Personal Responsibility:** It was found that they were prepared to be more informed and to be more aware of the actions taken as passengers, to make airport the security systems safer, and it was noted that 31.6 % respondent agreed, while 56.2 % respondent strongly agreed that if cyber security measures were taken, they would make a difference, while 1.7 % respondent strongly disagreed. 29 % respondent total respondents strongly agreed, and 54.5 % respondent agreed that one person's attempts to protect cyberspace at airports were futile, although 1.3 % respondent strongly disagreed. It was found that 33.7% of respondents strongly agreed, and 58.2% % respondent s agreed that every passenger could make a difference when it comes to cyber security, but 1% of respondents disagreed.

(g) **Constructs of Security Intentions:** Actions on the possibility of introducing security measures to secure themselves online when traveling at airports have been established are the future. It was noted that 39.4 % respondent strongly agreed, and 32.3 % respondent agreed and 10.1 per cent disagreed and 18.2 per cent were neutral. 33.3 % respondent strongly agreed, and 27.3 per cent disagreed that they would upgrade their security measures to better protect themselves while using free Wi-Fi at the airport, and 2 % respondent strongly disagreed, and 20.2 per cent disagreed. It was found that 39.1 per cent of respondents strongly agreed, and 30.6 % respondent agreed that they would not save their passwords while using mobile / computer at airports, and only 0.7 per cent of respondents strongly disagreed. 33.7% of respondents strongly agreed, and 41.8% of respondents agreed that they would use passwords that would be difficult to guess, and only 2% of respondents disagreed. It was noted that 36.4 % respondent strongly agreed to change their browser security settings to a higher level, were vigilant about using their airport device, and 5.1 % respondent strongly disagreed, and 13.1 per cent of respondents disagreed. 35.4 % respondent strongly agreed, and 25.3 % respondent agreed that they would learn how to be more secure online at the airport, while 8.1 % respondent strongly disagreed.

7.2 RELIABILITY MEASURES OF PARAMETERS OF PROTECTION MOTIVATION THEORY (PMT)

(a) **Threat Severity, Susceptibility, Coping Self-Efficacy, ResponseEfficacy, Cost:** It was found that the threat severity of 0.920 showed a high internal consistency of the measuring instrument for the constructed factor. Furthermore, the "threat susceptibility" of 0.752 showed a high internal consistency of the measuring instrument for the constructed factor. The "coping self-efficacy" of 0.85 was found to elucidate the high internal accuracy of the measuring instrument for the constructed component. The "response efficacy" of 0.669 was found to have adhered to the high internal consistency of the measuring instrument for the constructed factor. In addition, the "response cost" of 0.533 eluded the low internal accuracy (less than 0.6) of the measuring instrument for the constructed component.

(b) **Improved Reliability of Response Cost:** It explains that reliability of response cost will be 0.089 if we delete the first item of ready to pay extra for safer cyber environment, if we delete the second item, then reliability of response cost will be 0.818. It means that deleting the second item will increase our reliability of the instrument for response cost.

(c) **Prior Experience with Safety Hazards:** It was found that the previous experience of 0.907 showed a strong internal accuracy of the measuring instrument for the built component.

(d) **Reliability of Personal Responsibility:** It was found that the personal responsibility of 0.753.

(e) **Security Intentions:** It was found that the security intentions as 0.883, showing high internal consistency of the measuring instrument for the constructed factor.

7.2.1 Discriminant Validity

It was observed that the square root of AVE was higher than the correlation, which indicated that all the constructs exhibit discriminant validity.

7.3 FACTOR ANALYSIS WITH PRINCIPAL COMPONENT ANALYSIS

(a) **Security Intentions:** The KMO measure was 0.693 for multiple variables. Bartlett’s sphericity test, having a p-value of < 0.001, means that security purpose variable matrix measurement was not an identity matrix. It was stated that the security factor could explain higher variations with the variable security intention1 (0.869), security intention3 (0.828) and lower security intention5 (0.242). Out of a total of 7 components, two of them were equalized with a proprietary value < 1, sum of square loads, in That's the first element accounted for 43.16% of the variation and the second component accounted for 21.706 percent of the variance as the underlying factor. The first two components account for the most variance that can be seen as large drops in the graphs, and the other components, which account for very low variation, give small drops to the second component and have low own values. It also showed how the variables rotate under the factors to explain the maximum amount of variation based on their correlation.

(b) **Threat Severity:** The KMO measure amounted to 0.836. Bartlett's p-value alluding sphericity test of 0.001 suggested that the correlation matrix the risk variation measure was not an identity matrix. Together, both tests were provided for minimum standards before analyzing a factor. It also stated that the factor threat severity could explain higher variations in the variable threat severity1 (0.941) followed by threat severity6 (0.931) and threat severity4 (0.876). None of the community extracted is very low due to the severity of the threat factor. Of the total components, their two individual values were larger than 1, represented by the square load extraction sum, whereas the first element was 61,086 percent of the variation and the second 15,565 percent. "The first factor was 46,383 percent, while the second factor was 30,268 percent. And the first component explains the most variation that gives the biggest drop to the second component that has an own value of more than 1. After the second component has more than 1 own value, all other factors give a flat graph and are unable to explain much of the variation. As a result, it was shown how the variables rotate under the factors to explain the maximum amount of variation based on their correlation with them, and We found that variable intensity 1, 4, 5 and 6 element 1 and variable 2, 3 and 8 was highly associated.

(c) **Threat Susceptibility:** It was found that the KMO measure with respect to the susceptibility of the threat was found to be 0.567. "Bartlett's sphericity test showed a p-value of < 0.001 indicating that Matrix of probability measuring variables of the threat was not identical. The factor threat susceptibility was expected to explain higher variations from the variable threat sus3(0.868) followed by threat sus1 (0.0.665), threat sus2(0.646) and threat sus4(0.456). None of the community extracted is very low because of the threat susceptibility factor. It was noted that of the 4 total components, of which two of them had their own standard square load extraction sum was larger than 1, while the first factor explained 39,927 percent of the variation and the second element difference 25,959 percent. The first factor explained 39.77 percent of the variance and the second factor explained 26.116 percent of the variance after varimax rotation. "The first and second components with their own values more than 1 indicated large variance drops and the third and fourth components were associated with their own values less than 1.

It has therefore been shown how the variables rotate under the factors to explain the maximum amount of variation based on their correlation with them, and we have found that the variables threat sus1, threat sus2 are highly correlated with component 1 and the variables threat sus3 and threat sus4 are highly correlated with component 2.

(d) **Coping Self Efficacy:** KMO measure for coping self-efficiency was accounted to be 0.678. “Bartlett’s test of sphericity had the p-value of <0.001, which meant that the correlation matrix was not an identity matrix. It was stated the factor coping self-efficacy could explain higher amount of variation from the variable coping3 (0.765) followed by coping1 (0.708), coping2(0.588) and coping5 (0.532). None of the extracted communality is very low for the factor coping self-efficacy. Now the total variance explained by the extracted components from the It was observed that out of 6 total number of components, one out of them had its eigen values greater than 1 which represented the extraction sum of squared loadings, in which the first component explained 57.797% of the variation.” Hence it was shown that only one component is having its eigen value greater than one and giving the biggest drop in the variance to be explained and other components were going flat after that. And described how the variables were correlated within the component and no rotation can be performed because of the single component produced and we could see that variables coping3 followed by coping1 and coping2 were highly correlated to the component produced.

(e) **Response Efficacy:** The KMO measure for "response efficiency" was 0.669. "Bartlett's sphericity test referred to a p-value of < 0.001, indicating the non-identity of the matrix of the correlation. It was stated that the efficacy of the factor response could be explained by higher variations in response eff1 (0.664) followed by response eff2 (0.625) and response eff3 (0.590). None of the community extracted was very low for the efficacy of the response factor. It was observed that of the 3-total number of components, only one of them had its own values that represent edited square load, where 62,656 percent of the material is defined. So, it is described how the variables were related to the material and could not rotate due to the unit element produced and it was found that the variables response eff1 followed by response eff2 and response eff3 were highly correlated with the component produced.

(f) **Response Cost:** It was found that the KMO "response cost" measure was 0.555 for all variables "Bartlett's sphericity test accounted for a p-value of 0.005, which meant that the correlation matrix was not an identity matrix. Unpublished communalism shows that factor reaction costs can be explained by CS1 (0.461) and followed by Race CS2 (0.414) and Race CS3 (0.374). None of the communities that have been expelled are too low for threats. It was found that only one of the three components had its own value of 1 represented by the square load extraction sum while 41,634 percent of the material was explained. No rotation has been made because only one of the 3 elements has been removed. It was therefore shown that the variables were correlated within the component and could not be rotated due to the single component produced, and we could see that the variables res cs1 followed by res cs2 and res cs3 were highly correlated with the component produced.

(g) **Previous Experience with Safety Hazards:** The KMOs for the alleged side were 0.744. "The bartlett's inflation test shows a P-Value of 0.001 of the proposed non-recognition matrixes. It is said that previous experience can be explained by the high amount of Factor PE3 (0.830) variables followed by PE6 (0.793) and PE7 (0.791). Of the 7 totals, only two of them had their own standard square load extraction total was larger than 1, while the first element explained 49,381 percent and the second factor explained 14,943 percent of the variation". In this way, it is observed how variables are rotated under the factor to explain the maximum amount of variation based on diversity.

(h) **Personal Responsibility:** The KMO measure for personal responsibility was 0.609, and the Bartlett test with P-Value indicated that the relationship matrix was incomprehensible, indicating that the personal responsibility element could be explained by a higher amount of previous experience material, which was not very low in the community, one of the 3 elements in the community had its own value of more than 1 which represented the addition of square load extract. Where the material explains 69.81 percent of the diversity. No rotation was performed because only one of the 3 elements was removed. Thus, it shows how the variable was related to the material and could not be rotated due to the unit produced, and we found that the variable is highly related to the individual res2 produced after the individual res1 and the personal res3.

7.3.1 Hypothesis Testing

(a) **The Effect of Threat Severity and Aviation Cyber Security Intention:** It was observed that the effect of threat severity was as the R^2 value was 11% which indicates the amount of variability explained variability by threat severity from the Cyber Security intention. The effect was not significant since the test statistic was having its value lower than the required critical value for the rejection of the null hypothesis.

(b) **The Effect of Threat Susceptibility and Aviation Cyber Security Intention:** It was observed that the effect of threat susceptibility as the R^2 value was 0.1% which indicates the amount of variability explained variability by threat susceptibility from the Cyber Security intention. The effect was not significant since the test statistic was having its value lower than the required critical value for the rejection of the null hypothesis.

(c) **The Effect of Respondent's Prior Experience and Aviation Cyber Security Intention:** It was observed that the effect of respondent's prior experience with safety hazards as the R^2 value was 4.9% which indicates the amount of variability explained variability by prior experience from the Cyber Security intention. The effect was significant since the test statistic was having its value higher than the required critical value for the rejection of the null hypothesis.

(d) **The Effect of Respondent's Self Attributes on the Aviation Cyber Security Intention:** It was observed that the effect of respondent's personal responsibility as the R^2 value was 0.4% which indicates the amount of variability explained variability by personal responsibility from the Cyber Security intention. The effect was not significant since the test statistic was having its value lower than the required critical value for the rejection of the null hypothesis.

