10-Aug-24

NAVIGATING TURBULENCE: A RESEARCH ON CYBERSECURITY RISK AND ITS EFFECTS ON AVIATION BUSINESS

Research Methods & Dissertation

Dinto James
22201777

NAVIGATING TURBULENCE: A RESEARCH ON CYBERSECURITY RISK AND ITS EFFECTS ON AVIATION BUSINESS

Submission of Thesis and Dissertation

National College of Ireland
Research Students Declaration Form
(Thesis/Author Declaration Form)

Name	**:** Dinto James
Student Number	**:** 22201777
Degree for which thesis is submitted	**:** MSc International Business
Title of Thesis	**:** Navigating Turbulence: A Research on Cybersecurity Risk and Its Effects on Aviation Business
Date	**:** 10/08/2024

Material submitted for award

A. I declare that this work submitted has been composed by myself. ☑

B. I declare that all verbatim extracts contained in the thesis have been distinguished by quotation marks and the sources of information specifically acknowledged. ☑

C. I agree to my thesis being deposited in the NCI Library online open access repository NORMA. ☑

D. ***Either*** *I declare that no material contained in the thesis has been used in any other submission for an academic award. ☑
Or *I declare that the following material contained in the thesis formed part of a submission for the award of MSc International Business
_____
(State the award and the awarding body and list the material below)

National College of Ireland

Project Submission Sheet

Student Name:	Dinto James……
Student ID:	22201777……
Programme:	MSC International Business…… **Year:** 2023……
Module:	Research Methods & Dissertation……
Lecturer:	Tara Cheevers..……
Submission Due Date:	10/08/2024……
Project Title:	Navigating Turbulence: A Research on Cybersecurity Risk and Its Effects on Aviation Business
Word Count:	15897……

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the references section. Students are encouraged to use the Harvard Referencing Standard supplied by the Library. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action. Students may be required to undergo a viva (oral examination) if there is suspicion about the validity of their submitted work.

Signature: 

……

Date: 10/08/2024……

PLEASE READ THE FOLLOWING INSTRUCTIONS:

1. Please attach a completed copy of this sheet to each project (including multiple copies).
2. Projects should be submitted to your Programme Coordinator.
3. **You must ensure that you retain a HARD COPY of ALL projects**, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. Please do not bind projects or place in covers unless specifically requested.
4. You must ensure that all projects are submitted to your Programme Coordinator on or before the required submission date. **Late submissions will incur penalties.**

5. All projects must be submitted and passed in order to successfully complete the year. **Any project/assignment not submitted will be marked as a fail.**

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

AI Acknowledgement Supplement

Research Methods & Dissertation

Navigating Turbulence: A Research on Cybersecurity Risk And Its Effects On Aviation Business

Your Name/Student Number	Course	Date
Dinto James/22201777	MSC International Business	10/08/2024

This section is a supplement to the main assignment, to be used if AI was used in any capacity in the creation of your assignment; if you have queries about how to do this, please contact your lecturer. For an example of how to fill these sections out, please click here.

AI Acknowledgment

This section acknowledges the AI tools that were utilized in the process of completing this assignment.

Tool Name	Brief Description	Link to tool
N/A	N/A	N/A

Description of AI Usage

This section provides a more detailed description of how the AI tools were used in the assignment. It includes information about the prompts given to the AI tool, the responses received, and how these responses were utilized or modified in the assignment. **One table should be used for each tool used**.

N/A	
N/A	
N/A	N/A

Evidence of AI Usage

This section includes evidence of significant prompts and responses used or generated through the AI tool. It should provide a clear understanding of the extent to which the AI tool was used in the assignment. Evidence may be attached via screenshots or text.

Additional Evidence:

N/A

Additional Evidence:

N/A

Abstract

Cyberattacks have become a significant concern for Europe, a crucial hub of global aviation. The report focuses on a thorough investigation over the last two decades to estimate the impact of cyber breaches on the aviation business in this region, both directly and indirectly. The effort will use qualitative analytical methodologies to reveal the subtle linkages between cybersecurity breaches and corporate success that have hitherto been ignored in primary research. This study seeks more than merely factual determination; the goal is to provide fresh information and serve the interests of industry participants through research and forecasting. Following the COVID-19 outbreak, there has been a significant shift in the aviation industry that not only affects operating patterns but also has implications for digital security.

The latest developments seen highlight the importance of developing an effective cyber architecture. While the sector redefines itself, it must engage with improved cyber defences and establish preventative measures based on the most recent knowledge about the nature of the threats. Whereas most research is quantitative, this study is qualitative, revealing the hidden intricacies of cyber risk and security from people at the forefront of the battle. The ultimate goal is to generate relevant useful insights that are aligned with the strategic objectives of the aviation sector and resistant to the broad range of cyber threats that change with each wave of technology.

Table of Contents

NAVIGATING TURBULENCE: A RESEARCH ON CYBERSECURITY RISK AND ITS EFFECTS ON AVIATION BUSINESS

Chapter 1: Introduction

1.1 Chapter Introduction

An introduction is the foremost chapter, which provides a brief background to the overall study. With the help of this chapter, the researcher presents an outline of the present research and discusses all the major aspects of this dissertation. In this chapter, the overall background of the research topic is explained, which helps the reader gain brief information concerning the research area. Further, the researcher states the “aim”, “objectives” and “questions” of the research, which has been accomplished in the further sections of the study. In regards to the “research questions and objectives”, a “problem statement” has also been defined. In the context of this “problem statement”, the researcher informs the main problem addressed in this present dissertation. Apart from these, the “scope of the study” and the “limitations” have also been identified, along with brief information on the “overview of the dissertation”, which helps in enhancing the overall quality of this present dissertation.

1.2 Background Of The Study

It is observed that there is a perpetual trend in surging the levels of integrating ICT (“information and communication technology”) within mechanical instruments in their daily use, in the “aviation industry”. With respect to such integration activities, the “aviation industry” is found to be facing several challenges concerning “cybersecurity resilience” (Ukwandu et al., 2022). In the context of the “aviation industry,” it can be said that it plays a major role in maintaining a strategic threshold between countries (Ukwandu et al., 2022). Hence, it is necessary to assure that effective metrics are incorporated for preserving the “resilience of cybersecurity measures” within the “airline companies” for eradicating any latent indemnities.

In the UK, “cybersecurity breaches” and “cyber security attacks” are found to be the most significant challenges (Government of the UK, 2024). It is also found by the Government of the UK (2024), around 50% of the total businesses along with 32% of the total charities have identified certain type of “cyber security breach”.

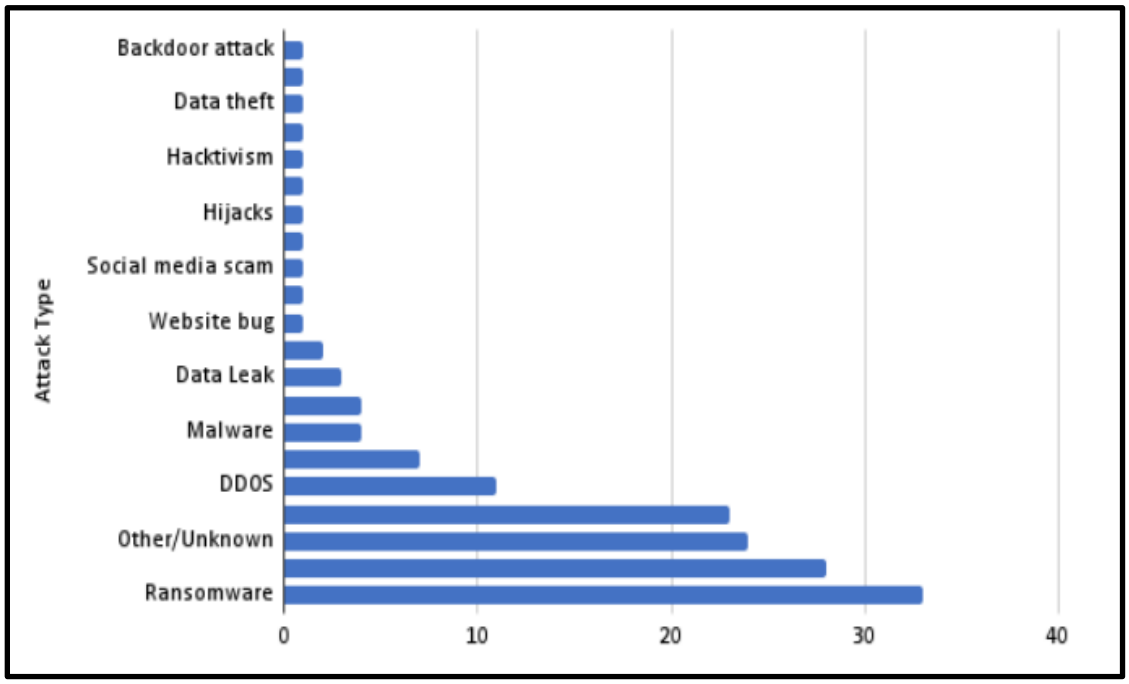

Figure 1.1: Various types of cyber security attacks from 2020 to 2022

(Source: International Civil Aviation Organisation, 2023)

As per the "International Civil Aviation Organisation” due to these cyber-attacks shown in Figure 1.1 many aviation companies faced several negative impacts which not only impacted financially but also affected to overall credibility and performance (International Civil Aviation Organisation, 2023). This organisation has also identified that such attacks have increased around 24% across the globe by June 2023. Thus, on the basis of these incidents, it is identified that there is a critical need to incorporate significant measures for ensuring “cyber security” in the industry.

1.3 Aim

The overall aim of this present dissertation is to “understand the overall impact of cybersecurity attacks on the performance of airline businesses, while significantly focusing on the European airlines”.

1.4 Objectives

With reference to the aim stated above, the researcher has prepared the objectives as follows:

- To analyse the overall impacts caused by the “cybersecurity breaches” on airline companies in Europe
- To assess the “cybersecurity measures” taken into consideration by “European Airline Companies” to address these “cybersecurity breaches”
- To evaluate the overall effectiveness of these “cybersecurity measures” implemented by the “European Airline Companies” for addressing “cybersecurity breaches”
- To identify the challenges faced by the “European Airline Companies” while implementing “cybersecurity measures”.

1.5 Research Questions

In this dissertation, the “primary question” and “sub-question” that have been addressed are mentioned as follows:

Primary question:

What is the overall impact of “cyber security attacks” on the business performance of “European Airline Companies”?

Sub questions:

- What “security measures” are being adopted by “European Airline Companies” to address these “cybersecurity breaches”?
- Are those measures efficient in addressing “cybersecurity breaches”?

- What are the challenges faced by the “European Airline Companies” while implementing “cybersecurity measures”?

1.6 Problem Statement

It is observed that the “aviation industry” is an interconnected industry and it is a highly sophisticated industry, which utilises the technologies significantly (Kabashkin et al., 2023). Therefore, I must state that these technologies simplify the operational activities in the “aviation industry”, at the same time, they pose a significant challenge to the industry in the form of “cybersecurity challenges”, similar to a coin posing two different phases. According to Stastny and Stoica (2022), a significant association in the “aviation industry” has increased the threat of “cybersecurity challenges”. With the advancement in the field of digital technologies, the threat of “cybersecurity challenges” has also increased along with their dependency on digital infrastructure, which has the potential to damage the overall operability of the organisation, including the “security of data and passengers”. Lykou et al. (2018) added that these challenges can lead an organisation to face significant financial loss and pose severe harm to the reputation of the industry. However, in order to address these challenges, the organisations and industry are found to be investing significantly such that robust measures are in place and the airline organisations and industry do not have to face adverse situations (Tong and Kwan, 2022). In spite of putting in such efforts, the organisations and industry sometimes fail to eliminate such challenges.

Therefore, this present study focuses on analysing the present situation of “cybersecurity threats” within the “aviation industry” along with the impact of such threats on the all-inclusive performance of “airline companies”. With the help of this dissertation, the most significant threats are determined and the efficacy of the current “cybersecurity measures” are evaluated. The findings provide a comprehensive understanding of the overall impact of “cybersecurity challenges” on the “aviation industry”, which further helps in providing critical information on the methods that can be implemented for maintaining the efficacy of “cybersecurity measures” and eliminating the threats associated with “cyber attacks” in the airline organisations.

1.7 Research Rationale

The “background of the study” informs the critical importance of the “airline industry”. In addition to this, the previous section of this chapter also informs that the “airline companies” significantly utilise digital networks and technologies to simplify their operational activities. Concerning the importance of digital technologies, airline organisations as well as the industry are found to be closely associated with the threat imposed by these technologies. This dissertation is significant because it provides an inclusive apprehension of the impact of these threats on the “aviation industry”. The main rationale for carrying out this dissertation is to find out the impact of “cyber security threats” on the aviation industry. Other than this, it is also found that the operability of airline companies is severely hurt due to “cybersecurity challenges” (Kizilcan and Mizrak, 2022). Therefore, this dissertation explores such threats and significantly accords in developing stringent measures for ensuring the safety of the operational activities of airline companies.

In addition to this, these threats are also found to be posing adverse impacts on the finances of the company along with a major threat to its notoriety (Ebert et al., 2021). Thus, this dissertation focuses on assessing this aftermath and provides considerable recommendations for minimising the risks and securing the financial position of the organisation. These threats also pose a negative impact on the trust of the consumers (Shaikh and Siponen, 2023). Therefore, it is another rationale for carrying out this dissertation, which helps in analysing the impact of such impacts on the relationship of an airline organisation, and further recommending certain suggestions for enhancing the trust among the customers. The current gap that has been addressed in this dissertation is regarding the “cyber security breaches” and the novel technologies used in aviation for addressing such breaches. This dissertation tries to focus on the efficacy of these technologies for eliminating “cyber security breaches”. Apart from these, this dissertation can prove to be crucial for directing the aviation industry to implement novel techniques securely. Thus, having a sheer apprehension of “cyber security challenges” the concerned authorities are capable of making sound strategies in terms of providing effective solutions and reducing the correlated threats.