(e) **The Effect of Respondent's Frequency of Travelling on the Aviation Cyber Security intention:** The effect of respondent's frequency of using flights to travel as the R^2 value was 0.1% which indicates the amount of variability explained variability by the frequency out of the Cyber Security intention. The effect was not significant since the test statistic was having its value lower than the required critical value for the rejection of the null hypothesis.

7.3.2 Multiple Linear Regression Model

This model took into account the standard deviation and total sample size of the following variables, the Aviation Cyber Security behavior (intention), Prior experience and personal responsibility. It was found that the total variation explained was 51.3%. This constructed model was significant with the test statistic of 43.41. It was mentioned the parameter estimates of our threat severity, coping efficacy, response efficacy and personal responsibility are the significant contributing variables for security intention and threat susceptibility, response cost and prior experience as the non-significant contributors.

(a) **The Relationship between the Demographic Variables of the Passengers and Aviation Cyber Security Intentions:** It was found that the relationship between them, the test statistic was 6.59 with 4 degrees of freedom and it was not significant (p-value=0.159). So, we were failed to reject the null hypothesis. A "Fisher's Exact" test was conducted to find out the relationship between them, the test statistic was 23.87 with 12 degrees of freedom and it was significant (p-value=0.021). So, we reject the null hypothesis to conclude that the relationship was significant. It was also found that the relationship between them, the test statistic was 17.79 with 8 degrees of freedom and it was significant (p-value=0.023). So, we reject the null hypothesis to conclude that the relationship between passenger's age and security intension was significant.

(b) **The Effect of the Demographic Variables on the Aviation Cyber Security Intensions:** It was found that the amount of variability explained by the independent variables out of the dependent variable (security intension) as 5%. The effect was not significant as the test statistic value of 0.513 was lower than the critical value. So, we failed to reject the null hypothesis and conclude that the effect of demographic variables (all combined) was not significant on the security intension of the passengers. It was shown that the structured model was constructed out of the significant relationships and effects appeared from the previously done tests and analysis. The fitted model was a good as the GFI achieved was 0.92, CFI was 0.931 and TLI was 0.901. The method used for parameter estimation was partial least squared which produced the estimates.

7.4 <u>LIMITATION OF STUDY</u>

Studying only perception/ behavioral aspects of ascertaining Aviation Cyber Security.

(a) The framework is limited to the theoretical premise and its applicability to the Aviation industry.

(b) Hesitant of Airport employees and lack of participation from airport due to trust deficit and sharing of info on security.

7.5 <u>CONTRIBUTION TO THEORY AND FUTURE SCOPE</u>

(a) The study reaffirms applicability of PMT in the Aviation Cyber Security.

(b) The results are conclusive of the facts that the so far Aviation Industry considered for leisure and business travel too shares an inherent risk of safety especially in Cyber domain and people have to be made aggressively aware of the same.

(c) To optimise the results of study there is requirement to create higher awareness of aviation cyber security among passengers and definitely to the employees: continuity-in-training, accountability, increase awareness in larger way.

7.6 CONCLUSION

Cybercrime is invigorating to new scales, rapidly targeting people, organizations and governments. The estimated costs of cybercrime for the global economy are around $445 billion per year, with 800 million being subject to cyber surveillance and loss of private data in 2013. Irrespective of many existing counter-measures to ensure client honesty by resisting malicious activities. Such activities may be coordinated either against themselves or against authoritative resources where the client is used as a backdoor by cyber criminals. As a key institution in international trade, travel and aviation are central to the global economy, contributing 3.5 per cent of global total national output (GDP). Low-cost aviation, combined with rising revenues, has had an impact on the growth of passenger traffic. India's passenger traffic increased by 11.64 percent year-on-year to 344,70 million in FY19. Moreover, India's domestic aviation market is reported to be fastest at the rate of 114 per cent between 2013-18 overcoming Japan and Germany as far as air passengers are concerned. India projected to have 482 million flyers by 2036. The situation is replicated with regard to the integration of cyberspace into the industry. The role of these technologies has increasingly shifted across multiple dimensions, including land, sea, air and space military operations. However, the intentions of cyberspace technology are often misplaced and there is ample evidence to confirm the abuse of its potential by criminals and terrorist groups. If it remained uncensored or regulated in some way, it might coax to be an independent theater of war. Cyberspace, as an independent threat, endangers the very ability to use these facilities: security services cannot be prevented in isolation. Effective constructive action would sincerely consider forging a rift of partnerships between public and government enterprises. Various frameworks for cyber security in the aviation sector and protection motivation theory and its role have been described in this research. Based on the PMT, it has been validated that threat assessments include online security protection. In some studies, the severity of the threat was an important factor in predicting safety-related protection, while some studies concluded otherwise. Threat variables have been further expanded in recent security research, integrating multiple variables to measure threat assessments.

The National Information Technology Center (NIC) was established in 1975. Between 1986 and 1988, three NWs were set up: INDONET (Indian Computer Infrastructure) and now multiple agencies like National Critical Infrastructure Information protection center (NCIIPC), CERTs, sector specific has been established. The number of Internet users is astounding 690 million in country today. Creating awareness on Cyber safety and Security too is another astounding challenge however being delved upon.

Cyber attackers are capitalizing on multiple vulnerabilities sustained by cyberspace software and hardware design. Using malware, hacking and D-DOS attacks on targeted websites. With each passing day, the scope and nature of the threats proliferate.

The additional framework has been drafted to address the far accomplishment point of cyber security for the aviation:

(a) **Establishment of a Regular Cyber Standard for Aircraft Systems**: NIST, ICAO and many other organizations globally are working towards this and likely to come up with suitable framework exclusively for Aviation Cyber Security.

(b) **Ensuring a Culture of Cyber Security**: A similar order in which a high level of aviation security is achieved should also be linked to the creation of a specific vision, robust strategy, objectives and classifications, and a unique framework for addressing the cyber threats.

(c) **Understanding the Threat:** The community should have a basic understanding of the type of threat and their contributions for effective design of safety framework.

(d) **Understanding the Risk**: To monitor cyber risk, it is essential for industry to recognize the components of the aviation framework that need to be guaranteed. With many partners, the Aviation Framework is a broad and complex international substance. Investment and a restricted procedure will be required to understand the networks of the framework.

(e) **High Awareness of the Situation**: A very high situational awareness among the travellers is equally essential and this can be achieved through various videos through kiosks or entertainment channels.

(f) **Provide an Incident Response:** The quickest way of recovery of the incident is through effective incident response and these must be adequately rehearsed and practiced to perfection with closed loop feedback.

(j) **Continuous Research and Progress:**

(i) Create secure and resilient framework architectures, including techniques to maintain a secure data exchange, basic data separation successful attacks recovery.

(ii) Quick detection of attacks; and clarity of the legal compliances.

(k) **Ensure that the Government and Industry Work Together:** This includes:

(i) Establishing a policy for advancing short and long-distance IT security.

(ii) Characterize recognized international standards of behaviour.

(iii) Strengthen the ramifications for horrible behavior; and Placing IT security as a major necessity in discretionary motivation.

7.7 THE ROAD AHEAD

The importance of the aviation industry cannot be diminished for the economy of any country. Currently the threads are down due to CoVID however the sector has shown tremendous growth in past few years. Because of this development and relentless dependence on technology. Further CoVID duration has also witnessed the increase of cyber-crimes on all sectors (Kashif et al, 2020) the threats to computer security along with integrated network of civil aviation remain a constant challenge. While computer security updates are in place the country's aviation systems need to be more secured and proactively chased for perfection using both technology and behavioral aspects. The study takes Protection Motivation theory as benchmark to study its applicability with respect to aviation Cyber Security behavior in Indian Civil Aviation sector. Following are the certain definitions used for reference:

(a) **Perception Management – the relevance:** People's behavior is influenced by their perceptual reality and not by actual reality and therefore the annoyance of cyber threats and their effects in various sectors facing it should be perceived accordingly.

(b) **Cyber Threats:** Cyber threats are the attacks on IoT in the domain of mobile, computing and web wherein any functional system can be jeopardized/compromised irrespective of physical presence of destroyer in the vicinity.

(c) **Cyber Security Behavior:** The constant secured conscious behavior among people to enhance the digital protection of data for secured and safe environment.

Cyber Attacks on the critical Infrastructure or any business cannot be predicted for its range and depth. The time taken to respond, mitigate and recover from the situation would estimate the losses. Thus, the criticality of Cyber-attack would determine its range and depth. In Aviation business, few of these may lead to-

- Shutting down Airport Terminal for few minutes to time taken to respond and recover.
- Delay in boarding, take-off.
- Delay in ticketing.
- Shutting down Runway lights.
- On flight emergency.
- Baggage/Cargo Management.
- Fraudulent booking.
- Fraudulent Credit/Debit card payments etc.
- Data theft

People around the world believe that aviation is one of the safest transportation systems in the world. Aviation is seen as a highly efficient, safe and powerful structure; However, people don't want it if they think their life is at risk.

Buildup Regular Cyber Standard practices for Aviation System uses of standard or common practice helps to provide relief against internal threats. For example, the application of basic cryptographic criteria for air communication and protocols may reduce the risk of hindering the future development of the structure. Global efforts are underway to address infrastructural data security. The aviation community must seek after the following work-plan in light of equipping against the cyber threats:

- Update the vision, strategy, objectives, and the typical cyber security framework to address emerging threats.
- Increase cooperation in dynamic support and cooperation among the air transport community of all-important players in this sector.

- The use, expansion and application industry are the best practice, feedback team and ongoing research and education efforts.
- Bringing suitable government institutions for discussion.
- Start creating a road map that differentiates short, medium and long-distance activities.

Any substantial framework attempting to integrate the government and private sector, would ideally intend to stimulate public discussion. Further, a framework for integrating public and private initiative in this regard addresses the following aspects: There is need to strengthen the inter-ministerial coordination and the following:

- Cyber Command must be structured to manage cyber nuisances.
- Use of Public-private partnerships (PPP) for information security and adherence to global standards is vital in today's scenario.
- Legislative measures must be enforced to address the evolving aspect of security in cyberspace.
- A proactive diplomatic policy can essentially facilitate national defense. Study of vulnerabilities as well as Potential competitors must accept to resist any form of intrusion or exploitation.

Comprehending the patterns of cyber warfare and its various dynamics is a sine qua'non. Various threat actors in different capacities poses a challenge to growth nevertheless these can be beaten by clearly defined objectives and national doctrines including law enforcement agencies supporting and restructuring cyber domain with respect to this critical Infrastructure. Section 4.2.3 of the National Cyber Security policy (NCSP) adheres to the very same attribute and very soon we have a latest NCSP in current year. Blockchain and Machine Learning systems are going to give positive impact on safer cyber secure practices in IoT and OT systems.

Cyber Security in India is being revived and shaping up to the requirement due to efforts by the governments and the industry. Nevertheless, the technologies on operational technology, Artificial Intelligence will be assisting to mitigate the nuisances of Cyber vulnerabilities. National policing and CISF too are gearing up on the occasion and strengthening of governing laws on subject shall further improve the threat scenario. No developed country has yet formalized any framework on Aviation Cyber Security however there exists multiple of them in various research papers and reports. There is a significant need to understand human psychology and integrate it into the operational technologies to prevent and address any future cyber threats. There remains a scope to address and make people talk on security issues; bring out the challenges on open domain and then collaborate to reach the solution. This study will help future researchers in including the cognitive domain into Aviation cyber security. This shall further assist the academicians and the industry to identify the costs of operations in sustaining the safe airport operations.