1.8 Limitations

Concerning this dissertation, the researcher has faced certain challenges. Some of these challenges are:

- Determining the reliability of the collected data. There is a lot of data concerning the threats of "cyber security" with respect to the aviation business. However, selecting the most appropriate data for the data among a huge database is the most significant challenge.
- Secondly, the dissertation focuses on the recent challenges faced by the "airline industry". However, considering the development of technologies, there could be an instance that the findings of this dissertation may become obsolete in the future.
- Further, this dissertation emphasises the airlines of Europe, which limits the findings of the overall study.

1.9 Dissertation Overview

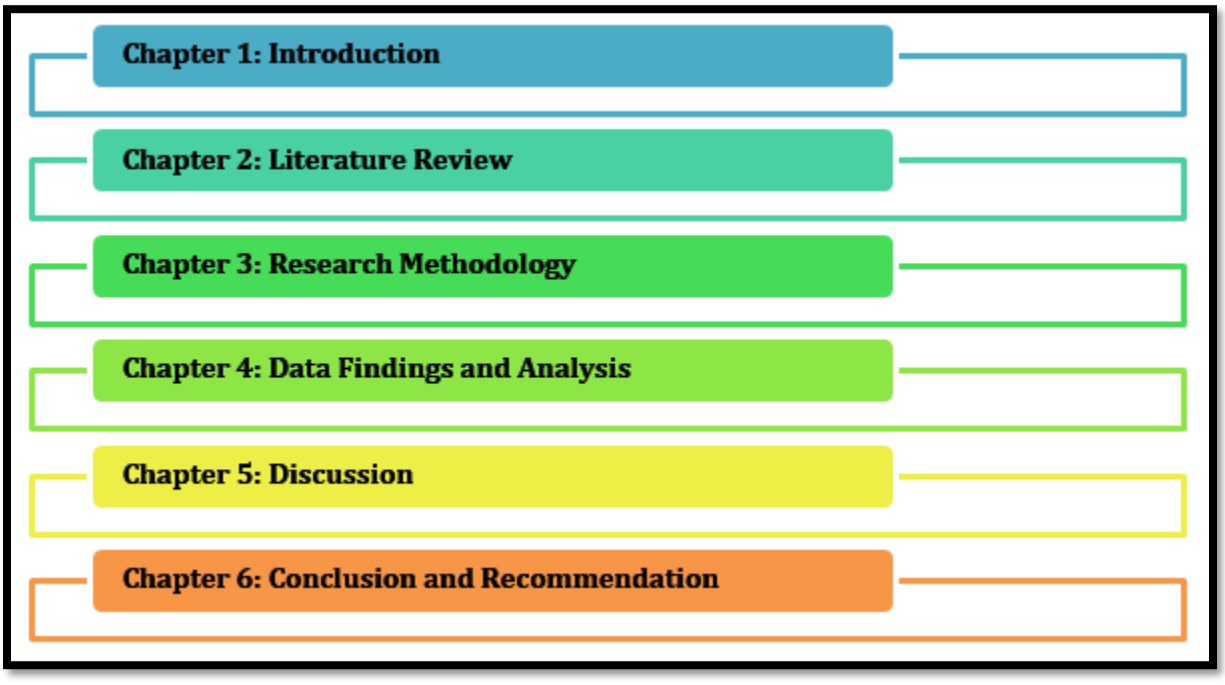

Figure 1.2: Dissertation structure

(Source: Self-created)

Based on the image (figure 1.2), this dissertation comprises five chapters. The first chapter is - "Introduction", which provides a brief about the research topic. The second chapter is "literature review". A "theoretical framework" as well as conceptual framework" for this study has been provided that helps in comprehending the overall literature of this "research topic". The third chapter comprises "Research Methodology", which informs the overall methodologies considered for accumulating and assessing the data. The fourth chapter is "Data Findings and Analysis", here the collected data are analysed to provide sound and meaningful outcomes. Followed by this chapter, a discussion chapter is added, which provides a profound discussion of the findings. This dissertation ends with "Conclusion and recommendations" chapter, where the total findings are concluded and final recommendations with respect to the study findings are provided. Additionally, recommendations for future research are also provided in this study.

1.10 Chapter Summary

On the basis of this chapter, it is summarised that this chapter offers crucial information on "cyber security challenges" and their impact on the "airline industry". The "aim and objectives" have been prepared by emphasising the "cyber security challenges". Additionally, "research questions" are prepared with respect to the identified "problem statement" of the dissertation. These are further followed by the "limitations", "rationale" and "overview" of the study.

Chapter 2: Literature Review

2.1 Introduction

Literature review is second and another important chapters of this study. It is a process that deals with the accumulation of academic as well as scholarly information concerning the research topic. This chapter mainly focuses on offering a comprehensive overview of the current literature on "cyber security risks" and how it impacts the "aviation industry". The primary purpose of this chapter is to offer inclusive information on varied literature with respect to the research topic. The findings from the literature are further applied to the research paper to carry out a qualitative and effective study (Oztemel and Gursev, 2020). Firstly, I will provide an overview of cyber security in the aviation industry. I will then reflect on an analysis of the evolution of cyber security within aviation. The cyber security risks involved in the aviation business will also be reviewed providing critical information on the risks involved in the aviation business. My focus will then move to the impact of these risks and the strategies implemented by the aviation business to address such risks. In order to enhance the quality of this review, the researcher has further reviewed the challenges associated with the risk management strategies for managing cyber security risks. Above all, some case studies regarding cyber security risks have also been reviewed, along with some theoretical frameworks that are used in the further chapters of this study.

2.2 Cybersecurity in Aviation

IATA (International Air Transport Association) represents the overall airline industry. Since then, this industry is found to be associated with several challenges and vulnerabilities, which has a significant adverse impact on the industry. These challenges are related to security, commercial as well as safety. In the current era of significant digitalisation as well as connectivity, the aviation industry is found to be dealing with complicated as well as critical challenges, which is also known as cyber security in aviation (ICAO, 2024). Cyber security in the aviation industry is regarded as the consolidation of people, technologies as well as processes that work together to safeguard the organisations associated with civil aviation, along with the operations as well as passengers from any type of digital attack (IATA, 2024). Therefore, in this context, Lehto (2020) stated that the main focus of IATA is to ensure that this body interacts with the overall environment of cyber

security interconnecting and interacting with the complete life cycle of the aircraft. This focus mainly aligns with the overall operational activities carried out by different stakeholders. However, it is not limited to airport operators, airlines, regulators and others.

Filinovych and Hu (2021) found cyber security in the aviation industry is the top priority in this industry. Ukwandu et al. (2022) added that the increased utilisation of digital technologies, and connectivity has allowed the industry to transform various approaches and methods for interacting with customers to enhance their experience, aviation operational activities, and delivery services along the regulatory framework. This transformation has not only exposed aviation to the benefits but has also attracted several challenges to the industry. The challenges that have been exposed to the aviation industry are numerous, some of these are managing vulnerabilities in the cyber security context, challenges associated with international operations, supply chain, service providers and others (IATA, 2023). Additionally, Korba et al. (2023) found technological issues as another major challenge in the aviation industry, which has the potential to attract cybersecurity risks. Due to these challenges and complexities, the aviation industry becomes significantly vulnerable to various risks as well as challenges as noted by Ukwandu et al (2022). Elmarady and Rahouma (2021) noted that despite various challenges and threats to the aviation industry, cyber-attacks pose limited threats to the aviation industry. Thus, in this regard, Dave (2022) stated that in order to address these challenges, it is important to implement continuous improvement as well as develop measures.

2.3 Evolution Of Cyber Security In Aviation

The aviation industry is found to be implementing various digital technologies, due to which the importance of cyber security has increased profoundly (Ukwandu et al., 2022). It is found that the aviation industry has implemented significant technologies, such as implementing systems in the flights to manage the data of the passengers (Stastny and Stoica, 2022). With the implementation of these technologies, the airline industry has gained substantial efficiency as well as financial benefits when air travel is taken into consideration. Despite such efficiency in terms of interconnectedness, various vulnerabilities have increased with respect to cyber security (Li and Liu, 2021). It is also found that there is an increased potential of threat with respect to accessing

the IT systems of the flights in an unauthorised way, which creates a high possibility for significant losses to the airlines.

In the context of the evolution of cyber security, Fadziso et al. (2023) found evolution was carried out in different phases. The first phase deals with the time when there were no digital technologies and the systems were not integrated with the technologies. Karpiuk and Kelemen (2022) opined that the systems were less integrated with the technologies and there was no discussion about any cyber security. During the 1990s, some digital technologies were introduced (Hilbert, 2020). When these technologies were introduced, the industry was aware of cyber security issues for the first time in the 1990s. Various digital systems were introduced during this time, which eventually exposed the industry to various cyber-attacks. For example, the cyber attack of 1988 known as "The Morris Worm Attack" led thousands of computer systems to crash down. However, this attack was unintentional which occurred due to an error in writing the program (Hagen, 2023). Along with this technology during the 1990s, the aviation industry was also introduced to early networking. Networking is mainly associated with aviation technologies used for carrying out aviation activities. Filinovych and Hu (2021) found this networking was mainly carried out for carrying out maintenance activities. Torens (2020) further argued that these networks are enclosed with various security reasons which dissociate the network from the external networks.

During the early years of the 2000s, the aviation industry gained increasing connectivity. In this regard, digital systems were used significantly for carrying out navigation as well as communication purposes (Pyzynski and Balcerzak, 2021). During this time, networks containing IP were also introduced which helped different systems to get connected in an effective way. Chowdhury and Gkioulos (2021) added that it also helped in enhancing efficiency along with great threats and challenges. With increased connectivity, various regulatory bodies, such as the FAA (Federal Aviation Administration) were set up in order to ensure that awareness regarding the regulations can be spread and these bodies can focus on implementing effective measures for addressing cybersecurity threats. In this regard, it is crucial for the companies to assure that sound legislations as well as standards are followed within the operations (Elmarady and Rahouma, 2021). It is also mandatory to ensure that such regulations are followed and complied and security aspects of the companies are not conceded. Such actions will help the industry to address any kind of cyber security issues (Efe et al., 2021). It is also important for the industry to ensure that all the

guidelines are being followed. It helps the industry as well as organisations to ensure that any gap present with respect to cyber security is addressed in an effective way.

In the modern era, various novel digital technologies have been introduced, such as broadband, APTs, in-flight connectivity and various other developments. The introduction of broadband as well as in-flight connectivity, has increased the threat of cyber attacks (Tong and Kwan, 2022). Due to this, it is important for these systems to ensure that the threats are detected early and reported, allowing for immediate actions to be implemented (Mishra et al., 2022). Apart from these, various regulatory frameworks were also implemented that help the aviation industry to address cyber security issues related to the aviation industry. When the recent developments are taken into consideration, it is found that IoT as well as advanced technologies have integrated eventually helps to ensure a regular flow of data as well as constant connectivity (Ebert et al., 2021). In addition to this, it has also been identified by Anaedevha and Ajibola (2020) that better measures for addressing cybersecurity issues have been introduced. In this regard, various technologies are used for monitoring the data on a real-time basis, along with the implementation of AI, ML as well as blockchain (Anaedevha and Ajibola, 2020). These technologies have substantially disrupted the current cyber security of the aviation industry.

2.4 Cyber Security Risks in Aviation

With reference to "cyber security risks", Genremeskel et al. (2023) found that cyber security risks are the major group of threats that are required to be addressed properly. The authors have further added that it helps the organisation in limiting the impacts of such risks. In this context, it is identified that cyber security risks have developed as a major concern when organisations associated with digital transformation are concerned (Gebremeskel et al., 2023). Development in technologies does only helps organisations or industries to gain various benefits or a competitive edge but also poses significant challenges (Koroniotis et al., 2020). With respect to the cyber security risks, it is found by Florackis et al. (2023) that there are various risks associated with cyber security within the aviation industry, eventually hampering the aviation industry.

First and foremost, it is identified that the airlines are significantly exposed to the risks. Florackis et al. (2023) stated that the major risk is related to the financial loss. In the context of the financial

loss, it can be said that due to weak cyber security, an airline organisation can incur various direct as well as indirect costs. When direct costs are considered, Mızrak (2023) noted that cyber-attacks in the organisation can attract various costs to the company, as the organisation may be required to hire external experts to address such attacks and secure the overall security of the organisation. Apart from this, direct costs may include the payments of a ransom, to enable the company to regain access to its crucial data. In addition to this, any cyberattacks may attract some indirect cost to the company, leading the company to face significant financial losses. Cains et al. (2022) argued that these financial losses occur due to the cancellation of flights in case of any cyber security challenges.