--------------------------------------Jai Hind---

Bibliography

1. Abraham, S. (2014), Hoover Institution, Stanford University Managing the Internet United States Security Hazard. Working Group on International Affairs and the Perfect Strategy. https://www.hoover.org/sites/2015/annualreport.pdf.
2. Accenture Ninth Annual cost of Cybercrime (2019). https://www.accenture.com/acnmedia/pdf96/accenture-2019-cost-of-cybercrime-studyfinal.pdf.
3. Air Transport Association of America (2007), Economic Report. www.aviation.org.
4. Air Transport Association of America (2004), Journal of Civil Aviation, Vol 3 No. 4, pp. 34-54.
5. Airlines International by IATA Security/ Global (2017), Cyber Crime Threat Demands Robust Defense.
6. Airports Council International, Boeing (2016), Airline strategies and business models. Aviation Systems: Management of the Integrated Aviation Value Chain. (pp.77-102).
7. Alessandro Pollini, Alessandra Tedeschi, Lorenzo Falciani (2014), Airports as Critical Transportation Infrastructures Increasingly Impacted by Cyber-attacks: A Case Study. Journal of Deep Blue Italy, Vol 7 No. 7, pp. 19-32.
8. Alan Kirschenbaum (2015), The social foundations of airport security, Journal of Air Transport Management, Elsevier 2015, Vol 48, pages 34-41.
9. Amar Infotech (2019). Global Airport and Aviation Industry Trends. https://www.amarinfotech.com/global-aviation-industry-trends.html
10. American Institute of Aeronautics and Astronautics (2013), Aerospace Leadership World Forum. Framework of Cyber Security. https://doi.org/10.2514/1.I010693.
11. Anderson, C. L., & Agarwal, R. (2010), Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security

Behavioral Intentions. Management Information System. (USA), Vol. 34 No.3, pp. 613 – 43.

12. Andrew Munro (2016), How Cyber (in) secure is air travel. https://globalriskinsights.com/2016/02/how-cyber-insecure-is-air-travel.

13. Annual Financial Report of Indigo Aviation of year (2018), https://www.goindigo.in/information/investor-relations.html.

14. Annual Report of Delhi Airport (2017). https://investor.gmrgroup.in /annualaccountsubsidiariesPDF/201819.

15. Arvind, R. (2015). CISF- Stands between Threat & Safety India today.

16. ATCA Aviation Cyber Security (2015), White Paper Executive Summary. Joining a Global Plan to Combat Emerging Information Security Threats. https://cybernautics.aero/images/pdf.

17. Aviation Perspectives Price Water Coopers (2016), Aviation Perspectives Special Report Series: Cybersecurity and the Airline Industry. Cyber Security and the Airline Industry Journal Vol I-IV No. 7, pp. 12-29.

18. Bada, K. and Sase, L. (2014), Cyber Security Awareness Campaigns Why do they fail to change behavior?' Global Cyber security Capacity Centre. Journal of Cyber Crime, Vol. 17 No. 8, pp. 237-256.

19. Baheti, R. and Gill, H. (2011), Cyber-physical systems. *The Impact of Control Technology, Vol. 34 No. 2, pp.* 161-166.

20. Benedikt et al (2013). IEEE Computer Society. https://www.acm.org /binaries/content/assets/education/cs2013_web_final.pdf. 1530-1605/12.

21. Bernard Lim (2014), Aviation Security - Emerging Threats from Cyber Security in Aviation– Challenges and Mitigations. Journal of Aviation Management, Vol. 10 No.6, pp. 45-67.

22. BEA (2016). France Aviation safety report.

23. Boer, H., & Seydel, E. R. (1996), Protection Motivation theory.

24. Boer, H., & Seydel, E. R. (1996), Protection Motivation Theory. In M. Conner, & P. Norman (Eds.), Predicting Health Behaviour: *Research and*

Practice with Social Cognition Models. Eds Mark Conner, Paul Norman (pp. 95-120).

25. Boer, H., and Seydel, E.R. (2001), Protection Motivation Theory. In M. Conner, & P. Norman (Eds.), Chapter 4Predicting Health Behaviour: Research and Practice with Social Cognition Models. Eds Mark Conner, Paul Norman (pp. 95-120*)*.

26. Brian, A, J. & Tom, L, F. (2018). Air Transportation Direct Share Analysis and Forecast https://doi.org/10.1155/2020/8924095.

27. Business Standard (2018), News of Delhi Airport.

28. Business today (2019), Aviation Industry. https://www.businesstoday.in /magazine/issue/june22019.

29. Case Study by Arctic Wolf Networks on Stevens Aviation, a premier US Aviation Services Company (2009). http://wpengine.netdna-cdn.com/wp-content/uploads/CS03-Stevens-Aviation.pdf. 226.

30. Center for the Protection of National Infrastructure CPNI (2012). https://www.cpni.gov.uk.

31. Centre for Strategy and Evaluation Services (2011), European Union Aviation Security and Detection Systems - Case Study. Journal of Cyber Security, Vol. 8 No.7 pp. 78-90.

32. Centre of Strategy and Evaluation Services (2011), United Kingdom Case Study on Aviation Security and Detection Systems, European Union. Ex-post Evaluation of PASR Activities in the field of Security https://ec.europa.eu/homeaffairs/sites/homeaffairs/files/elibrary/documents /policies/security/pdf/aviation_case_study__cses_en.pdf.

33. Chen, H., & Zahedi, F M. (2016), “Individuals’ Internet Security perceptions and Behaviours: Polycontextual contrasts between the United States and China. MIS Quartertly Vol. 40 No 1, pp.205-222.

34. Christian Beckner (2015), Centre for Cyber and Homeland Security, Risk based security and the aviation system: Operational objectives and policy

changes.https://www.yumpu.com/en/document/view/37026790/gw-cchs-risk-based-securityand-the-aviation-system-jan-20151.

35. Civil air navigation services organization (2014), Global Air Navigation Services Performance Report. https://www.canso.org/sites/default/files/GlobalANSPerformanceReport2014_0.pdf.

36. Civil Aviation and Cyber Security Dr. Daniel P. Johnson Honeywell Aerospace Advanced Technology (2013),

37. Comprehensive European Approach to the Protective of Civil Aviation. (2013), Recommendations on future research and Developments, https://cordis.europa.eu/project/id/261651

38. Costantino, F., Di Gravio, G., & Patriarca, R. (2016), Resilience engineering to assess risks for the air traffic management system: a new systemic method. International Journal of Reliability and Safety, Vol.10 No.4, pp. 112-134 https://doi.org/10.1504/ijrs.2016.10005344.

39. CRN Magazine (2015), The Total Global Cost of Cybercrime? $400 Billion A Year and CSCSS, Aviation and Hacking, August 14. http://cscss.org/CS1/index.

40. Cyber Global Security Awareness Campaigns (2010), Why do they fail to change behaviors International Conference on Cyber Security for Sustainable Society https://arxiv.org/abs/1901.02672.

41. Cyrille, R.(2015), Implementation of a European Centre for Cyber Security in Aviation. https://www.easa.europa.eu/newsroomandevents/news /implemen-tationeuropeancentrecybersecurity-aviation.

42. Daryle, W. Z & Duerwr, L. (1970), Determining Sample Size for Research Activities, University of Minnesota. Morgan Educational and Psychological Measurement, Vol. 30 No. 12, pp. 607-610.

43. David Mc.A Baker (2014), Tourism and Terrorism: Threats to Commercial Aviation and Security in Tourism. International Journal of Religious Tourism and Pilgrimage. Vol 2 No. 5 pp. 60-67.

44. Defence Technical Information Centre (2015), Department of Defense, United States GCN, Cyber risks inherent in Next Gen transition. *GAO Journal*, Vol.12 No. 5, pp. 34-56.

45. Director General of Civil Aviation, FRTP research (2017), Mumbai India, Indian Brand Equity Foundation Annual Safety Review-2016 Indian Civil Aviation. Indian Aviation Industry. https://www.ibef.org.

46. Dominic, N. (2016), Cyber Security-Tackling the Threat-The Airport Approach- ACI World Cybers Security task force. Journal Air Transport, Vol. 9 No. 2, pp. 78-99.

47. Daniel P. Johnson (2012), Civil Aviation and Cyber Security Honeywell Aerospace Advanced Technology.

48. Maria Bada & Professor Angela Sasse (2014), Global Cyber Security Capacity Centre: Draft Working Paper Cyber Security Awareness Campaigns Why do they fail to change behaviour. https://discovery.ucl.ac.uk/id/eprint /Awareness CampaignsDraft WorkingPaper.pdf.

49. Economic Effects of Cyber-Crime (2018), Center for Strategic and International Studies https://www.mcafee.com/enterprise/assets/reports /rp- /restricted economic-impact cybercrime.

50. Florent Frederix Online Trust and Cyber Security unit European Commission (2015), http://www.csap.cam.ac.uk/network/florent-frederix.

51. Fornell C, Larcker DF (1981), J. Mark. Discriminant Validity Assessment Res. 139-50.

52. Francis, J.J., O'Connor, D. & Curran, J. Theories of Behaviour Change Synthesized Into a set of Theoretical Groupings (2012), Introducing a Thematic Series on the Theoretical Domains Framework. Implementation Sci, Vol 17 No. 35 pp. 132-146. (2012). https://doi.org/10.1186/1748-5908-7-35.

53. Bisignani, G. (2006), State of the Air Transport Industry. Address to the Annual General Meeting International Air Transport Association, Vancouver, June 2006, www.iata.org.

54. Tsoukalas, G. (2007), Convergence in the US Aviation Industry: A Unit Cost and Productivity Analysis MIT Master's Thesis, Department of Aviation and Astronautics, August 2007.

55. Georgia, L. M. (2019), Sensors. https://www.mdpi.com/journal/sensors.

56. Georgia, L. (2019), Aviation Cybersecurity and Cyber-Resilience: Assessing Risk in Air Traffic Management: Theories, Methods, Tools and Technologies Critical Infrastructure Security and Resilience, Journal of Resilience of Values, Vol. 23 No. 4 pp.245-260.

57. Gil Mulin, Airbus Regan Brossad (2014), Guidance for Digital Security in Commercial Aviation-ATA Spec42.http://www.ataebiz.org//eBusinessForum/2014Antonio/8Guidance_for_Digital_Security_Brossard_Mullin.pdf.

58. Global Airlines Industry (2019), Analysis and Forecast 2010 – 2019. https://www.prnewswire.com/newsreleases/globalairlinesindustryanalysisandforecast/html.

59. Global Cyber Security Capacity Centre (2016), Draft Working Paper Cyber Security Awareness Campaigns Why do they fail to change behaviour. https://discovery.ucl.ac.uk/id/eprint/1468954/1/AwarenessCampaignsDraftWorkingPaper.pdf.

60. Government of India Ministry of Home Affairs from a Question Posed in Rajya Sabha (2015), Breaches of security at Indian airports. https://www.mha.gov.in/MHA1/Par2017/pdfs/par2015pdfs/rs-250215/213.pdf.

61. Haas, Jane W., Gerrold S. Bagley and Ronald W. Rogers (1975), Coping with the Energy Crisis: Effects of Fear Appeals Upon Attitudes Toward Energy Consumption. Journal of Applied Psychology, Vol. 60 No. 4 pp. 78-89. 230.

62. Hair, J.F., Hult, G.T.M., Ringle, C.M. and Sarstedt, M. (2014), A Primer on Partial Least squares Structural Equation Modeling (*PLS-SEM).* SAGE Publications, Inc., ISBN: 978-1- 4522-1744-4.

63. Hamid Salim (2014), Cyber Safety: A Systems Thinking and Systems Theory Approach to Managing Cyber Security Risk. http://web.mit.edu /smadnick/www/wp/2014-07.pdf.

64. Hamid Salim (2014), Cyber Safety: A systems thinking and Systems Theory approach to Managing Cyber Security Risk. Composite Information Systems Laboratory (CISL) Sloan School of Management, Room E62-422 Massachusetts Institute of Technology Cambridge, MA 02142.http://web.mit.edu /smadnick/www/wp/2014-07.pdf.

65. Hans de Brujin, MarijinJannsen (2017), Building Cybersecurity Awareness: The need for evidence-based framing strategies. Government Information Quarterly: An International. Journal of Information Technology Management Policies and Practices, Vol 34 No.1 pp. 23-45. https://doi.org/10.1016/j.giq.2017.02.007.

66. Henseler, J. Christian M. Ringle , Rudolf R. Sinkovics (2009).The Use of Partial Least Squares Path Modeling in International Marketing.

67. Herath, T., & Rao, H. R. (2009), Protection Motivation and Deterrence: A framework for security policy compliance in organisations. European Journal of Information Systems, Vol.18 No.2 pp. 106–125 doi:10.1057/ejis.2009.6

68. Hsin-Yi, Sandy Tsai (2016), Online Safety Behavior, Understanding Online Safety Behaviours: A PMT perspective Taiwan, *USA* Computers and Security 59 Elsevier.

69. Tsai. S., H., Mengtian Jiang (2016), Understanding Online safety behaviors: A Protection Motivation Theory. Science Direct Computers & Security, Vol. 59 No. 7 pp. 89-102. I: 10.1016/j.cose.2016.02.009.

70. IATA (2016), Closer Collaboration with Governments to Tackle Threat of Terrorism https://www.iata.org/en/pressroom/pr/2016-06-02-04/ 231.

71. ICAO, Working Paper (2018), 13th Air Navigation Conference, Montreal https://www.icao.int/Meetings/anconf13/Documents/WP/wp_311_gen_en.pdf.

72. IQPC Cyber Security and System Safety in the Aviation Industry http://www.jadecreative.com/media/19058.

73. Ifinedo, P. (2012), Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory. In Computers and Security (Vol. 31, pp. 83–95). https://doi.org/10.1016/j.cose.2011.10.007.

74. Indian Brand Equity Foundation ibef.org/about-us.aspx.

75. Industry High-Level Group IHLG (2017), Aviation Benefits 2017 Report.

76. International Air Transport Association IATA (2015), Fact Sheet: World Industry Statistics www.iata.org.

77. International Federation of Airline Pilot Associations (2013), Paper on Cyber Threats as expected by Pilots, World Body for Airline https://www Pilots. ifalpa.org/publications/library/cyberthreats1665.

78. Heimlich, J. (2007), Outlook: Reaching for the Skies? Air Transport Association of America www.Aviation.org.

79. Jaatun, M & Koelle, R (2016), Cyber Security Incident Management in the Aviation Domain. 510-516. 10.1109/ARES.2016.41.

80. Jaatun, M., and Koelle, R. (2016), Cyber Security Incident Management in the Aviation Domain',11th International Conference on Availability. Reliability and Security, Vol. 12 No. 9 pp. 23-47. pp. 510-516.

81. Jeff Schmidt, CEO, JAS Global Advisors (2015), Managing Cyber-Risk in the Aviation Industry https://www.complianceweek.com/managing-cyber-risk-in-the-aviation-industry/3222.

82. Jenkins, Brian M, (2012), Aviation Security: After Four Decades, It's Time for a Fundamental Review. https://www.complianceweek.com/managing-cyber-risk-in-the-aviation industry/3222.article

83. Jill J Francis, Denise O’Connor and Janet Curran (2012), Theories of Behavior Change Synthesized into a Set of Theoretical Groupings, Aberdeen University UK.

84. Johnston, Allen & Warkentin, Merrill. (2010), Fear Appeals and Information Security Behaviors: An Empirical Study. MIS Quarterly. Vol. 34 No. 9 pp. 98-123. 10.2307/25750691.

85. Juan Lopez Jr. MS & Deanne W. Otto (2016), Analysis of Cybersecurity Content in the Air Traffic Collegiate Training Initiative (AT-CTI) Program. International Journal of Technology Humanities and Human Security, Vol 12 No. 6.

86. Kantola, S.J. Nesdale, A. R. & Geoffrey J. Syme (2006), The Effects of Appraised Severity and Efficacy in Promoting Water Conservation: An Informational Analysis. Journal of Applied Social Psychology, Vol. 13 No. 2, pp. 164-182.

87. Kasthuriangan Gopalakrishnan, Manimaran Govindarasu, Doug W. Jacobson, Brent M.Phares (2013), Cyber Protection for Airports United States International Journal of Traffic and Transport.

88. L. Ren, H. Liao, M. Castillo-Effen, B. Beckmann, T. Citriniti (2017), Transformation of MissionCritical Applications in Aviation to Cyber-Physical Systems n book: Cyber-Physical Systems, pp.339-362.

89. Lee, K. (2008), Cyber Physical Systems: Design Challenges. E: IEEE Explore ·Conference: Object Oriented Real-Time Distributed Computing (ISORC).

90. Liang, H., & Xue, Y. (2009), Avoidance of Information Technology Threats: A Theoretical Perspective. Management Information Systems Quarterly, Vol 33 No. 1, pp. 71–90. http://aisel.aisnet.org/cgi/view

91. Liang, H., &Xue, Y. (2010), Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. Journal of the Association of Information Systems, Vol. 11 No. 7, pp. 394–413. http://www.scopus.com/inward/record.url

92. Liang, L and Xue, K. (2010), Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. Journal of the Association for Information Systems Vol. 11 No. 7, pp. 394-413 .234

93. 94. Lim, B., (2014). Emerging Threats from Cyber Security in Aviation-challenges and Mitigations Journal of Aviation Management, pp. 83-95.

94. Loui, R., & Hope, (2017), 'Information Warfare amplified by cyber warfare and Hacking the National Knowledge Infrastructure' IEEE proceedings, pp 280-283.

95. Lim. B., (2014), Aviation Security - Emerging Threats from Cyber Security in Aviation Challenges and Mitigations, Journal of Aviation Management, Vol.12 No.4, pp.90-121.

96. Lippke, Sonia & Plotnikoff, Ronald. (2009), The Protection Motivation Theory within the stages of the Trans theoretical Model - Stage-specific interplay of variables and prediction of stage transitions. British journal of health psychology. Vol. 14 No. 4, pp. 211-29. https://doi.org/10.1348/135910708X399906.

97. Ludek Lucas (2016), Department of Security Engineering, Czech Republic. Secure ware The Tenth International Conference on Emerging Security Information, Systems and Technologies, pp. 146-165.

98. Lykou, Georgia & Iakovakis, George &Gritzalis, Dimitris. (2019), Aviation Cybersecurity and Cyber-Resilience: Assessing Risk in Air Traffic Management: Theories, Methods, Tools and Technologies. https://doi.org 10.1007/978-3-030-00024.

99. Marco Gericke (2012), Understanding Cyber Crime: Phenomenon Challenges and Legal response. ITU Report https://pdfs.semanticscholar.org/.

100. Maria Bada & Professor Angela Sass (2015), Global Cyber Security Capacity Centre Cyber Global Security Awareness Campaigns: Why do they Fail to Change Behaviors, International Conference on Cyber Security for Sustainable Society.

https://arxiv.org/abs/1901.02672.

101. Martin et al NATO (2016), https://www.nato.int/cps/en/natohq/79511 MDPI Journal, Vol. 12 No. 9, pp. 123-145.

102. Maryruth belsey Priebe International Quality and Productivity Centre, Berlin Germany (2015), McCarthy, C., Harnett, K., & Carter, A. (2014, October). A summary of cyber security best practices. (Report No. DOT HS 812 075). Washington, DC: National Highway Traffic Safety Administration.

103. McCarthy, C., Harnett, K., & Carter, A., (2014), A Summary of Cyber Security Best Practices (Report No. DOT HS 812 075). Washington, DC: National Highway Traffic Safety Administration.

104. Michael L. Papay Frank J. Cilluffo Sharon L. Cardash (2014), Growing the Cyber Bar Security and Acquisition, Cyber Security Initiative, Northrop Grumman. https://www.gigamon.com/content/dam/resourcelibrary/english/analystindustryreport/tagcybersecurity-annual-cyber-security-handbook-and-reference-guide-vol-3. pdf.

105. Mike Pierides, Brian E. Finch, Rafi Azim-Khan and Steven P. (2015), Farmer Cyber Security task force, Pillsbury Winthrop Shaw Pittman LLP. Cyber Security and the Aviation Sector: Recent Incidents Highlight Unique Risks. https://www.pillsburylaw.com/images/content/1/1/v2/1196/AlertAug2015 GlobalSourcing /Cyber security and The Aviation Sector.pdf.

106. Monica Whitty, James Doodson, Sadie Creese, and Duncan Hodges (2015), Cyber Psychology Behavior & Social Networking Mary Ann Liebert, Inc. Individual Differences in Cyber Security Behaviors: An Examination of Who is Sharing Passwords. Cyberpsychology, Behavior, 236 and Social Networking, Volume 18 No 1, pp.31-72.doi: 10.1089/cyber.2014.0179.

107. Mrabet, Z. E., Kaabouch, N., Ghazi, H. E., & Ghazi, H. E. (2018), Cyber-security in Smart grid: Survey and Challenges. Computers & Electrical

Engineering, Vol.67 No. 7, pp. 469–482. Available at https://doi.org/10.1016/j.compeleceng.2018.01.015.

108. Muhammed Abdul (2016), The Disappearance of MH 370: and Search Operations – The Role of Technology and Emerging Research Challenges. IEEE Aerospace and Electronic Systems Magazine, Vol.31, No. 3, pp. 67-89. 10.1109/MAES.2016.150065.

109. Murali Patibandla (2005), Foreign Investment and Productivity: A Study of Post-Reform Indian Industry. Review of Applied Economics.

110. National Critical Information Infrastructure Protection Centre (2017), India Newsletter https://nciipc.gov.in/documents/NCIIPC_Newsletter_Apr17.pdf.

111. National Strategy for Aviation Security (2018).https://www.whitehouse .gov/wpcontent/uploads/2019/02/NSAS-Signed.pdf.

112. Nigel (2014) Book/Novel by Nigel Cawthorne, 2014.

113. Rebecca C. Leng. Federal Aviation Regulations Administration (2009), Department of Transportation of the United States Global Threat Intelligence Report https://gcn.com/Articles/2009/05/06/Air-traffic-control-vulnerabilities.