Apart from this, it is also found by Cremer et al. (2022) that loss of data is another major risk. In this context, it can be said that when there is any cyber-attack on an aviation company, the data is mainly affected. In this regard, the consumers' data, crew members' data and other important information of the airline company are attacked and eventually, the company loses trust in the market (Shaikh and Siponen, 2023). Any such incident can lead an organisation to severely hamper the trust in the market. As a result, the passengers would avoid taking flights from the affected airline company. Eventually, the company would have a smaller number of customers and may attract a negative reputation in the industry (Kalinin et al., 2021). In addition to this, Ganin et al. (2020) added that when there is any cyber security risk related to the loss of data or any issue, the customers start losing trust in the company. As a result, the organisation faces several other losses such as revenue, credibility, trust, reputation and customers. Any kind of cyber security risk or cyber security attack creates a negative impact on the reputation as well as the trust of the industry. A significant cyber-attack has the potential to damage the overall image of the airline as well as the industry. Therefore, it becomes difficult for organisations to gain the trust of their customers. In addition to this, it is also found that any cyber-attack compromises the data of the passengers as well as the crew members. Such attacks cannot only hamper the organisation but can also impose a negative impact on an individual customer or crew member (Alsulami and Zein-Sabatto, 2020). It is also found by Chung and Tan (2022) that the aviation industry is mainly dependent upon various external suppliers and vendors such that the passengers and customers may get services easily. If any vulnerabilities regarding "cyber security" are present in the systems of vendors as well as suppliers, it may create a major bottleneck in the activities of the aviation industry.

These are some major threats that poses substantial vulnerability to the aviation industry.

2.5 Impact Of Cyber Security Risks In Aviation

With respect to the cyber security risks, these risks impose the aviation industry to several threats and lead the aviation industry to face several challenges. Some of the major impacts of the cyber security risks in the field of aviation industry are described as follows:

Firstly, it is identified that cyber security exposes the aviation industry to various regulatory liabilities. In this context, it is identified that this industry deals with huge amounts of personal data of the crew members as well as the customers. It is also found that these deal with sensitive personal information such that any threat to this information can compromise the overall operational activities as well as the reputation of the industry (Turtiainen et al., 2022). Aydın and Kahraman (2021) added that it may introduce the industry to face several regulatory liabilities. Misuse of any such private and confidential information may lead organisations to face charges for not following GDPR, eventually posing a significant threat to the industry and organisations.

Secondly, it is also found by Kamiya et al. (2021) that cyber risks can expose the industry to significant legal actions from the stakeholders of the company. The legal environment is developing at a significant rate. There are various challenges that the aviation industry faces, which leaves the organisation to face challenges imposed by the clients as well as customers due to the threat of personal information (Strohmeier et al., 2022). Apart from this, it is also found by Alhayani et al. (2021) that cyber risks significantly impact the data of customers. Any attack on the airline company leads the company to expose its crucial data to attackers, eventually corroding the trust of the customers from the airline company (Alhayani et al., 2021). Further, it is also found by Najaf et al. (2021) that cyber security risk also adversely impacts the supply chain of the organisation. Further, Najaf et al. (2021) opined that the supply chain of an airline company is very complex, and includes several stakeholders and suppliers. Thus, as a result, any risk or challenge in terms of cyber security has the potential to adversely disrupt the supply chain of the organisation.

Cyber security risk is also found to impose various disruptions in the operational activities of the industry. In this context, it is identified that it may lead the flights to cancellations as well as delays. It also imposes a negative impact on the ground operations (Gnatyuk et al., 2020). In this regard,

it can be said that cyber-attack has an adverse impact on the IT systems, ground operations as well and scheduling systems of the industry which leads to measurement challenges even for the passengers as well as to the airline. On the other hand, when ground operations are taken into consideration it is found that any cyber security risk may create various logistical challenges as well as develop several inefficiencies in terms of carrying out operational activities (Xie et al., 2022). All these contribute to the challenges faced by the airline companies operating in the aviation industry. These inefficiencies not only hamper the operations of an organisation but also create challenges for customers, by causing them discomfort. For example, due to cyber security challenges in ground operations, customers have to wait for long hours for their security check-in.

Cyber security risk is also found to impose a significant impact on the financial aspect of the industry. In this context, a direct financial loss can be observed due to any kind of ransomware attack (Shafik et al., 2023). Apart from that the company may also face legal costs due to its non-compliance with the safety measures regarding cyber security legislation (Tran et al., 2022). Tran et al. (2022) further found that implementing various safety measures in order to ensure that cyber-attacks do not harm the organisation requires significant cost. Eventually, it costs significantly to the organisation and eventually increases the operational cost.

Thus, these are certain major impacts of the cyber security risk on the aviation industry.

2.6 Cybersecurity strategies implemented in aviation

The above section of this literature review informs about various risks as well as their impact on the aviation industry. Therefore, it is noted by Habler et al. (2023) that it is important for the industry as well as the organisations to implement strategic measures as these help them in addressing the cybersecurity threats in an effective way. The implementation of these strategies would not only help to eliminate such risks and address the cyber security attacks but can also help the organisation gain several nonfinancial benefits.

Secondly, it is required to conduct various assessments for managing the risks in an effective way. In this context, a regular risk evaluation is required to be implemented such that any potential threats within the system or the industry can be identified and appropriate measures can be implemented (Habler et al., 2023). It helps the industry to address the risks in an effective way,

which eventually allows the organisation to ensure that it does not hamper the effectiveness of the industry. In addition to these various techniques can be used for forecasting the threats and implementing certain measures such that any type of security attack can be eliminated in an effective way.

Further, it is identified that isolating the important systems can help in avoiding such threats from the industry (Lykou et al., 2020). In addition to this, if the network is segmented in an effective way it will help to minimise the overall impact of the threat and minimise the possibility of the threat on the industry as well as organisations. In addition to this, it is also important to implement highly developed security technology that can help encrypt the data and safeguard the important information of the industry as well as the organisation (Khandker et al., 2022). In this regard, it can be said that it can help organisations as well as the industry to protect crucial information from any kind of unauthorised access. Apart from that it is also important for industry as well as organisations to implement various systems that can help in monitoring the activities, especially any kind of suspicious activities and eventually prevent such activities from negatively affecting the industry or organisation.

Further, it is identified that it is important to implement an incident report along with an effective response plan (James, 2023). It will help to ensure that effective actions are implemented when there is any kind of cyber-attack in the industry or the organisation. In addition to this various cyber security actions as well as measures are required to be implemented such that any cyber-attack as well as their potential action can be evaluated and then implemented such that the overall impact of such risks can be minimised (Onwubiko, 2022).

Apart from this, it is also important for organisations to ensure that all their employees are properly trained and have effective awareness regarding cyber security measures and their risks. In this context, they are required to provide significant training on addressing any kind of cyber security risks within the organisation (Habler et al., 2022). In addition to this, they are also required to provide efficient training on identifying the risks and implementing effective measures to address them in an effective way.

2.7 Challenges faced by the aviation industry in implementing cybersecurity measures

With respect to the challenges faced by the aviation industry when the implementation of effective cyber security measures is taken into consideration, it is found that there are complicated systems in the industry that face huge difficulty in terms of updating them or securing them with the highly advanced technologies being used in the present day (Stansbury et al., 2022). When interconnectivity is taken into consideration it is found to be one of the greatest challenges as there is a significant level of interconnectivity among different stakeholders. It is also found that the operational activities of this industry are interconnected, which eventually enhances the overall potential of cyber security attacks (Vu and Rajaratnam, 2022). Apart from that it is also identified that there are several regulatory challenges that need to be addressed by the industry. It is also found that different countries have different legislative requirements that are required for the airline industry for all the countries to follow. However, some of the countries have different regulations and are quite complicated. Following them in an effective way becomes a significant challenge for the industry as well as organisations operating in this particular industry.

Cost as well as resources are another major challenge that is being faced by the aviation industry when it comes to implementing effective cyber security measures (Alghamdi et al., 2024). In order to implement cyber security measures, requires a significant amount of resources as well as the cost for implementing these measures. It is also found that the organisation or the industry may face several difficulties in allocating resources or getting funds (Babu et al., 2023). Therefore, eventually creates a major challenge for the organisation as well as the industry to implement such measures. In addition to this, the speed of technological advancement in the country is another major challenge. It is identified by Galkovskaya and Volos (2022) that some countries do not have efficiency in implementing and developing the technology at a rapid speed. However, they implement such technology at a lower speed which creates a significant gap in terms of security (Scholl et al., 2023). Therefore, it is a major challenge for the aviation industry across the world in terms of addressing cybersecurity risks when it comes to implementing effective cyber security measures.

The supply chain challenge is another major challenge that is being faced by the aviation industry in terms of implementing effective cyber security measures. It is identified that this particular industry is majorly dependent on external vendors (Taylor and Steven Cotter, 2020). These vendors provide products as well as services to the end consumers. Therefore, while implementing any cyber security measures there could be an instance that these suppliers may pose certain risks to the industry as they may not be ready for such changes and may resist them (Mäurer et al., 2022). Eventually, it creates a significant gap in the implementation of cyber security measures.

2.8 Importance of regulatory frameworks concerning cybersecurity in aviation

According to Faruk et al. (2021), the aviation industry is bound to follow certain regulations included in regulatory frameworks which include several guidelines as well as regulations that help them to carry out their overall activities in such a way that the industry can ensure that its operational activities are being carried out in an effective as well as ethical and a legal way. Some of the major reasons that determine the importance of the regulatory framework standards that are required to be followed by the industry are as follows:

First and foremost, it is identified that implementing and following effective regulations in the aviation industry helps enhance the overall safety of the consumers and also ensures that effective security practices are implemented within the industry (Kayan et al., 2022). In this context, it can be said that this framework ensures that strict measures are taken into consideration such that any incidence of cyber-attacks can be eliminated. On the other hand, it is also important to ensure that passengers' data are safeguarded. The implementation of these measures in the aviation industry allows the private as well as confidential data of the customers along with the company to be safeguarded and used wisely, to eliminate any cyber-attacks. Furthermore, Freeman and Garcia, 2021) found that an effective regulatory framework allows organisations to protect the data and maintain the privacy of their stakeholders. The implementation of a regulatory framework is very important in safeguarding the private information and confidential data of the organisation. It helps the organisation to ensure that the integrity of the data is maintained and safeguarded in an effective way. Apart from that it also helps the organisation to maintain a trustworthy relationship with their customers (Beckner, 2022). If the organisation is found to be safeguarding the private information of the customers in an effective way it eventually allows the customers to trust that particular

organisation and maintain a long-term relationship with that organisation eventually building loyalty.

Kaushik and Thakur (2022) noted that the regulatory frameworks in the industry allow the organisation to carry out their actions as well as activities in a proper way. Additionally, Lu and Wu (2022) found that carrying out these activities uniformly ensures that all organisations in the industry implement a consistent approach such that any issues related to cyber security can be eliminated in an effective way Apart from that, the implementation of effective regulatory frameworks also allows the organisations to carry out best practices such that any challenges in the industry can be eliminated and effective measures can be implemented for eliminating such challenges and issues. Furthermore (Canito et al., 2020) articulate that effective implementation of the regulatory framework also allows the organisation to ensure that the risks are identified in an effective way and mitigated at the earliest before they become harmful to the overall organisation. It also helps the organisation to forecast potential challenges and implement instant mitigating actions such that no further harm is caused to the organisation.

2.9 Theoretical Framework

Risk management framework: This particular framework has several guidelines and policies that are required to be followed by the organisation in order to determine the risk and then implement effective strategies to eliminate those risks (Esteki et al., 2020). In the data analysis section, this framework is used for analysing the strategies implemented by the organisations in the aviation industry for identifying the risks and mitigating them, which further helps in presenting the analysis of the strategies in an effective way.

Technology acceptance model: According to this model, it is a system that deals with different information and helps in providing information on how the technology would be accepted by the users and provide benefits to the users (Sagnier et al., 2020). This model is implemented in this study to inform the effectiveness of technologies being implemented by the organisations and provide information on how they benefit the customers.

2.10 Summary

On an overall basis, it is summarised that this chapter plays a very important role in the study. It helps in informing various information on different literature on the research topic. This chapter has helped in enhancing the overall knowledge of the research topic. Additionally, the case studies as well as the theoretical model demonstrate the practical efficiency of the research topic.

Chapter 3: Research Methodology

3.1 Introduction

The aim of this study focuses on gaining an inclusive understanding of the impact of “cyber security attacks” on the performance of “airline companies”, specifically focusing on “European Airlines”. Based on the aim of this study, the previous chapter has been prepared. In the previous chapter, various literature on the current research topic has been reviewed. Based on critical knowledge gained from the literature review, the researcher is now able to structure the implemented research methodologies. According to Sileyew (2019), a research methodology is referred to as a set of processes as well as procedures carried out to collect data and conduct a systematic study. With the help of a sound and appropriate research methodology, researchers can manage and compare different methods and implement the most effective method for the current research study. In this chapter, the researcher has emphasised different procedures taken into consideration, while addressing the stated “research questions”, “aim” as well as “objectives”. To make this study more informative and highly qualitative, selected research procedures are justified, which makes this chapter more effective.