114. Olivier Delain, Olivier Ruhlmann and Eric Vautier (Groupe ADP) Matt Shreeve and Piotr Sirko Veronika Prozserin (2016), This study was undertaken within the context of SESAR Project 06.03.011 and led by SESAR member, Eurocontrol, in collaboration with Helios, Groupe ADP and Professor Chris Johnson from the University of Glasgow.

115. PA Consulting (2018), UK Overcome the Silent Threat: Building Cyber Resilience in Airports, 2018.http://www2.paconsulting.com.

116. Parida, Purna Chandra, et al., (2012), Economic impact study of Delhi Airport, National Council of Applied Economic Research, M/s. Cirrus Graphics. page 53-54.

117. Pfleeger, Shari., & Caputo., DD., (2012), Leveraging Behavioral Science to Mitigate Cyber Security Risk. Elsevier Computers and Security, Vol.31 No.12, pp., 597.

118. Philip Menard, Gregory J.Bott & Robert E. Crossler,(2018), Cyber Security Information System. Journal of Management Information Systems. Vol 34 No. 4, pp. 1203-1230.

119. Pierides, M. Brian E. Finch, Rafi Azim-Khan and Steven P. Farmer (2015), Cybersecurity and the Aviation Sector: Recent Incidents Highlight Unique Risks. Cybersecurity Task Force, 1-4.

120. Posey, C, Tom L Roberts, and Paul Benjamin Lowry (2015), The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets. Journal of Management Information Systems, Vol. 32 No. 4, pp.179-214.

121. Posey, C., Roberts, T., Lowry, P. B., Courtney, J., & Bennett, R. J. (2011), Motivating the Insider to Protect Organizational Information Assets: Evidence from Protection Motivation Theory and Rival Explanations. In Proceedings of the Dewald Roode Workshop in Information Systems Security 2011, pp.1–51. Blacksburg, Virginia, September 22-23.

122. Practical Aviation Security Book on Aviation Protecting Critical Infrastructure &Role of Government (2010).

123. Rafal Le Szczyna (2013). Cost Assessment of Computer Security Activities Computer Fraud & Security.

124. Rafique, S., Humayun, M., Gul, Z., Abbas, A., & Javed, H. (2015), Systematic Review of Web Application Security Vulnerabilities Detection Methods. Journal of Computer and Communications, Vol. 3 (09), 28–40 https://doi.org/10.4236/jcc.2015.39004.

125. Randall J Murphy's, Michael, Michael Sukkarieh I & Jon Haas' Paul Hriljac's. The FAA Sponsored Airport Cyber Security Best Practices Guide (2015), The Year 2015 Airport Community Research Programme. Journal of Community, Vol. 23 No. 9, pp.234-245.

126. Randall J. Murphy Michael Sukkarieh Jon Haass Paul Hriljac (2015), Guidebook on Best Practices for Airport Cybersecurity Airport cooperative research program (ACRP) 140.

127. Report of Accenture of (2019), On the costs of cyber-crime https:/www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime Study.

128. Revelle, W. (2017), psych: Procedures for Personality and Psychological Research. Northwestern University, Evanston. http:/cran.r-project.org/web/ packages/psych/. R package version 1.6.4.

129. Ringle, C.M., Wende, S. and Will, A. (2005), "Smart PLS 2.0.M3", Hamburg: Smart PLS. http://www.smartpls.com.

130. Robert W. Poole Jr, The reason Foundation USA (2015), Fresh Thinking on Aviation Security, Journal of ATM. International Summer School of Aviation Psychologist.

131. Rogers, R. W. (1975), A Protection Motivation Theory of Fear Appeals and Attitude Change. The Journal of Psychology, Vol 91 No.1, pp 93–114.

132. Rogers, R. W. (1983), Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change. Journal of Experimental Social Psychology, Vol 19 No. 5, pp. 469-479.

133. Ronald W Rogers (2010), University of South California A Protection Motivation Theory of Fear Appeals and Attitude Change 1975 The Journal of Psychology published in 2010. https://doi.org/10.1080/00223980.1975.9915803.

134. Ruwantissa, I.R. Abeyratne (2004), Aviation in Crisis, IJDA Journal, Cybersecurity Threat to Aircraft Is Being Addressed by FAA.

135. Ruwantissa, A. (2011), Cyber-Terrorism and Aviation-National and International Reactions. Journal of Transportation Security. Vol 4 No.4, pp.337-349.

136. Safa, N. A, Rossouw Von Solms A., Steven Furnell (2015), Information Security Policy Compliance Model in Organizations. Computers & Security, Vol 56 No. 9, pp.1–13.

137. Sampigethaya, K., & Shetty, S., (2011), Future E-Enabled Aircraft Communications and Security: The Next 20 Years and Beyond' IEEE proceedings, Vol 99, No 11, pp. 2040-2054.

138. Sampigethaya. K., Poovendran. R., L. Bushnell., (2008), Secure Operation, Control and Maintenance of Future E-enabled Airplanes. Network Security Lab (NSL). EE Department. University of Washington Seattle.

139. Sanislav, Teodora &Miclea, Liviu. (2012), Cyber-Physical Systems - Concept, Challenges and Research Areas. Control Engineering and Applied Informatics. Vol.14 No. 3, pp. 28-33. 240

140. Satish, A.P., & Xu, B. (2017), Vulnerability Assessment for security in Aviation Cyber-Physical Systems' IEEE 4th International conference on cyber security and cloud computing, PP., 145-150.

141. Schmitt, A.R., Edinger, C., Mayer, Simulation-supported Aviation Cyber-Security Risk Analysis: A Case Study (2019), CEAS Aeronaut Journal, Vol 10 No. 4, pp. 517–530 (2019). https://doi.org/10.1007/s132720180331-2.

142. Stefan Frei (2015). Cyber threats in aviation any lessons from other industries experience with cyber? Swiss Federal Institute of technology, Zurich

143. Secure Skies (2020), European Cockpit Association (ECA), Belgium. https://www.eurocockpit.be/about-us.

144. Shari, Deanna (2011). Leveraging Behavioural Science to Mitigate Cyber Security Risk in Computers and Security, Elsevier, Dec 2011.

145. Siponen, M., Adam Mahmood., & M. Adam Mahmood (2010). Compliance with Information Security Policies: An Empirical Investigation. Computer Journal, Vol 43 No.2, pp. 64 – 71. Mar 2010. https://doi.org DOI: 10.1109/MC.2010.35.

146. Sjoberg, L., Moen, B. and Rundmo, T. (2004), Explaining Risk Perception. An Evaluation of the Psychometric Paradigm in Risk Perception Research. Norwegian University of Science and Technology.

147. Stefan, S. (2018), Computing Community Consortium. https://www. cccblog.org/2018/01.

148. Strohmeier, Martin & Schäfer, Matthias & Lenders, Vincent & Martinovic, Ivan. (2014). Realities and challenges of nextgen air traffic management: The case of ADS-B. IEEE Communications Magazine. Vol. 52 No. 12, pp. 111-118. https://doi.org 10.1109.

149. Sztipanovits, (2007), Composition of Cyber-Physical Systems. Control Engineering and Applied Informatics, Vol. 14 No.2, pp. 28-33 ·

150. Tan Y. Steve Goddard, Lance C. Perez., (2008), A Prototype Architecture for Cyber-Physical Systems.

151. Teodora Sanislav, Liviu Miclea (2008), Cyber-Physical Systems - Concept, Challenges and Research Areas. Control Engineering and Applied Informatics. Vol. 23 No.8, pp.25-32.

152. The Boeing Company (2013), Developing a framework to improve cyber security critical infrastructure. https://www.nist.gov/system/files/documents /2017/06/01/040513_cgi.pdf.

153. The international federation of Air Line Pilots Associations (IFALPA) (2013), The Global Voice of Pilot's Threats: Who Controls Your Aircrafts?

154. The Worlds Forum for Aerospace Leadership (2013),

155. Thongchai Jeeradist, Natcha Thawesaengs, kulthai, T., Sangsuwan (2016). Using TRIZ to enhance passengers' perceptions of an airline's image through service quality and safety. Journal of Air Transport Management Vol. 53, Vol.16, No. 6, pp.131-139.

156. Timothy B. Holt, Prescott, holtt, Daytona Beach, Linda Weil, Sonya Mc Mulle (2016), Aircraft Cyber Security and Information Exchange Safety Analysis for Department of Commerce Embry Riddle Aviation university upward trajectory continue.

157. Tsai, H., Jiang, M., (2016), Understanding Online Safety behaviours: A protection Motivation theory perspective', Journal Elsevier, Computers and security 59(138-150).

158. Tsai, H., Jiang, M., et al, (2016) 'Understanding online safety behaviours: A protection Motivation theory perspective', Journal Elsevier, Computers and Security, Vol. 59 No. 23 pp.138-150. 242

159. United States Government Accountability Office Air Traffic Control Association, (2015). FAA Needs a More Comprehensive Approach to Address Cybersecurity (2013). As Agency Transitions to NextGen. https://www.gao.gov/assets/670/668169.pdf.

160. US Department of Transportation Bureau of Transportation Statistics (2017), Form 41 Aviation Traffic and Financial Reports.

161. Valero (2016), Hackers bombard aviation sector with over 1000 attacks per month. Euractiv.com, Von Solms & Warren, 2011.

162. Vance, A., Mikko S., & Seppo, P. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. Journal of Information and Management, Elseiver, Vol 49, Issue 3-4, page 190-198.

163. Vikram K. & Edward W. Powers (2014), Please Fasten Your Seat Belts: Managing digital risk to support aviation innovation https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/consumerbusiness/aviationcyberrisk-report-04222015.pdf.

164. West, K. and Parmar. L. (2006), A Software architecture for next-generation cyber-physical system**.** Control Engineering and Applied Informatics, Vol 14 No. 2, pp. 28-33.

165. West, Richard & Parmer, Gabriel. (2006), A software architecture for next-generation cyber physical systems.

166. Wolf, F. M. & Hgais, J. (1986), Meta-Analysis: Quantitative Methods for Research Synthesis. Beverly Hills, CA, Sage Publications.

167. Wong et al., (2016). https://www.sciencedirect.com/science /article/ pii/ S016503271630430X.

168. Yan Chen & Fatemeh Mariam Zahedi (2012). Individuals Internet security perceptions and Behaviours Polycontextual Contrasts between US and the China: MIS Quarterly, Vol. 40 No.1 pp.205-222 · 10.25300/MISQ/2016/40.1.09. 243

169. Yeah, Jon Haass, Radhakrishna Sampigethaia, Vincent Capezzuto's (2016), Aviation and cybersecurity: opportunities Applied Analysis, National Academy of Sciences, Washington D.C USA. TR News, (304). https://commons .erau.edu/publication/299.

170. Yin, X. C., Liu, Z. G., Nkenyereye, L., & Ndibanje, B. (2019), Toward an Applied Cyber Security Solution in IoT-Based Smart Grids: An Intrusion Detection System Approach.*Sensors*,*19*(22) 4952.https://doi.org/10.3390s192249 52.

171. Yoann Viaouet (2017), Aerospace and Security Research, Association of Europe, Position Paper of the ASD Civil Aviation Cyber Security Task Force https://www.asdeurope.org/positionpaperof-the-asd-civil-aviation-cybersecurity-task-force.

172. ZDNet (2019). Data breaches to cost global economy $2 trillion by 2019.https://www.zdnet.com/article/data-breaches-to-cost-2-trillion-by-2019.