3.2 Research Onion

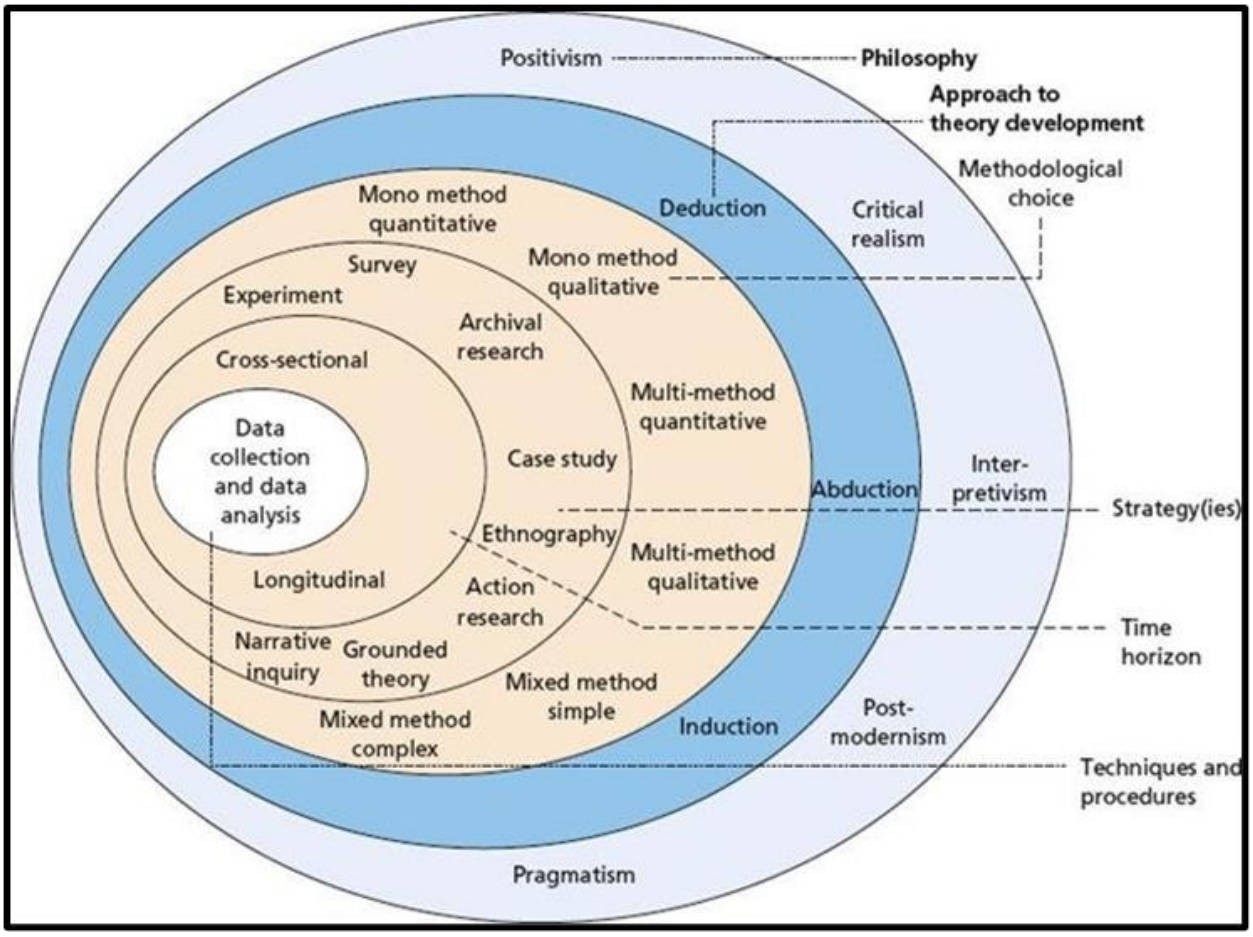

Figure 3.1: Research onion

(Source: Mbedzi et al., 2020)

"Research onion" is one of the most critical aspects when any research methodology is taken into consideration. A research onion is used to explain several types of research methods that can be implemented by the researcher to guide him/her throughout his/her research journey (Mbedzi et al., 2020). The given figure *(figure 3.1)* demonstrates the "research onion" proposed by "Saunders". It is helpful in describing several methods considered while developing an appropriate methodology for a particular study. However, Alturki (2021) stated that the research onion proposed by Saunders is not always perfect, but it acts as a helpful tool for thinking comprehensively when the methodology is considered. On an overall basis, research onion is crucial as it helps the researcher to understand the decisions taken with respect to research

methodology as well as design. With the help of this research onion, the researcher is able to proceed with the research study in a systematic way. It also allowed the researcher in guiding the further steps required to be implemented while carrying out the planned research methodology. This research onion has helped the researcher in designing the current methodology for this study.

3.3 Research Philosophy

The previous section of this chapter informs about the research onion. Based on this research onion, the research philosophy section is prepared, which further helps in preparing and providing information on "research philosophy". "Research philosophy" is also known as a collection of beliefs that assists in supervising the overall execution of the study (Lim, 2023). The research onion *(figure 3.1)* determines the "research philosophy" in the topmost layer. It also informs that research philosophy is of five types, which are "positivism", "critical realism", "interpretivism", "post-modernism", and "pragmatism". According to Mauthner (2020), research philosophies focus on theory development regarding the nature of the research topic that is being studied and provide information on how knowledge and information regarding the research topic are produced as well as justified. Research philosophy is associated with the development of knowledge. It is a crucial aspect of research philosophy because while stating the philosophies, different researchers have varied assumptions and considerations regarding the attributes of truth as well as knowledge, and implementing the appropriate philosophy plays a critical role in understanding those assumptions. Based on the types of research philosophies presented in the given figure *(figure 3.1)*, the researcher has selected the ***"interpretivism research philosophy"***.

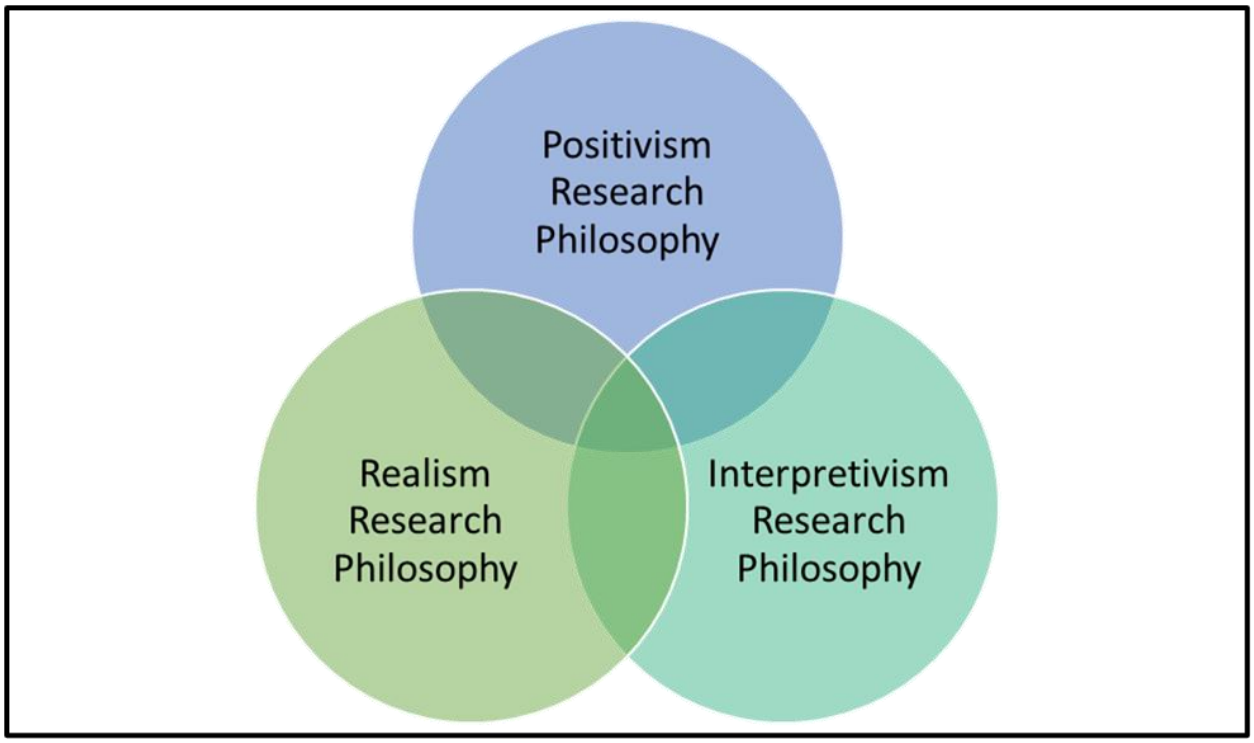

Figure 3.2: Major types of research philosophy

(Source: Mauthner, 2020)

Interpretivism research philosophy includes a process where the researcher interprets various elements of the study. Thus, Bonache and Festing (2020) stated that researchers implementing interpretivism philosophy consider that reality can only be accessed through social aspects such as instruments, shared meanings, languages as well as consciousness. Additionally, the interpretivism philosophy mainly focuses on qualitative analysis.

Justification: The researcher has selected "interpretivism philosophy" in this study as it has helped the researcher to have a comprehensive understanding of subjective aspects as well as experiences concerning the people from the aviation industry. It has further allowed the researcher to gain significant information on the way threats from cybersecurity in the aviation industry are recognised and further managed to ensure these threats do not impact the industry adversely. Matta (2022) opined that "interpretivism philosophy" emphasises the meanings of several aspects at an individual level, resulting in the high validity of the findings. Therefore, concerning this present study, "interpretivism philosophy" has permitted the researcher to ensure the validity of the study

is not compromised. I consider myself as an interpretivist because I have taken a comprehensive approach for analysing the collected data on the impact of "cyber security attacks" on the "aviation industry".

3.4 Research Approach

The above section of research methodology informs about the research philosophy. In this section, the research approach is emphasised. With respect to the stated research onion, the research approach is in the second layer of the onion *(refer to Figure 3.1)*. According to Taherdoost (2022), the research approach is defined as a "set of plans and procedures" for conducting out a "research study" that covers significant steps from conventions regarding the research topic to stating comprehensive information on data collection, interpretation as well as analysis methods. Therefore, the research approach is found to be segregated into three different types, which are (a) "inductive" (b) "deductive" and (c) "abductive" (Taherdoost, 2022).

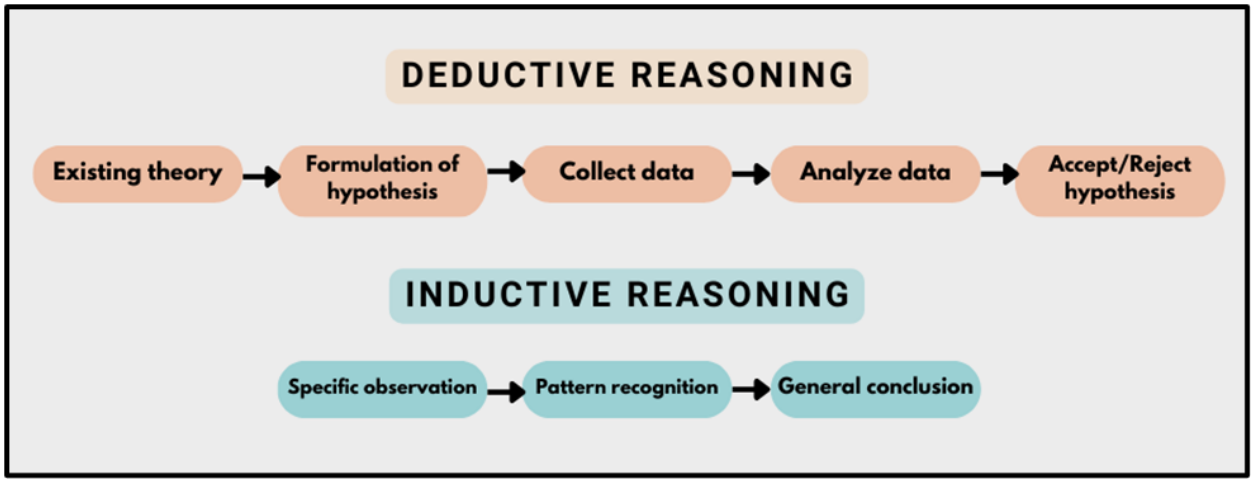

Figure 3.3 Deductive vs inductive approach

(Source: Taherdoost, 2022)

With respect to the given types of research approaches, the difference present among these approaches is based on the relevance of the hypotheses stated in the study. However, differences in hypotheses can only be considered for the "deductive approach" and "inductive approach". In this context, Kankam (2020) opined that the "deductive research approach" is useful in testing the

validity of assumptions and considerations taken within a study. On the other hand, the “inductive research approach” is useful in providing significant contributions to the development of the latest theories as well as generalisations. Apart from this, the “abductive research approach” initiates with puzzles as well as surprising information and the entire study is further carried out while focusing on the justification and explanation of these facts as well as puzzles identified in the research study (Vaughn and Jacquez, 2020). Based on the definitions as well as the selected philosophy, the researcher has taken a qualitative approach in this study. Thence, the researcher has considered the “inductive research approach” for this present study.

Justification: "Inductive approach" is selected for this present study. In the context of the research approach, Lahiri, 2023 found that it mainly emphasizes generating theories while implementing a procedural collection as well as analysis of data. When the present research topic is taken into consideration, the inductive approach has helped the researcher to collect substantial data regarding incidents related to cybersecurity, perceptions as well as responses from the stakeholders, which has further helped in developing new theories about cybersecurity risks as well as their impacts. Considering, the current research study, the inductive research approach has allowed the researcher to develop theories on the basis of the collected empirical data. It further contributed to providing assistance in gaining crucial information on several aspects related to cybersecurity risks as well as their impact on the business activities of the aviation industry.

3.5 Research Design

The research approach and philosophy indicate that the researcher has implemented a qualitative approach to collecting data. Thus, in this regard, the researcher is further required to select the research design in an effective way. With reference to the "research design", Ranganathan (2019) defined it as one of the most important strategic frameworks implemented by the researcher to ensure that the overall research objectives are accomplished in an effective way. Banerjee et al. (2022) also opined that research design focuses on a planned structure allowing the researcher to carry out the study effectively and eliminating its potential impact on different activities of the research study. Therefore, it can be said that an effective research design, the researcher is able to carry out a structured approach to analyse as well as interpret the data collected for the study. In the context of the research design, there are generally three major types of research design, which

are (a) “experimental”, (b) “exploratory”, and (c) “descriptive”. Here, the researcher has carefully chosen a "descriptive research design". According to Aggarwal and Ranganathan (2019), "descriptive design" specifically concentrates on collecting information concerning the research topic, which allows the researcher to describe the entire research topic effectively.