173. Nordfjærn, T., & Rundmo, T. (2015). Personality, risk cognitions and motivation related to demand of risk mitigation in transport among Norwegians. *Safety Science*, *73,* 15–22. https://doi.org/10.1016/j.ssci.2014.11.008.

174. Scott, N. (2015). Cyber Crime: 10 Things Every Leader Should Know. Director, 69(2), 68–72. http://search.ebscohost.com.

Appx 'A'

(Refer Para to 1.2 Page No 3)

THE AVERAGE ANNUAL COSTING OF CYBERCRIMES BY INDUSTRY

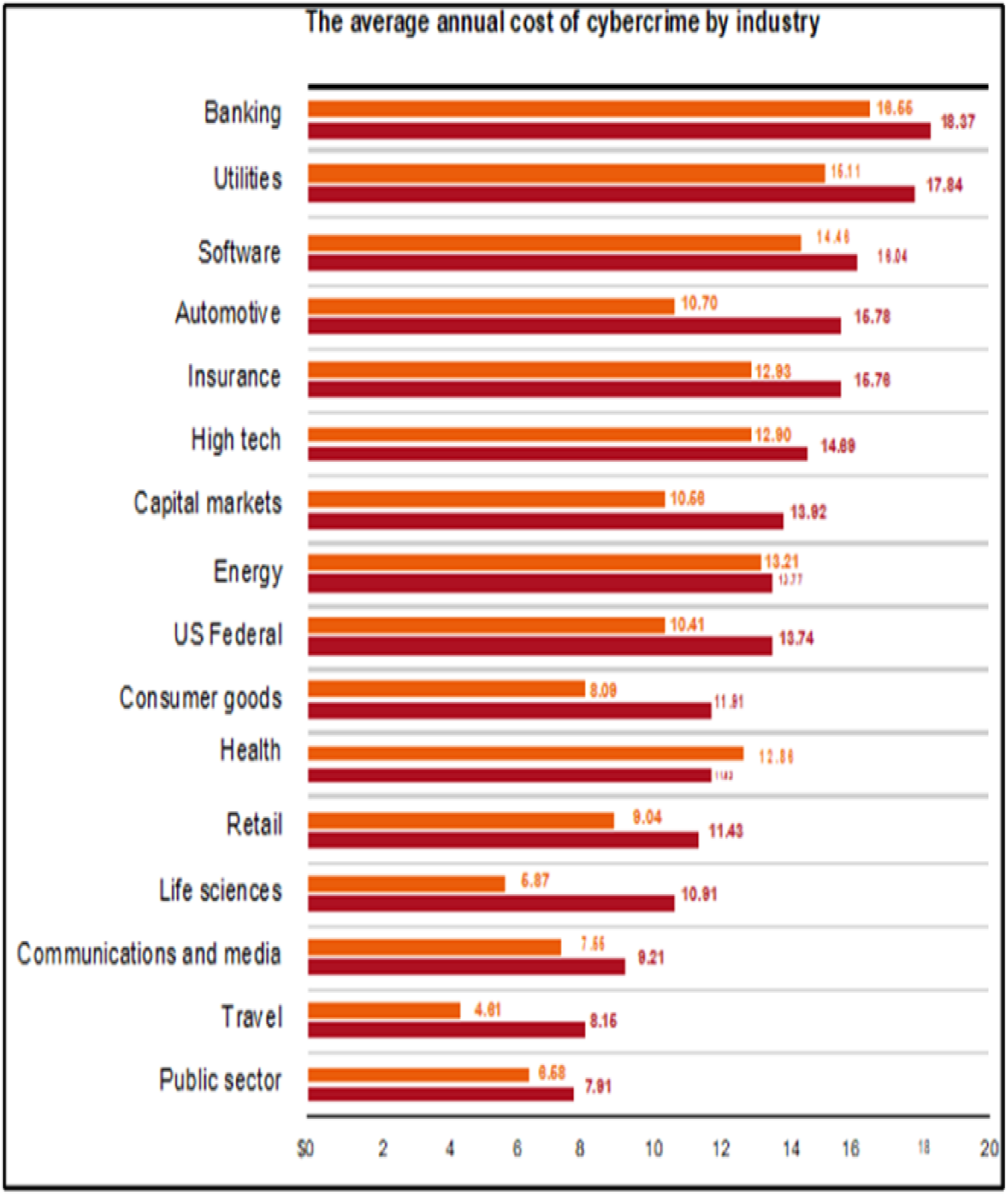
Cybercrime by Industries	**Average Annual Cost in 2017**	**Average Annual Cost in 2018**
	(US$ Millions)	**(US$ Millions)**
Automotive	10.7	16.78
Banking	18.66	18.37
Capital market	10.58	13.92
Consumer good	8.09	11.81
Energy	13.21	12.37
Health	12.88	12.88
High Tech	12.9	14.69
Insurance	12.93	16.78
Life science	6.87	10.91
Retail	9.04	11.43
Software	14.48	18.04
US federal	10.41	13.74
Utility	16.11	17.84
Communication and media	7.66	9.21
*Travel	4.81	8.16
Public sector	6.68	7.91

(Source: Accenture Report on Cyber Crimes 2019)

Appx 'A' contd…

(Refer Para to 1.2 Page No 3)

AVERAGE ANNUAL COST OF CYBERCRIME BY INDUSTRY

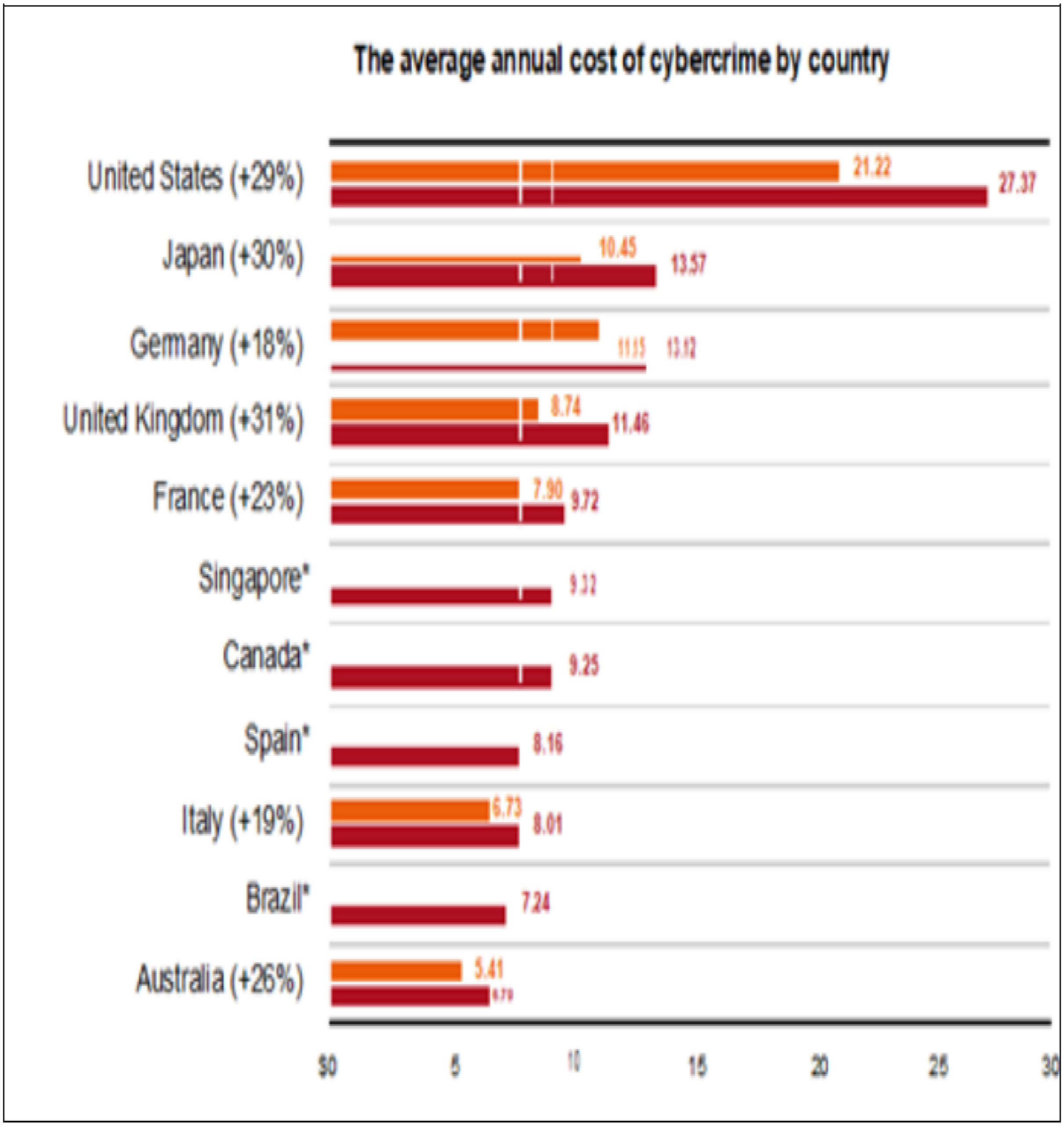


(Source: Accenture report on cyber-crime 2019)

Appx 'A' contd…

(Refer Para to 1.2 Page No 3)

AVERAGE ANNUAL COST OF CYBERCRIME BY COUNTRY



(Source: Accenture report on cyber-crime 2019)

Appx 'A' contd…..

(Refer Para to 1.2 Page No 3)

THE AVERAGE ANNUAL COST OF CYBERCRIME BY COUNTRY

Cybercrime by Industries	Average Annual Cost in 2017 (US$ Millions)	Average Annual Cost in 2018 (US$ Millions)
United States (+29%)	21.22	27.37
Japan (+30%)	10.45	13.57
Germany (+18%)	11.15	13.12
United Kingdom	8.75	11.47
(+13%)	7.91	9.73
France (+23%)	-	9.33
Singapore*	-	9.24
Canada*	-	8.15
Spain*	6.74	8.00
Italy (+19%)	-	7.25
Brazil* Australia (+25%)	5.42	6.78

(Source: Accenture Report 2019)

Appx 'B'

(Refer Para to 1.5.1 Page No 11)

PAST STUDIES ON THEORY OF PMT

Authors and Year of publication	**PMT variables**	**Country/ Area of the study**	**Subject area on which PMT was used. (Health, Addiction, security etc.)**	**Results (relationship Observed between variables)**
Maria Bada, Angela Sasse, Jul 2014	Vulnerability	UK for Global Cyber security Capacity Centre. United Kingdom Australia, Canada and Africa	Cyber Security Education Campaigns: Why do not you adjust. your conduct?	PMT: originally Develops to explains the impacts of fear. Invocation on health behavior and attitudes. Centered on cognitive process.
Bandura ,1977	Self-efficiency		Theory of Self-efficiency	Adopting mental Protective fitness relies in different variables.

Authors and Year of publication	PMT variables	Country/ Area of the study	Subject area on which PMT was used. (Health, Addiction, security etc.)	Results (relationship Observed between variables)
Yan Chen, Fatemah Mariam Zahedi, Mar 2016	Assessment of the hazard (Personal susceptibility and perceived severity of the situation) Coping evaluation (perceived efficacy of response and perceived. self-efficacy)	Quarterly Error, Analysis notes United States of America & China's	Web safety Perceptions and Behaviours for Individuals: Poly contextual Contrasts between the US and China	Findings followed the conceptualized model, suggesting substantial moderating country power and widespread impacts of discrepancies. between persons. Further recommendations: How espoused culture; societal and individual factor interplay shapes perceptions of online security and behaviours dynamic interest of coping behaviours at time on threat evaluation and coping appraisals at time t+1 and onward.

Appx B contd..

(Refer Para to 1.5.1 Page No 11)

Authors and Year of publication	**PMT variables**	**Country/ Area of the study**	**Subject area on which PMT was used. (Health, Addiction, Security etc.)**	**Results (relationship Observed between variables)**
Hsin-Yi Sandy Tsai et al., 2016	Security intentions, Coping appraisals, habit strengths, response efficacy, personal responsibility	Understanding Online safety behaviours:A PMT perspective	Online Safety behaviour	For threat assessment, it is the severity of online threats that predict security threats. Response efficacy and personal responsibility are also the significant predictors. Threat frequency, self-efficacy dealing with, and perceived protection was negative predictors toward PMT.

Authors and Year of publication	PMT variables	Country/ Area of the study	Subject area on which PMT was used. (Health, Addiction, Security etc.)	Results (relationship Observed between variables)
Van der Velde and Van der Pligt ,1991	LISREL's path-analysis techniques were used to evaluate the goodness of fit of the structural equation models.	To examine Rogers' PMT and aspects of Janis and Mann's conflict theory in the context of AIDS-related health behaviour. Subjects were 84 heterosexual men and women and 147 homosexual men with multiple sexual partners.	AIDS related behaviour; predictive value of the components of PMT	It was concluded that although protection motivation theory did fit the data adequately, expanding the theory with other variables-especially those related to previous behaviour-could improve our understanding of AIDS-related health behaviour.

(Refer Para to 1.5.1 Page No 11)

Authors and Year of publication	**PMT variables**	**Country/ Area of the study**	**Subject area on which PMT was used. (Health, Addiction, security etc.)**	**Results (relationship Observed between variables)**
Hass et al.,1975	Coping Fear appeal	Washington/ Experiment. Journal of Applied Psychology	Persuading consumers to use less energy	Although, increase improved perceived noxiousness or seriousness of the oil crisis strengthened efforts to reduce oil in the expected possibility of electricity scarcity.
Wolf et al.,1986	Perceived Severity, Perceived Efficacy, Perceived Capability	Washington/ Experiment. Journal of Applied Psychology	Prevention of nuclear war	Effect on viewers. An experiment was carried out for fear arousal cognition predict behavioral intentions on consequences of Nuclear War

Authors and Year of publication	PMT variables	Country/ Area of the study	Subject area on which PMT was used. (Health, Addiction, Security etc.)	Results (relationship Observed between variables)
Maddux et al., 1986	Expectancy Self efficacy earnings expectations price for outcome Outcome expectancy Outcome value	Washington/ Journal of Personality and Social Psychology	Increasing asserting behavior in assertive communication	Used a persuasive communication paradigm to examine the relative contributions of assessment. Were all significant and roughly equivalent predictors of behavioral intentions.
Chapter 4 on PMT by Henk Boer Erwin R Seydel	Covers detailed analysis and background of PMT			

Appx 'C'

(Refer Para to 4.5 Page No 72)

The History of Cyber-Attacks into the Aviation Industry

Year	Sector	Occurrences	Cost	Source
2002	U.S. Federal Aviation Administration	Hackers were able to infiltrate the Federal Aviation Administration system		https://fortune.com/2015/06/29/faa-Aviation-planes-hacked
2008		Western Pacific	Hackers later steal FAA company manager password in its western Pacific region	
2008	Western Pacific Region	Alaska	Hackers have the ability to retrieve more than 40,000 FAA user IDs, passwords and other information used to control a portion of the FAA Mission Support Network.	

Year	Sector	Occurrences	Cost	Source
2013		Miami International Airport (MIA)	About 20,000 hack trials were conducted every day to protect themselves from Cyber-attacks.	
2011		Los Angeles World Airports" (LAX, ONT, VNY, and PMD)	More than 60,000 cases of cyber abuse Have been closed. Lax has also encountered several malware-related cyber incidents that targeted a network baggage system.	
11Jun	DIAL	Delhi Airport system, CUPPS for issues of boarding gates, flight announcing system was down for 12 hours, CBI investigations revealed that it was a virus attack.	50 Flights were delayed by 20-25 minutes, 60 Lakhs	

Appx ‘C’ contd

(Refer Para to 4.5 Page No 72)

Year	Sector	Occurrences	Cost	Source
2013	Dubai International Airport (DXB)	Hackers from Portugal Cyber Army and Hi-Tech Brazil Hack Team	Had 50 email addresses and associated passwords stolen	
2013	Miami International Airport(MIA)	Cyber-attacks hacked; system weakened	Hackers attack nearly 20,000 hack trials per day before investing in training.	
2014	Airports Authority of India			Vijay (2014), The Asian Age
May15	United Airlines	United Aviation's Computer system is believed to be Linked to the Chinese government	The breach caused a computer error that grounded all of its aircraft for almost two hours	

Year	Sector	Occurrences	Cost	Source
Oct 15	07 Countries 252 Companies	The annualized Cost to detect, Respond to, and Mitigate a breach globally Was around global IT breach	$7.7 million (1.9% Increase)	
May 17	50 nations, 2 lakh computers	Wannacry ransomware	$4 billion	Money Watch, 16 May 2017
Jun 17	All Sectors	2014:44,679 (incidents) 2015: 49,455 2016: 50,362 27000 Cyber Security threat Incidents till Jun 17		Cert-In
2017	Israeli Airport	Cyber-attacks, 3 million		https://cyberprism.com/cyber-threats-to-the-viation-industry/

Appx 'C' contd

(Refer Para to 4.5 Page No 72)

Year	Sector	Occurrences	Cost	Source
Mar 18	Atlanta International Airport	Close Wi-Fi network Personal and financial details of 380,000 passengers have been stolen		
Aug 18	Air Canada	Private Information in the app was stolen	By its 1.7 million app users. Delta sys customer data was stolen earlier this year after a security flaw at one of its third-party customer support service vendors	https://techcrunch.com/2018/0/8/29/air-canada-confirms-mobile-app-data-breach/
Sep 18	British airways	Data Breach putting thousands of data at risk	3800,000 passengers stole Personal and financial details, names, credit cards and details of CVV's hackers.	

Year	Sector	Occurrences	Cost	Source
Oct 18	Cathay Pacific	Hong Kong	Airways for failing to Protect customers' personal data, 000 500,000. The ICAO says that Cathy was aware of the Pacific issue when she was attacked by a "brute force" passwords in March 2018.	
Apr 19	India (Kolkata to Delhi areas)	Technical glitch and server crash	155 flights delayed	

Appx 'C' contd

(Refer Para to 4.5 Page No 72)

Year	Sector	Occurrences	Cost	Source
May 19	Kolkata airport	4000 flyer stranded as cyber attacks	30 flights delayed	https://www.cybersecurity-insiders.com/ransomware-attack-on-cleveland-hopkins-international - airport/
Aug 19	Heathrow Airport	Phishing scam targeting hundreds of thousands of Aviation customers Queen's travel routes, up to 50 Heathrow"	£120,000	

Appx 'D'

QUESTIONAIRE

A. THREAT SEVERITY

Airline travel are leisure and business travel. However, accidents in aviation industry are fatal or near fatal. In this electronic age, how secure one is, while flying? Do we realise as passengers, the nuisances of cyber security while passing from one Airport to another? Further, there are chances your mobile being used by others to create disruptions or damage to network. The following are some of the threats to your online safety that malware can cause. Please rate how harmful they would be if they happened to you by clicking an answer in each row.

1. Do you feel Airports too are vulnerable for cyber threats?

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

2. Using free Wi-Fi at airport makes my computer/mobile/I-pad run more slowly.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

3. There is a possibility that your personal mobile being used by others to cause disruptions.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

4. You feel highly comfortable using free Wi-Fi / Hotspots at Delhi Airport compared to other Airports.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

5. Do you feel higher awareness among passengers can make one safer in rendering Cyber Security at Airports?

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

6. Using free Wi-Fi at Airports can compromise your personal identity Aadhar/ ID/ PAN number or credit card details.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

7. The information shared at public places such as Airport/Railway Station can be used to commit crimes.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

B. THREAT SUSCEPTIBILITY

Thinking about Airports and Aviation sector and its vulnerability to cyber domain, how safe you feel in operating your personal IT devices the Airport/Aircraft. Please tell us how much you agree or disagree with each statement.

1. My personal devices are highly safe to operate in an Airport/Aircraft as anywhere else.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

2. I recommend use of all mobiles and computers inside the Airport/Aircraft.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

3. Delhi Airport takes adequate precautionary measures to safeguard Airport Cyber Security

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

4. I feel Airport's IT systems cannot be hacked and we are not susceptible to any risks using internet at the Airport (R).

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

C. COPING SELF EFFICACY

We appreciate that Airports take adequate measures to secure themselves from cyber nuisances. Please tell us how much you agree or disagree with each statement.

1. I feel comfortable taking measures to secure my devices while using public internet at Airports.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

2. Taking necessary security measures is entirely within my control.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

3. I have the expertise to take required security measures.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

4. Taking the required security measures is easy at Airports as anywhere else.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

5. I feel paranoid when thinking about cyber security.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

6. In general, I am safe from any threat when using public Wi-Fi at Airports /Aircrafts.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

D. RESPONSE EFFICACY

One is aware of nuisances of Cyber security in the environment. As a passenger, one takes necessary steps in keeping the cyber space safe at all points of time. Please tell us how much you agree or disagree with each statement.

1. Security software would be useful for detecting and removing a malware.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

2. Security software will increase my level of protection.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

3. Security software will help in detecting and removing threats faster.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

E. RESPONSE COST

Added safety and security comes with a cost to society. Please tell us how much you agree or disagree with each statement.

1. I am ready to pay extra for safer cyber environment at Airports.

Highly Disagree		Disagree	Neutral	Agree	Highly Agree

2. Security programs interfere with other programs in my phone.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

3. Using Security software is too much of a hassle.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

F. PRIOR EXPERIENCE WITH SAFETY HAZARDS

Have you ever experienced the following while travelling by Air anytime earlier after browsing at airports? Please tell us how much you agree or disagree with each statement.

1. Slowing down of your IT device.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

2. I got a virus attack from opening a link.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

3. Virus attack from just visiting a web site.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

4. Mysterious icons or programs appeared on my phone.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

5. A pop-up message offering a free computer security scan.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

6. Had important personal information stolen, such as your Social Security Number or credit card number.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

7. Been the victim of an online scam and lost money.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

G. PERSONAL RESPONSIBILITY

While we know that our awareness and actions as passengers can make the Airport IT safety systems more secure. Am I prepared to be more educated and aware? Please tell us how much you agree or disagree with each statement.

1. If I adopt cyber security measures, I can make a difference in helping the Airport much safer.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

2. The efforts of one person are useless in securing the cyber space in Airports.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

3. Every passenger can make a difference when it comes to cyber security.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

H. SECURITY INTENTIONS

Thinking of your future actions, indicate the degree to which you agree or disagree with the following statements regarding your likelihood of implementing security measures to protect yourself online while travelling at Airports. These questions will still refer to the home computer or other device you would feel safe to use for online financial transactions.