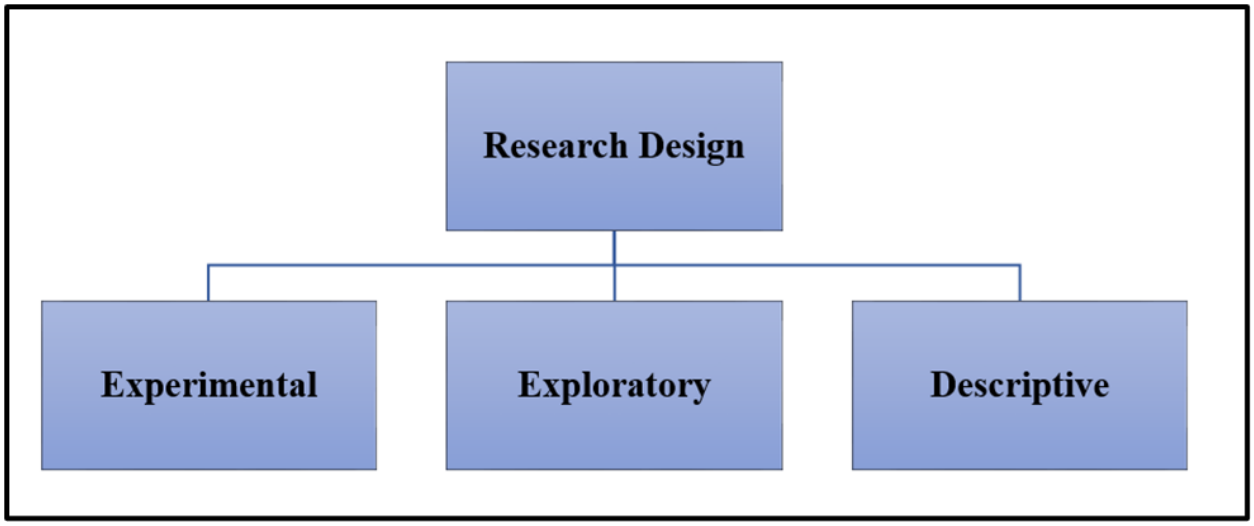

Figure 3.4: Types of research design

(Source: Edmonds and Kennedy, 2017)

Justification: The researcher has selected a descriptive design for this research study because this design allows the researcher to portray the collected data regarding cybersecurity risks in an accurate way while taking several aspects and characteristics of risks. Edmonds and Kennedy (2017) stated that "descriptive design" is helpful in understanding the overall scope of the risks imposed regarding cybersecurity and the way it impacts the aviation industry. Further, when this research study is considered, "descriptive design" helps in providing information on the types of risks associated with cybersecurity and eventually provides detailed information on the research topic.

3.6 Research Method

Research method is the most important aspect of a research methodology. Scholtz et al. (2020) defined research method as the crucial strategies, techniques as well as processes taken into consideration for collecting data such that the topic can be understood in a better way. When the

research method is taken into consideration, there are generally two major types of research methods. These are (i) "primary research" and the other one is (ii) "secondary method". In a primary study, the researcher himself collected data for the study directly from the participants. On the other hand, secondary research is referred to as the method used for summarising and analysing the overall data as well as literature, which has been already collected by others (Osuagwu et al., 2020). Both of these research types are crucial with respect to the concerning research topic. In the context of the selected research topic, the researcher has implemented a mixed methods approach.

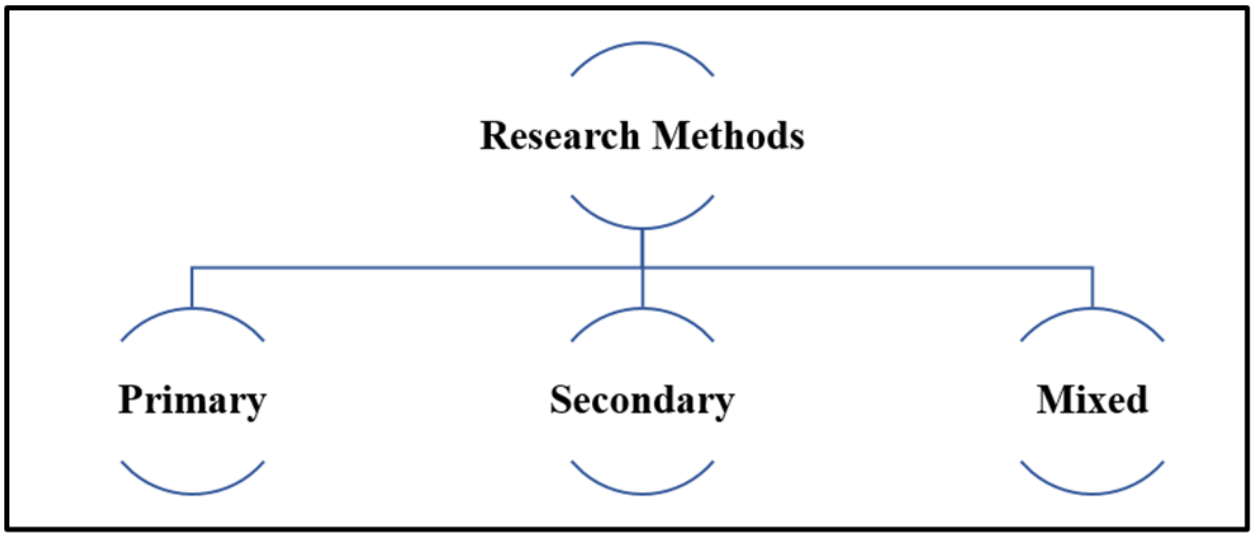

Figure 3.5: Types of research methods

(Source: Osuagwu et al., 2020)

Justification: With regard to the present study, the researcher has selected “mixed methods” for this present study. In the context of the mixed methods, it can be said that it involves both, “primary” as well as “secondary methods” for carrying out the study. With reference to the current research study, the implementation of a mixed method approach allows the researcher to collect first-hand information from the stakeholders, along with secondary data information about the cybersecurity risks impacting the aviation industry. Therefore, it can be said that with the help of the primary method, the researcher has been able to collect crucial information on cybersecurity risks directly from the stakeholders. Apart from this, the researcher also needs to collect some industry data, therefore, in this context, a secondary method is implemented. Therefore, in order

to carry out this present study in an effective way and address the stated research objectives, mixed methods allowed the researcher to accomplish this study thereby addressing all the major objectives as well as the overall aim of the study.

3.7 Data Collection Strategy

The researcher performed a mixed method approach for carrying out the research study in an effective way. When the primary data is taken into consideration, the researcher has taken interviews with various stakeholders of the aviation industry into consideration. With the help of interviews, the researcher is able to collect qualitative data for the study. Additionally, interviews can help the researcher in gathering comprehensive and detailed information that is further utilised for accomplishing the overall aim and objectives of the study. The researcher has selected "semi-structured interview" for collecting data because it allows "two-way communication" with "open-ended questionnaire" and the interviewer can ask several questions with respect to the response provided by the interviewee that further allows to structure the final outcome of the study. To carry out an interview five employees from aviation industry are considered. They were 3 males and 2 female. These employees are in managerial & consultant roles specifically handling IT related activities within the organisation. According to Rouder et al. (2021), an "open-ended questionnaire" can have several answers, on the basis of the experiences of the responder. It further helps the researcher to collect detailed information with respect to the asked question and the research topic. Apart from this, the researcher has also focused on some secondary sources for collecting information on the aviation business and industry. In this regard, various secondary sources such as industry reports, and several case studies available on the internet have been considered.

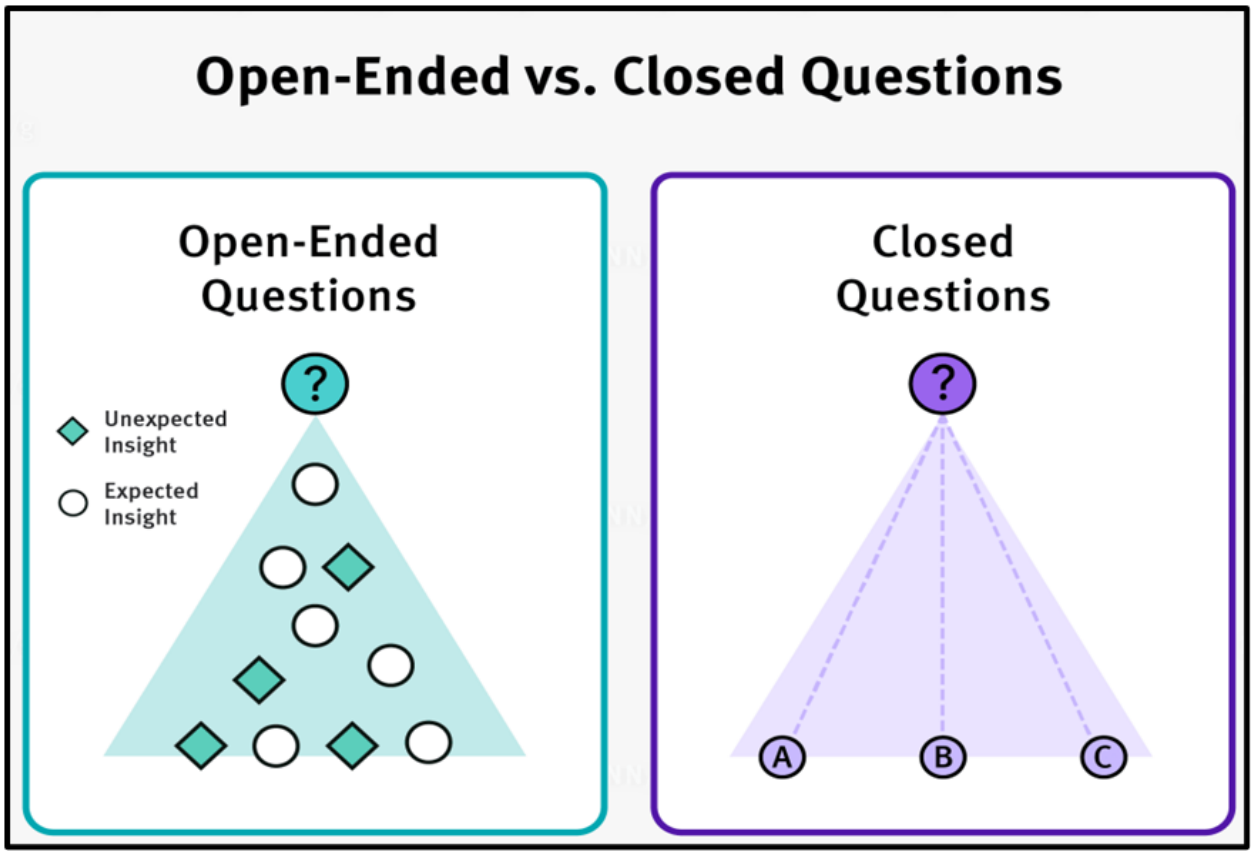

Figure 3.6: Open-ended questionnaire vs. close-ended questionnaire

(Source: Rouder et al., 2021)

Justification: With respect to the selected strategies for data collection, an open-ended questionnaire as well as secondary sources such as industry reports and case studies has been taken into consideration. "Open-ended questionnaire" allows the respondent to provide the response in detail, eventually promoting a "two-way discussion". Unlike "close-ended questionnaire", where the respondents have limited choices for a particular question. Therefore, assisting the researcher in accomplishing the interpretivist philosophy in the study. As, this philosophy requires comprehensive understanding about the research topic. Thus, implementing "open-ended questionnaire" helps in promoting such comprehensive analysis for the study. In regard to these sources, it can be said that these sources allow the researcher to collect comprehensive information regarding the research topic. These sources are further effective in terms of collecting data as these sources allow the researcher to collect quality data for the study, which eventually helps in enhancing the overall study. The interview is also carried out with the airline professionals such

as “IT Consultants” “Information Security Consultants”, “Crew and Logistics Manager”, “IT manager” and other professionals from airline industry. The main exclusion criteria for selecting the respondent are their “experience” within the industry. The personnel having an experience of more than five years are “included” in this study.

3.8 Sampling Strategy

Whenever any study is taken into consideration, it is important for the researcher to collect data from an effective sample. According to Turner (2020), the sample is extracted from a particular population because it helps in representing the entire population. Also, these populations are generally high in number, due to which it extremely difficult for the researcher to collect data from each participant present in the population. Therefore, a sample is drawn from the population such that the data collection process can be carried out smoothly. There are generally two major types of “sampling strategies” (A) “Probability sampling” and (B) “Non-probability sampling” (Berndt, 2020). With respect to “probability sampling”, the “probability” of a “sample” getting selected from the entire “population” is equal. It also allows for better findings in terms of quality, as there are fewer chances of bias while selecting the sample. On the other hand, in “non-probability sampling”, the “probability” of selecting a “sample” is not justified, and the researcher selects the sample on the basis of convenience. Additionally, it is helpful in saving time and can be implemented quickly. However, the samples obtained from this sampling technique have a higher probability of bias. Therefore, in this regard, the researcher has selected probability sampling.