1. I am likely to take security measures to protect my mobile device while using at airport.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

2. I will upgrade my security measures to protect myself better while using free Wi-Fi at Airport.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

3. I will not save my passwords while using mobile/computer at Airports.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

4. I will use passwords that are harder to guess.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

5. I will change my browser security settings to a higher level, and I am vigilant using my device at Airport.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

6. I will learn how to be more secure online at Airport.

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

7. I run protective software regularly to remove spyware from my computer/ mobile at Airport

Highly Disagree	Disagree	Neutral	Agree	Highly Agree

Personal Details

1. Your Email address
2. Gender

   *Female

   * Male
3. Age *

   *19-29

   *30-40

   *41 & above

4. Education Level
   *Graduate
   * Post graduate
   *Others

5. Income per annum
   * Less than 4 lakhs
   *4-10 Lakhs
   *10 lakhs & above

6. Frequency of Flying through Delhi Airport
   * Once a year
   *2 to 5 times in a year
   * 6 to 10 times in a year
   * 11 or more times in a year

Appx 'E'

Publications

1. ISSN: 2455-3085 (Online) *Issue-12* research review **International Journal of Multidisciplinary** December -2018 www.rrjournals.com [UGC Listed Journal] RRIJM 2015,

Perceived Cyber Threats to Aviation Industry in India

Anjan Kumar Sinha, Nikhil Kulshrestha & Binod Kumar Singh

Abstract

World over it is progressively helpless against cyber-attacks due to interruptions that influence the respectability of data. This failure is an element of world economy which is quiet substantial. Aviation sector contributes to 7% of World GDP and Indian Civil Aviation close to 9%, thus any disruptions can cause huge losses. Another muddling factor is the thickness of India's cyberspace, which does not allow a uniform legitimate or specialized limit for data protection laws. Security threats to civil aviation have turned out to be more challenging due to cyber-physical systems and their integration. One of them is that it is seeming considerably more confounded and advanced to oversee is cyber-attack. Today, the worldwide civil aviation network is depending on Information Technology (IT) frameworks. Apart from these issues, due to primarily based oppressor attacks on airplane and air systems, air terrorism carries the threats to aviation sector across the globe. There is a need to be certain degree of awareness of the situation by the environment. The Aviation ecosystem in India must get down building multiple layers of secured firewalls in order to remain safe and overpower the menace of cyber threats and Cyber terrorism. IT frameworks will be a key driver of development and proficiency, including frameworks to upgrade safety and security. In this paper an effort is made to highlight the cyber security threats in the civil aviation industry to Indian subcontinent and the solution for limiting them.

2. **International Journal of Management, IT & Engineering** Vol. 8 Issue 1(1), January 2019, ISSN: 2249-0558 Impact Factor: 7.119 Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in cabell‘s Directories of Publishing Opportunities, U.S.A http://www.ijmra.us, Email: editorijmie@gmail.com

Role of Protection Motivation Theory in Cyber Security of Indian Aviation sector

Anjan Kumar Sinha, Nikhil Kulshrestha & Binod Kumar Singh

Abstract: Cybercrime is increasing, targeting to the people, organizations, and governments rapidly. The estimated expenses of cybercrime for the global economy are around $445 billion every year, where 800 million only in 2013 were influenced by cyber surveillance and loss of the private data. Regardless of many existing countermeasures going for securing clients' honesty by resistance against malicious activities. Such activities can be either coordinated against themselves or against authoritative resources where the client is utilized as the backdoor by cyber criminals.This strong, safe and effective transport service which cover up to 2.6 billion passengers a year and 48 million tons of goods every day, Aviation's global financial affects (immediate, backhanded, prompted, and the travel industry) is assessed at $2.2 trillion or 3.5% of global total national output (GDP). In this article we described different frameworks for cyber security in Aviation sector and the protection motivation theory and its role.

3. **International Journal of Scientific & Technology Research**

Volume 8, Issue 10, October 2019 ISSN 2277-8616 2167 IJSTR©2019 www.ijstr.org

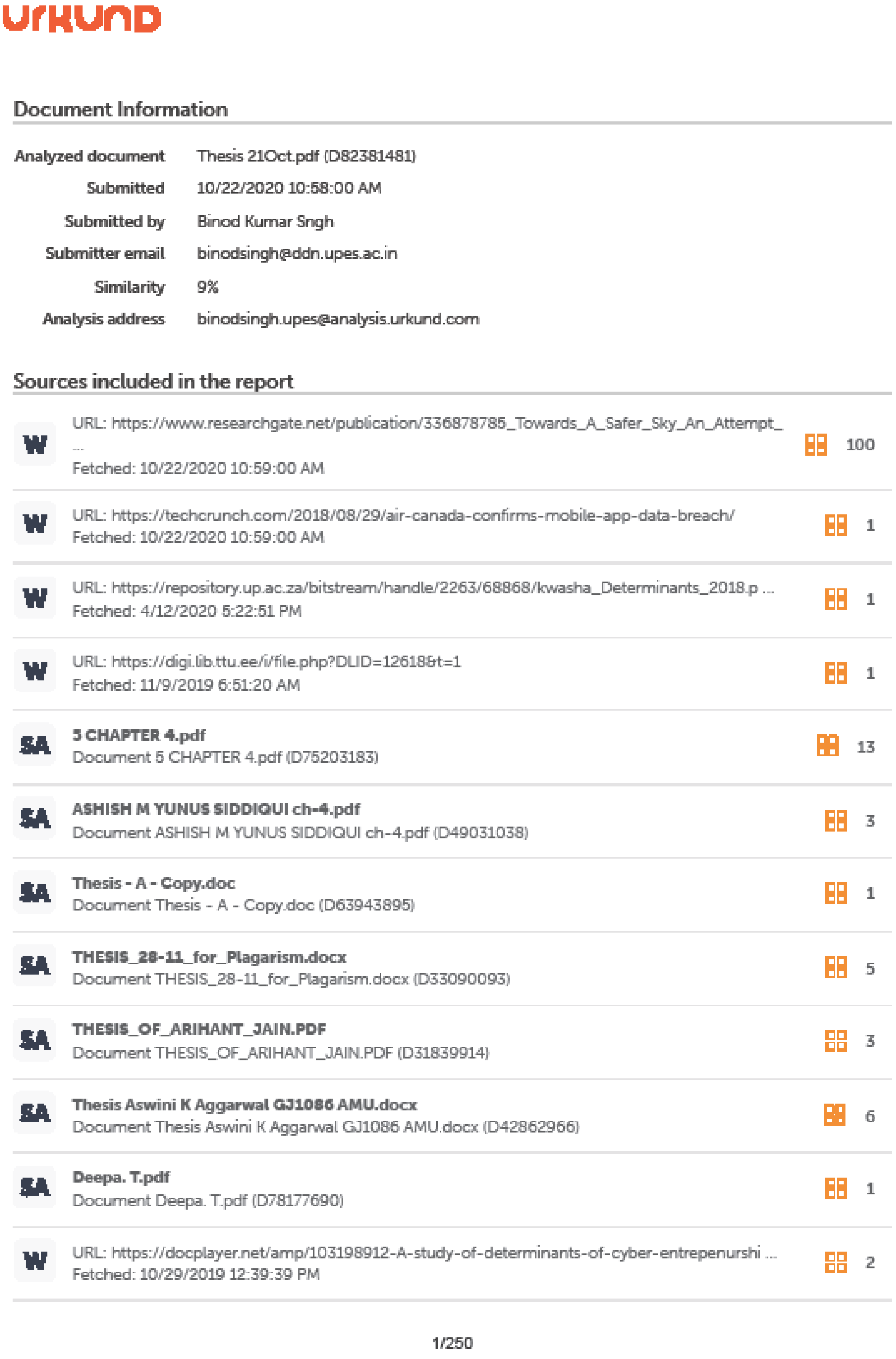
Towards A Safer Sky: An Attempt to Study Indian Minds and Security Intentions in The Aviation Sector

Anjan Kumar Sinha, Nikhil Kulshrestha & Binod Kumar Singh

Abstract:

Aviation industry has a global business model and the global standardized safety and security norms governed by International Civil Aviation Organization (ICAO) and Federal Aviation Administration. (FAA). IT security has been on top of the charts for the past few years and will remain so for all kind of industries. The motivation for the present study is drawn from few incidents in Aviation sector worldwide which didn't 't have conclusive results. World over there are numerous studies on Cyber security and even on Aviation Cyber security however there is limited or nil study collective on Aviation Cyber Security behaviour. Present study tries to explore awareness among Indian fliers and their behaviour to achieve safe cyber environment in the Civil Aviation sector. The study uses Protection Motivation theory as a framework to understand whether the consciousness of human mind that can make a difference in the Cyber posture in travel industry specific to Indian Aviation. From a mail survey, 298 responses were obtained on the developed measures. The paper uses Exploratory Factor analysis as a tool to measure the responses and step Regression model to identify the factor affecting Aviation Cyber Security behavior. The results of the study indicate that prior experience with Cyber threats is the most significant predictor of passengers Cyber Security behaviour. Index Terms: Aviation, Airport Cyber Security, Protection Motivation theory, Cyber security behaviour.

Appx 'F'



URKUND

Document Information

Analyzed document	Thesis 21Oct.pdf (D82381481)
Submitted	10/22/2020 10:58:00 AM
Submitted by	Binod Kumar Sngh
Submitter email	binodsingh@ddn.upes.ac.in
Similarity	9%
Analysis address	binodsingh.upes@analysis.urkund.com

Sources included in the report

W	URL: https://www.researchgate.net/publication/336878785_Towards_A_Safer_Sky_An_Attempt_ ... Fetched: 10/22/2020 10:59:00 AM	100
W	URL: https://techcrunch.com/2018/08/29/air-canada-confirms-mobile-app-data-breach/ Fetched: 10/22/2020 10:59:00 AM	1
W	URL: https://repository.up.ac.za/bitstream/handle/2263/68868/kwasha_Determinants_2018.p ... Fetched: 4/12/2020 5:22:51 PM	1
W	URL: https://digi.lib.ttu.ee/i/file.php?DLID=12618&t=1 Fetched: 11/9/2019 6:51:20 AM	1
SA	**5 CHAPTER 4.pdf** Document 5 CHAPTER 4.pdf (D75203183)	13
SA	**ASHISH M YUNUS SIDDIQUI ch-4.pdf** Document ASHISH M YUNUS SIDDIQUI ch-4.pdf (D49031038)	3
SA	**Thesis - A - Copy.doc** Document Thesis - A - Copy.doc (D63943895)	1
SA	**THESIS_28-11_for_Plagarism.docx** Document THESIS_28-11_for_Plagarism.docx (D33090093)	5
SA	**THESIS_OF_ARIHANT_JAIN.PDF** Document THESIS_OF_ARIHANT_JAIN.PDF (D31839914)	3
SA	**Thesis Aswini K Aggarwal GJ1086 AMU.docx** Document Thesis Aswini K Aggarwal GJ1086 AMU.docx (D42862966)	6
SA	**Deepa. T.pdf** Document Deepa. T.pdf (D78177690)	1
W	URL: https://docplayer.net/amp/103198912-A-study-of-determinants-of-cyber-entrepenurshi ... Fetched: 10/29/2019 12:39:39 PM	2

1/250