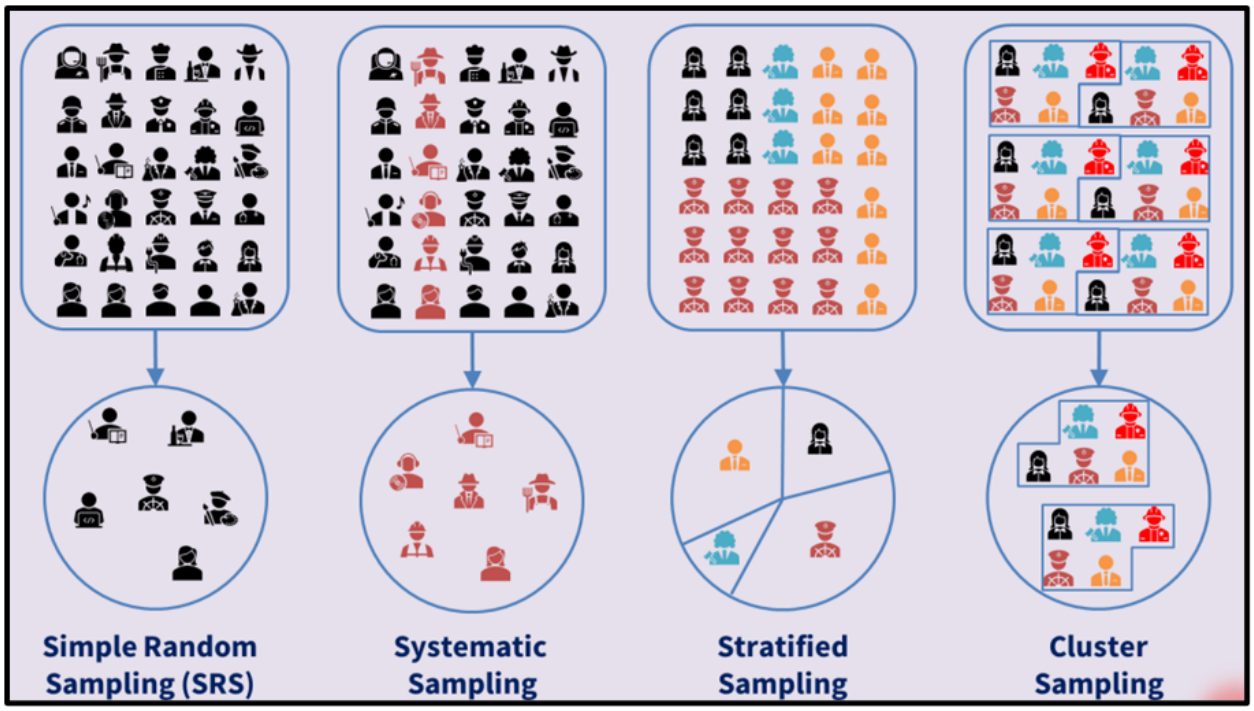

Figure 3.7: Types of probability sampling

(Source: Berndt, 2020)

Justification: In the context of "random sampling", it has allowed the researcher to remain unbiased while selecting the sample for the study. In "random sampling", each item in the population has an "equal opportunity" to be selected as a sample (Cash et al., 2022). Thus, it eliminates the instances of bias. Therefore, it can be said that it allows the researcher to carry out the study independently and ensure that the data is not affected by his/her decisions and perspectives.

3.9 Data Analysis Method

Data analysis is one of the most crucial aspects of a research study. With respect to the above sections of this chapter, it has been identified that the researcher focuses on collecting qualitative data for the study. Therefore, in this context, it can be said that the researcher is required to conduct a thematic analysis on the basis of the collected data. The researcher has implemented a primary and secondary method for collecting data. However, the nature of collected data is "qualitative", therefore appropriate methods such as "interview" and "secondary sources" are considered for

collecting the data. Both of these methods has helped the researcher to gain “qualitative data” for the study. The data collected from the interviews will be transcribed and further analysed. In order to analyse the data, the researcher has implemented a “thematic analysis”. In the context of this method for analysing the data, it can be further said that while analysis, the researcher needs to prepare several themes. Thus, in this regard, various themes are prepared while focusing on the “research objectives” as well as “research questions”.

The data collected from “primary and secondary” sources are firstly grouped in terms of the questions asked from the respondents. Then, the findings of the data is further prepared into themes. Once, the themes are prepared, the researcher further analyses those, while taking the “objectives” as well as “questions” of the research study into consideration. Thus, allowing the researcher to analyse the collected data in an effective way and provide conclusive results for the study.

3.10 Ethical Considerations

In order to ensure that the researcher carries out the study ethically, a few ethical considerations have been followed. Some of these considerations are:

- Firstly, the researcher needs has consent from the university before starting with the study.
- While collecting data, the researcher has ensured that informed consent is gained from the participants. An informed consent is a process of taking consent from the respondent by providing all the related information regarding the interview.
- The researcher has ensured that the participants are not forced to give responses. In this context, the participants were allowed to leave the interview, at any moment they felt discomfort or when they did not want to continue with the interview. When, the respondents decide to leave the interview, they are not asked any questions about why do they want to leave, they can just opt out from the interview, whenever they want.
- The researcher ensured that all the secondary sources were duly acknowledged and cited.
- The researcher also focused on ensuring that no data manipulation activities are endorsed. In order to ensure no data manipulation is done, the researcher ensued that the data is presented as it is collected from the original source. The results are presented in the exact way they have been provided by the respondents.

- Above all, the researcher also ensured to inform the participants that they may leave the process, whenever they wanted.

These are some of the major “ethical considerations” ensured by the researcher that has been followed in this study, which is to determine the impact of cybersecurity risks on the aviation business.

3.11 Summary

It is concluded that the researcher has significantly taken assistance from the "research onion". This "research onion" has helped the researcher in framing this chapter. With respect to the current study, the researcher has focused on implementing an "interpretivism philosophy", which informs that the researcher needs to carry out a qualitative study further. In this regard, the researcher also selected an "inductive approach", which helped the researcher to generate new theories on the basis of the empirical data collected concerning the risks associated with cybersecurity in the aviation industry. Further, when the research design is taken into consideration, the researcher has opted for a “descriptive design” for the present study. With the help of “descriptive design”, the researcher is able to present the findings in an effective way. Further, this chapter also informs that the researcher has implemented a "mixed method" for meeting the “research objectives” of the study. In this regard, the researcher further collected data by carrying out interviews with the stakeholders such as (IT staff, crew members, and customers) to collect efficient primary information with respect to the impact of cybersecurity risks. After collecting data, it is realised that the researcher has collected qualitative data. Therefore, the researcher has focused on analysing data through thematic analysis. Above all, it is also concluded that the data collection process is effectively managed because of the probability sampling strategy. However, while collecting data and conducting this study, the researcher focused on following all the major “ethical considerations”.

Chapter 4: Data Findings and Analysis

4.1 Chapter Introduction

The previous chapter informs about the "research methodology" taken into consideration for accomplishing the stated "aim and objectives" along with the identified "research questions". In the previous chapter, it is stated that a "primary method" along with a "secondary method" is implemented to accumulate data for this study. For gathering data for this study, a "semi-structured interview" is considered for gathering "primary data" and various "secondary sources" such as "industry reports", and several "case studies". In this chapter, the data collected from these sources are analysed to gain an informative and structured meaning from them. This chapter consists of the findings and their analysis. This chapter provides crucial information regarding different companies and their encounter with "cyber security breach" incidents.

4.2 Data Findings

4.2.1 Interview Transcripts

Interview Transcript for Question 1: ***Can you describe any instance associated with the issue of "cyber security attack"?***

Respondent 1	*"Yes! There was a breach in the security system of outline, where the "cyber attackers" have muddled through our system and gained access to our confidential information such as passengers' data."*
Respondent 2	*"In recent years, we were exposed to a ransomware attack, where our vital information was acquired by the attackers, and they commanded a significant amount as a ransom for releasing back the data to us".*
Respondent 3	*"Two years back, our company faced a breach, where some of the employees received a fake email from our official site, which demanded some critical*

	information regarding our organisation".
Respondent 4	*"In the year 2022, our organisation encountered a DDoS issue, which led our website to malfunction for several hours".*
Respondent 5	*"We faced a breach, where crucial information regarding our loyal customers and others were accessed by the attackers".*

Analysis: In the context of this interview question, the main intention behind this question is to determine the different incidents of "cyber-attacks" faced by the "airline companies". With respect to the data and information collected from the respondents, it was found that the airline companies faced severe incidents regarding the "cyber security attacks". The respondents stated that the attackers have severely disrupted their overall "operational activities". The companies have faced severe incidents of "ransomware attack", "phishing attack", "malware attack", and "DDoS attack". These severe negative attacks have significantly disrupted the overall operability of airline companies. In addition to this, the companies also encountered a breach in their security system, which caused severe issues and challenges to the companies.

Interview Transcript for Question 2: How did this incident impact the overall airline?

Respondent 1	*"This incident has imposed a negative impact on our operability. Customers seem losing trust in us eventually reducing our annual revenue."*
Respondent 2	*"It impacted negatively on our operations, finances and even customers. We found that our relationship with the customers weakened after this incident".*
Respondent 3	*"It negatively affected our organisation, where we had lost severe data about our company and customers. Additionally, it disturbed the entire operability of our organisation and imposed severe financial costs".*

Respondent 4	*"It impacted our overall strategy and imposed a significant impact on our relationship with our customers and employees".*
Respondent 5	*"This incident led our company to face severe financial losses and disturbed our entire operational capabilities. Our relationship with our customers was also negatively affected".*

Analysis: On the basis of this question, the main intention behind this question is to determine the impact of the incident on the organisation. With respect to the collected information from the interview, it was found that these "cyber security attacks" imposed a significant negative impact on the overall performance as well as operations of the airline companies. Through this question, the researcher was able to determine the overall aftermath of the "cyber security breach" incident in the organisation. In the context of the collected responses, it is found that the incidents of breaches in "cyber security" led the organisations to face a negative impact on an overall basis, considering the "performance", "financial resources", as well as "reputation in the industry". Therefore, it can be said that these incidents of "cyber security" created a significant negative impact on the overall organisation.

Interview Transcript for Question 3: What measures are implemented by your airline to address such negative incidents?

Respondent 1	*"We implemented stringent metrics for ascertaining malicious activities earlier. Additionally, we increased the security of our authentication along with regular assessments of the overall scenario for determining risks and threats"*
Respondent 2	*"We have increased the security of our database, along with ensured that we have a secured security system and implemented a quick response system for addressing such incidents in the future".*

Respondent 3	*"We have provided training to all the employees to determine such incidents and the methods to encounter those. We always try to inform our customers to ensure that they are aware of such incidents. Apart from these, we have incorporated a robust system and team (SOC – Security Operations Centre) for identifying these incidents at the earliest".*
Respondent 4	*"We have implemented a robust security framework for safeguarding our database and systems. It helps us in securing data and eliminating incidents of data breach".*
Respondent 5	*"We have implemented an inclusive framework for overseeing and managing critical information. Additionally, we also ensured that a continuous development framework is in place".*

Analysis: On the basis of the interview, the interviewer asked this question to determine different measures implemented by the organisations such that they can address the incident of "cyber security" that impacted their organisation adversely. Therefore, with respect to the responses, it is found that the companies have implemented varied measures for addressing such incidents. It has allowed the organisation to ensure that they get protection from such incidents in the future. The measures that were implemented by the organisations were "incorporating a strict and significant framework" for managing as well as supervising the overall operational tasks within the organisation, which helps the organisation in limiting the occurrence of such incidents. Additionally, it was also reported that the organisations implemented a significant development framework within the organisation for determining the risks and planning strategies for addressing such risks within an organisation. In addition to this, various training programs are incorporated for the employees which helps in enhancing their skills in determining the risks within the organisation. Thus, assisting the companies in achieving an effective framework for addressing such incidents in the future.

Interview Transcript for Question 4: Were those measures effective in addressing such incidents?

Respondent 1	*"Yes, the methods that we have implemented have proven to be effective. These methods have allowed us to address such negative incidents effectively. Additionally, the implemented measures have allowed in mitigating such incidents".*
Respondent 2	*"Yes, the measures that the company has implemented, are found to be effective. However, according to my perception, I assume that these measures can be further improved."*
Respondent 3	*"With respect to the measures that have been implemented by the company are found to be effective and sound. These measures have helped the organisation in mitigating the negative incidents associated with cyber security attacks".*
Respondent 4	*"In the context of the measures implemented within our organisation, I would like to inform you that yes, these measures are effective in addressing the incidents associated with data breach and helped us in eliminating further incidents in the organisation".*
Respondent 5	*"Yes, the implemented measures have proven to be effective in terms of addressing such negative incidents within the company. However, I found that we need to emphasise providing training to our employees to enhance the effectiveness of these measures implemented within the organisation".*

Analysis: In the context of this interview question, it can be said that this question helps to provide information regarding the effectiveness of the measures implemented for addressing the incidents of "cyber security attacks" in the airline companies. On the basis of the collected responses, it has been found that the strategies implemented by the companies allow the organisations to gain

positive and desirable results. The respondents have further informed that implementation of security measures have helped the companies in limiting the incidents of cyber attacks in the company. However, one of the respondent have stated that in spite of implementing effective strategies the company had faced certain challenges in terms of their implementation.

Interview Transcript for Question 5: Have you encountered any issues while incorporating these measures?

Respondent 1	*"Yes, we have faced certain challenges while implementing these measures. First, we found that the employees were reluctant to implement the new methods of maintaining security for the database. Secondly, the incorporation of security measures was a complex method and also a tedious method.*
Respondent 2	*"Yes, we have faced significant challenges while incorporating the aforementioned strategies. Firstly, a limited budget is a significant challenge that we faced. Second, the company also faced challenges in terms of meeting legal obligations".*
Respondent 3	*"We faced a major issue while meeting the legal obligations while incorporating security measures and training sessions for the employees. Incorporation of such measures required significant financial resources, which created a major challenge for us".*
Respondent 4	*"Yes, we have encountered certain challenges while incorporating the mitigating measures for addressing the cyber security attacks in the company. In this regard, we have faced a major financial limitation. Further, we also faced a significant backlash from our existing employees as they had to shift to a new software for carrying out their organisational activities".*
Respondent 5	*"Yes, we have faced certain challenges. Firstly, we found that the employees*

	did not have sufficient skills to implement the mitigating measures. The organisation also struggled while minimising the gap between the safety of consumer data and user interface while utilising the framework".

Analysis: In the context of this interview question, it is analysed that this question mainly emphasises the issues being faced by companies, while they implement sound strategies for addressing and encountering the cybersecurity vulnerabilities. Therefore, in this regard, it is analysed from the responses that organisations face substantial challenge while incorporating such strategies in limiting the impacts of such risks. In this regard, the organisations faced an issue of limited "financial resources". Apart from this, "compliance as well as resistance" were the main challenges that impacted the incorporation of the strategies. Therefore, on an overall basis, it can be said that the strategies that were implemented to address the risks, also imposed significant challenges to the organisation.

4.2.2 Case studies

Case studies regarding the "cyber security challenge"

A few case studies have been considered in this dissertation. These are considered in this dissertation because it helps in informing real-life "cyber security challenges" faced by the airline companies. These case studies also help in determining the impact of such attacks on the organisations. Adding these case studies here, helped in analysing the findings from "primary and secondary data" for this dissertation. With respect to the cyber security challenges, it is identified that various organisations have faced several instances of cyber security challenges. In this context, some of the real-time case scenarios have been assessed as follows:

British Airways: With respect to this organisation, a significant issue of data breach was detected in the year 2018. Due to this incident, the organisation suffered significantly in terms of financial costs and a huge number of customers also suffered due to this incident (BBC, 2020). The main reason for this cyber-attack was due to the security concerns in the website as well as the application of the company. There was a significant attack on the supply chain of the company due to which the services of the organisation were compromised (BBC, 2020). As a result of this attack,

it was found that various personal information of the customers was stolen by the attackers, which also included the financial data of the consumers. The company faced severe financial loss of £20m for the loss of data and around 400,000 customers were affected due to this breach (BBC, 2020). Thus, on the basis of this challenge, a few lessons were learned, which state that the company should focus on its supply chain which would help in carrying out the audit of its suppliers and eventually determine the challenges involved in the supply chain, such that effective measures could have been taken.

Polish Airlines: The airline suffered a major attack in the year 2015. Due to this attack, it was found that the ground operations of the company were compromised. As a result, various flights were cancelled and around 1400 passengers faced critical challenges (Industrial Cybersecurity Pulse, 2022). In the context of this attack, it was identified that the hackers mainly attacked the systems due to which the flight schedules were disturbed, and the flights were rescheduled and cancelled, causing trouble to the passengers (Industrial Cybersecurity Pulse, 2022). It is found that this attack took place due to Denial of Service with respect to the flight plan system of the company (CIAB,2024). With respect to this attack, it was found that various lessons were learned in terms of implementing a resilient system such that backup operations can be implemented to avoid any type of cyber-attacks. Apart from this, a rapid response is required to be implemented such that any such issues can be handled in a shorter period without much loss.

4.3 Data Analysis

Thematic Analysis:

Theme 1: Aftermath of cyber security issues on the airline companies

With respect to the "interviews" as well as "secondary data" collected for this study, it has been found that the cyber security issues impose a significant negative impact on the organisations. Based on the collected responses, one of the respondents stated that due to this incident, customers lost trust with the company, eventually weakening the relationship of the company with their customers. In this regard, it is also reported by Cremer et al. (2022) that "cyber security incidents" lead to severe commercial losses, along with significant damage to the reputation of an organisation and sometimes loss of trust among their customer base. With reference to the

determination of several aftermaths regarding the “cyber security issues”, various secondary sources are considered. Considering these sources, Ohrimenco and Cernei (2024) opined that due to the “cyber attacks”, organisations are significantly exposed to “financial losses”. With reference to these losses, the authors have further identified that there are certain “direct expenses” as well as “indirect expenses” associated with the losses of the company. In the context of this challenge, Lee (2020) added that organisations facing financial issues due to the “cyber security attacks” faced certain expenditures as they may be required to recruit professionals to address such incidents. In addition to this, the organisations also incur legal costs to prove the conviction of the identified breach within the organisation. In this regard, one of the respondents stated that “cyber security breaches” also disturbed the entire operability of the organisation, eventually posing significant expenses of the organisation. Williams et al. (2020) stated that airline companies are required to ensure that they comply with all the legislations and regulations concerning data safety and privacy of customers. If any of the regulations concerning these aspects are hampered, the organisation also have to face a significant amount as a fine for not complying with the stated regulations. Cains et al. (2020) also added that an organisation also need to compensate their customers if they are affected by any malfunctioning within the organisation. All these attract significant losses (financial) within the organisation.

Apart from the monetary expenses, the data collected from the interview also suggests that the companies are also found to be losing their image in the industry due to the breach and “cyber security issues” within the company. Mızrak (2023) reported that these challenges are enduring and have a substantial potential to adversely impact the organisation. In this regard, Durst et al. (2024) further opined that such incidents have attracted significant negative public interest, hampering their corporate identity. In this regard, it can be further said that such a negative image among the public delineates the organisation as erratic or inept when it comes to securing critical information, which also attracts oblivion. In addition to this, Palko et al. (2023) stated that such incidents also negatively impact the customers’ perspectives when it comes to securing critical information, which eventually impacts the relationship shared by the organisation with its customers. Hence, after such incidents it becomes very difficult to establish that position in the market or in the minds of the customers, eventually hampering the overall performance of the organisations.

Such incidents are reportedly found to be affecting the operability of an organisation. Meshkat and Miller (2022) found that such attacks severely influence the overall operating systems of the company. Firstly, the organisations have cancelled and impeded their flights due to glitches in their technical systems or any breach in the security system of the organisation. Additionally, organisations can also face a major challenge in managing their logistical aspects. Any negative incident due to a "cyber security issue" leads organisations to create significant disarray within the organisation, which further creates challenges in managing the overall aspects of an airline company, causing severe disarrangements. Due to such aspects, organisations face severe disturbances in their activities. Above all, such incidents mainly affect the organisation in terms of their "loss of critical information", which further leaves the organisation unprotected against such "cyber security issues".

Theme 2: Strategies for addressing cyber security issues

The above part of this analysis informs varied aftermath faced by the organisation. Therefore, in order to ensure that such incidents are not repeated, organisations tend to implement certain strategies. With respect to these strategies, primary data and various secondary sources are analysed to collect appropriate information. In the context of the strategies, participant one informed that their organisation has implemented stringent measures that helps them determine malicious activities. This participant also informed that regular evaluations are carried out that help them determine any threats. The second participant stated that the company enhances the security system of the database that help them determining any risks in the least possible time. Another respondent informed that several training sessions were conducted for up-skilling the skillsets of the employees. Other two respondents informed a similar response that their organisation ensure a strict framework for assessing and determining risks. Thus, the findings determine that the "airline companies" have implemented various different strategies such that the companies are ready to combat such "cyber security issues" in the future. Therefore, in this regard, it is found by Liu et al. (2022) that organisations have incorporated various technical methods for addressing the issues. In this regard, the organisations have incorporated technologies such as "firewalls", "encryption", and "multi-factor authentication" among others to address the challenges imposed due to "cyber security issues". These technical systems are helpful for organisations in ensuring that the systems of the organisation are not muddled through any

unidentified person or source. Such systems are helpful in determining any form of distrustful actions and eventually warning the organisation of any such actions. Organisations secure their systems as well as data through encodes. In this method of protecting the systems and data, the organisations are assured that their data cannot be accessed by anyone outside the organisation. Even if the data is accessed outside the organisation, it cannot be decoded without the availability of an accurate deciphering code (Woods and Seymour, 2023). Hence, it can be said that it helps organisations in addressing the negative impacts faced by them due to "cyber security issues". Further, it is also found that organisations utilise significant methods for authorising the authentication, which helps in providing higher security to the database of the organisation.

Apart from this, organisations are also found to be utilising several policies that help organisations ensure that they have safe systems. These further provide critical information on the way of storing as well as transferring critical information, which deals with segregating different information, providing control and retaining information and data (Shevchenko et al., 2023). It has also been found that these organisations prepare response plans for determining the overall process that needs to be incorporated when an organisation faces or encounters any "cyber attack". Further, the organisations are also found to be ensuring that they have strict regulations in terms of accessing the system as well as information stored in the systems (Stine et al., 2021). These allow the organisations to ensure that they are able to protect their systems as well as information.

In addition to this, Backman (2023) found that humans play a critical role in an organisation and they also have considerable constituents when "cyber security risks" are associated. Therefore, in this regard, it is important to ensure that they have the critical expertise and skills to eliminate such instances. In this context, Maalem et al. (2020) opined that the concerned workforce is provided with the required training on gaining information regarding these attacks and the expertise they can demonstrate to address these challenges. These allow the workforce to determine any such attacks within the organisations and offer critical opinions for enhancing the overall action on limiting the "cyber security attacks". Kandasamy et al. (2020) stated that training sessions also involved various mechanisms that help in safeguarding the overall security systems. These are some of the major strategies implemented by organisations that help address "cyber security issues" within the organisation.

Theme 3: Efficacy of measures implemented to address cyber security issues

With respect to the analysis done in the previous theme, it is identified that the organisations have implemented various strategies that help them in addressing "cyber security risks". These strategies are also found to be effective in terms of eliminating these issues. In the context of these strategies that have been implemented within the organisation, it is identified that these allow an organisation to determine any kind of security issue present in an organisation. It is opined by Eling et al. (2021) that if an organisation is able to determine such issues quickly it eventually allows the organisation to ensure that they do not have to face significant negative impacts or they can reduce the impact of such actions in an effective way. A similar response was given by the respondents in the interview that with the implementation of "cyber security measures" helped them achieve desired outcomes.

In addition to this it is also found that the measures implemented by the organisations are also effective in implementing certain preventions within the systems of an organisation to maintain security. These help in minimising the unsecured access to data or system of an organisation (Pandey et al., 2020). It eventually allows an organisation to ensure that the organisation is able to reduce the number of "cyber attacks" on its premises. Apart from that, it is also found that training are also provided to the workforce of an organisation for enhancing the skills of the current workforce (Saeed et al., 2023). Kadena and Gupi (2022) also added that providing required training on enhancing the skills as well as expertise of the workers allows an organisation to ensure that they are capable of detecting these unwanted incidents at the early stage and help the organisation in reducing the number of attacks within an organisation. The respondent three stated that with the help of training the company was able to enhance the skillsets of the workforce, eventually allowing the company to gain efficacious results. Thus, it can be correctly said that the strategies implemented by the organisations are effective in addressing the "cyber security attacks" and "risks".

Theme 4: Challenges faced while incorporating strategies to address cyber security issues

With respect to the above part of this analysis, it is found that the strategies implemented by the companies in addressing the "cyber security issues" can help in minimising the impact. Despite their efficacy, the strategies are found to be posing severe challenges to the organisations, in terms

of their incorporation. In this regard, Thakur (2024) stated that limited “financial resources” pose a severe threat while incorporating the “mitigating strategies” within the organisation. With reference to this challenge, it can be said that incorporating the latest technologies might require significant investment, which creates a major hurdle for the organisation.

In addition to this, “limited expertise” in terms of handling these advanced technical systems is also a major challenge for the organisation. In this context, Clarke and Martin (2024) stated that with the advancement in technologies, the workforce is also required to demonstrate significant expertise in handling these technologies, which becomes obsolete with the evolution in technical aspects. Similar findings were found while collecting information through surveys. Therefore, as a result, there could be an instance in which the organisation does not have the appropriate skills to ensure that they are able to work with the developed technologies. Cele and Kwenda (2024) added that accomplishing the required regulations is another challenge for the organisations while incorporating strategies in addressing the “cyber security challenges” within the organisation. It is found that organisations are required to ensure that they meet all the required regulations and legislations, which is a complex process, and eventually adds to the challenge of an organisation when it comes to the incorporation of strategies to deal with the “cyber security challenges”.

Apart from these, organisations can also face challenges in the form of resistance from the current workforce in terms of implementing strategies. Such resistance occurs due to limited information on the incorporated or planned strategies. Eling et al. (2021) added limited information concerning “cyber security challenges”, within an organisation, can cause an organisation to face significant challenges when it comes to the incorporation or implementation of the strategies. Therefore, as a result, the organisation must provide substantial information to the concerned stakeholders within the organisation such that they do not pose any resistance while incorporating the strategies for eliminating such challenges from the organisation.

These analyses mainly inform the information collected from secondary sources. However, a few instances inform the perception of the respondents considered for this study.

4.4 Chapter Summary

On the basis of this chapter, it is summarised that this chapter crucial information regarding the findings of this study. With respect to the findings, “interview transcripts” are used along with the “secondary sources” for collecting relevant and reliable information. This chapter informs the major challenges that an organisation suffers from “cyber security attacks”. Additionally, some strategies incorporated to address these attacks have also been analysed along with the challenges imposed by those strategies. At the end, this chapter ends with a final note on the overall findings that “cyber security attacks” impose an adverse impact on the entire “operability” of the organisation.

Chapter 5: Discussion

5.1 Chapter Introduction

The previous chapter focuses on the findings from the collected primary and secondary sources. With the help of primary and secondary data, this chapter is prepared. In this chapter, the overall findings from the “primary and secondary data” are discussed. This chapter enhances the overall quality of the findings and in turn this dissertation.

5.2 Discussion

On the basis of the entire analysis, it is analysed that “airline companies” are prone to significant “cyber-attacks”. These attacks impose a significant negative impact on their “performance”, “financial status”, “their relationship with the stakeholders” and most importantly their “status and image” in the market. Therefore, it becomes crucially important to eliminate all the instances of “cyber attacks” from these airline companies. In this context, it has been found from the primary analyses that the “cyber security attacks” are very severe, which imposes a significant adverse impact on the operations of the organisation. Various secondary sources have also found a similar impact on the overall operability of the organisations. Therefore, with reference to the collected information, this study informs that the “cyber security attacks” impose a negative impact on the organisation.

The “case studies” stated above informs about the adverse impact of these attacks. Along with these “case studies”, some “primary data” were also collected to determine the challenges poses by these “cyber-attacks”. With respect to the primary data, it has been found that the organisations have found several negative incidents related to the “cyber security breaches”. One of the respondent stated that their organisation encountered a DDoS issue, along with some security breaches in the systems. These incidents affected the organisations negatively and imposed several challenges against the companies. When the impacts are considered, the organisations faced severe negative impacts against their reputation, image, financial position and relationship with customers and stakeholders. Such incidents have also been explained in the case studies mentioned above.

Apart from negative impacts, the analyses stated above inform that the companies implement various “strategic measures” that allow them to mitigate negative impacts due to the “cyber security challenges”. These measures include “training sessions” for the employees, robust measures for addressing the “cyber security challenges”, enhancing the “security systems” of the company to ensure that critical information are safeguarded and secured. In the context of these measures, the analyses from secondary sources inform that the incorporation of such measures allow the organisation to minimise the incidents of “cyber security breaches”. A similar response was also reported by the respondents in the interview that the incorporation of such measures have allowed the company to eliminate the challenges faces by them and also reduce the number of such incidents within the organisation. Therefore, in this context, it can be analysed that with an effective implementation of the strategies measures for mitigating the negative incidents and impacts of “cyber security challenges” can assist organisation in limiting the overall impact of such incidents and also minimise the number of incidents that occur due to “cyber security breaches”. Hence, on the basis of the findings of this study, the measures that are implemented by the companies for managing the “cyber security breaches” within the company were found to be effective.

The data analysis section also informs that despite helping organisations in limiting the number of “cyber security incidents” in the company, the implemented measures poses certain challenges. In this context, this study informs that despite offering effectual results, the strategies implemented by the companies, pose major challenges to the companies. In this regard, on the basis of the analysis of the collected data from “primary and secondary sources” it is identified that the strategies implemented in the organisations poses significant challenges such as “limited skills”, “financial limitations” and sometimes, organisation also face “regulatory and compliance challenges”. These are the crucial challenges that needs to be focused by the companies to ensure that the mitigating strategies are being implemented in an effective way.

On the basis of the analyses from the interview questionnaire, as well as from the collected “secondary data”, it has been found that the airline organisations need to incorporate effective measures that can help the organisation to combat against the “cyber security breaches”. These breaches impose significant negative impact on the organisation, which eventually disturbs the entire operability of the company. Thus, it is analysed that these attacks are very vigilant and

organisations must incorporate immediate and strategic methods for addressing such attacks in the future.

5.3 Chapter Summary

On the basis of this chapter, it can be summarised that the collected “primary and secondary” data plays a critical role in this dissertation. Both of the data sources have helped in gathering critical “data and information” for this study. Thus, this chapter further discusses the analysed data, which helps in preparing a profound conclusion of this study.

Chapter 6: Conclusion and Recommendation

6.1 Chapter Introduction

In this chapter, the overall study is concluded. Based on this chapter, critical information on the overall aim of this dissertation is cited along with the overall findings of this study. In addition to this, the research questions of this study are answered here along with recommendations as well as suggestions on carrying out further research.

6.2 Answering the research question

With respect to the “research questions” as well as the sub questions, the collected data and their analyses helped in accomplishing them.

The findings of the study informs that the “cyber security attacks” posed a considerable negative impact on the overall performance of an organisation. Therefore, it can be said that there is a significant requirement for implementing appropriate “cyber security strategies” to eliminate such negative scenarios from the organisations. It is also required to have a sheer understanding of these impacts such that appropriate actions can be incorporated. Apart from this it is also found that various measures have been implemented by the airline organisations that help them address the “cyber security attacks”. In the context of the appropriate implemented tactics, it is found that making investments in the technical systems, providing training to the workforce for up-skilling their current skill set as well as ensuring that the regulations as well as legislations are appropriately followed, are some of the main strategies that are implemented to ensure that the “cyber security challenges” are being addressed in an effective way.

With respect to the strategies as well as methodologies that have been implemented to address the “cyber security challenges”, it is found that these tactics are quite helpful for the organisations. It is also found in the analysis that these actions have helped the organisation to reduce the number of “cyber security attacks” in their organisation. Apart from that, it has also been found that organisations are also able to determine the “cyber security attacks” before it becomes worse. Therefore, in this regard it can be said that strategies that have been implemented by the organisations in order to address the “cyber security challenges” have proven to be effective.

Despite, this effectiveness, it is also found that while incorporating the strategies, the organisations faces a lot of struggles. When it comes to the struggle, it is found that the organisations may have limited financial budget. The incorporation of advanced technical systems requires significant financial investment. However, with the limitation in financial budgets the organisations face a major challenge. Apart from that, there can be several resistance from the current workforce due to their knowledge gap in the context of "cyber security challenges" and their impact. Apart from this, the limited skill set also impose a significant challenge to the organisation when it comes to the incorporation of the abovementioned strategies to eliminate "cyber security risks" from the organisation.

These are the main findings of the study which has helped to provide a concluded result that "cyber security challenges" are significant and pose an adverse impact on an overall organisation. Therefore, it is important to implement efficient methods to ensure that these challenges are addressed in an effective way and does not pose much harm to the organisation.

6.3 Recommendations

On the basis of the above part of this chapter, it is found that the organisations face severe challenges when it comes to addressing "cyber security challenges". Therefore, in this regard, some of crucial strategies are recommended to ensure that organisations carry out their operational activities in an effective and ensuring that they do not get affected from any such challenges.

Thus, in this context, it is firstly recommended that the organisation must focus on making substantial investment in order to enhance their technical abilities. Such investment will allow an organisation to ensure that they have latest technologies for addressing any unforeseen circumstance hampering the organisation (Sleem, 2022). It will also help an organisation to detect the risks at the early phase and allows the workforce to put significant efforts to address them effectively.

Secondly, it is recommended that the organisations ensure that they effectively comply with the significant frameworks that allow them to ensure that they follow all the required regulations and legislations. In this regard, Kandasamy et al. (2020) opined that organisations can carry out regular checks on the systems and legislations to ensure that they are following them strictly.

It is also recommended to ensure that the organisations have a vigorous training sessions for up skilling the workforce. Trainings allow the workforce to enhance their current set of skills, but at the same time, they also allow the organisations to gain a competitive edge (Backman, 2023). Providing training on determining the “cyber security risks” and implementing appropriate strategies for eliminating the identified risks helps organisation to protect against significant vulnerabilities associated with “cyber security”.

6.4 Further Research

On the basis of the findings of this study, it has been found that there is a scope to carry out further research on this domain. However, in this regard, it is recommended to carry out further studies by taking the “training and development” with respect to “cyber security”. In this regard, Alahmari and Duncan (2021) stated that incorporating training sessions allows the organisation to ensure that the knowledge set of the employees are enhanced regarding the “cyber security risks” and also help in minimising the threats concerning “cyber risks” and enhance the overall structure of the “cyber security” in the airline-based organisations. Apart from this, it is also suggested that a future study can be carried out by focusing on the implementation of developed technologies in the field of aviation industry with respect to “cyber security issues and challenges”. Ambreen et al. (2023) informs those various technologies such as “artificial intelligence”, “data analytics” and other developed technologies can be incorporated within airline companies that can allow them in treating and determining threats associated with “cyber security”.

6.5 Conclusion

This study focused on determining the impact of “cyber security challenges” on aviation. Therefore, in order to meet this aim, appropriate strategies were implemented. Various literature was reviewed and “primary and secondary” method was incorporated for collecting data. On the basis of the previous chapters, it is concluded that “cyber security challenges” imposes an adverse impact on the aviation.

References

Aggarwal, R., and Ranganathan, P., 2019. Study designs: Part 2 – Descriptive studies. *Perspectives in Clinical Research*, *10*(1), 34. https://doi.org/10.4103/picr.picr_154_18

Alahmari, A.A. and Duncan, R.A., 2021, July. Investigating potential barriers to cybersecurity risk management investment in smes. In *2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)* (pp. 1-6). IEEE. https://doi.org/10.1109/ECAI52376.2021.9515166

Alghamdi, S.A., Daim, T. and Alzahrani, S.M., 2024. Technology Assessment for Cybersecurity Organizational Readiness: Case of Airlines Sector and Electronic Payment.

Alhayani, B., Mohammed, H.J., Chaloob, I.Z. and Ahmed, J.S., 2021. Effectiveness of artificial intelligence techniques against cyber security risks apply of IT industry. *Materials Today: Proceedings*, *531*.

Alsulami, A.A. and Zein-Sabatto, S., 2020, December. Detection and defense from false data injection attacks in aviation cyber-physical systems using artificial immune systems. In *2020 international conference on computational science and computational intelligence (CSCI)* (pp. 69-75). IEEE.

Alturki, R., 2021. Research Onion for Smart IoT-Enabled Mobile Applications. *Scientific programming*, *2021*(1), p.4270998. https://doi.org/10.1155/2021/4270998

Ambreen, L., Jain, M., Yadav, R.K. and Loonkar, S., 2023. Effective cybersecurity risk management practices for small and medium-sized enterprises: A comprehensive review. *Multidisciplinary Reviews*, *6*. https://doi.org/10.31893/multirev.2023ss080

Anaedevha, R.N. and Ajibola, A., 2020. Cyber Security Framework for Nigerian Civil Aviation Authority, Headquarters. *International Journal of*.

Aydın, S. and Kahraman, C., 2021. Aviation 4.0 Revolution. In *Intelligent and Fuzzy Techniques in Aviation 4.0: Theory and Applications* (pp. 3-19). Cham: Springer International Publishing.

Aydın, S. and Kahraman, C., 2021. Aviation 4.0 Revolution. In *Intelligent and Fuzzy Techniques in Aviation 4.0: Theory and Applications* (pp. 3-19). Cham: Springer International Publishing.

Babu, C.S., Simon, P.A. and Kumar, S.B., 2023. The Future of Cyber Security Starts Today, Not Tomorrow. In *Malware Analysis and Intrusion Detection in Cyber-Physical Systems* (pp. 348375). IGI Global.

Babu, C.S., Simon, P.A. and Kumar, S.B., 2023. The Future of Cyber Security Starts Today, Not Tomorrow. In *Malware Analysis and Intrusion Detection in Cyber-Physical Systems* (pp. 348-375). IGI Global.

Backman, S., 2023. Risk vs. threat-based cybersecurity: the case of the EU. *European Security*, *32*(1), pp.85-103.https://doi.org/10.1080/09662839.2022.2069464

Banerjee, S., Mohapatra, S. and Bharati, M., 2022. Research Design and Methodology. In *AI in Fashion Industry* (pp. 51-91). Emerald Publishing Limited. https://doi.org/10.1108/978-1-80262-633-920221004

BBC, 2020. *British Airways fined £20m over data breach.* Available at: https://www.bbc.com/news/technology-54568784 [Accessed on 18 June 2024]

BBC, 2020. *British Airways fined £20m over data breach.* Available at: https://www.bbc.com/news/technology-54568784 [Accessed on 18 June 2024]

Beckner, C., 2022. *Risk-Based Security and the Aviation System: Operational Objectives and Policy Challenges*. Center for Cyber and Homeland Security at Auburn University.

Beckner, C., 2022. *Risk-Based Security and the Aviation System: Operational Objectives and Policy Challenges*. Center for Cyber and Homeland Security at Auburn University.

Berndt, A.E., 2020. Sampling methods. *Journal of Human Lactation*, *36*(2), pp.224-226. https://doi.org/10.1177/0890334420906850

Bonache, J. and Festing, M., 2020. Research paradigms in international human resource management: An epistemological systematisation of the field. *German Journal of Human Resource Management*, *34*(2), pp.99-123. https://doi.org/10.1177/2397002220909780

Cains, M.G., Flora, L., Taber, D., King, Z. and Henshel, D.S., 2022. Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. *Risk Analysis*, *42*(8), pp.1643-1669.https://doi.org/10.1111/risa.13687

Cains, M.G., Flora, L., Taber, D., King, Z. and Henshel, D.S., 2022. Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. *Risk Analysis*, *42*(8), pp.1643-1669.

Cains, M.G., Flora, L., Taber, D., King, Z. and Henshel, D.S., 2022. Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. *Risk Analysis*, *42*(8), pp.1643-1669.

Canito, A., Aleid, K., Praça, I., Corchado, J. and Marreiros, G., 2020, December. An ontology to promote interoperability between cyber-physical security systems in critical infrastructures. In *2020 IEEE 6th International Conference on Computer and Communications (ICCC)* (pp. 553560). IEEE.

Canito, A., Aleid, K., Praça, I., Corchado, J. and Marreiros, G., 2020, December. An ontology to promote interoperability between cyber-physical security systems in critical infrastructures. In *2020 IEEE 6th International Conference on Computer and Communications (ICCC)* (pp. 553-560). IEEE.

Cash, P., Isaksson, O., Maier, A. and Summers, J., 2022. Sampling in design research: Eight key considerations. *Design studies*, *78*, p.101077. https://doi.org/10.1016/j.destud.2021.101077

Cele, N.N. and Kwenda, S., 2024. Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. *Journal of Financial Crime*.https://doi.org/10.1108/JFC-10-2023-0263

Chowdhury, N. and Gkioulos, V., 2021. Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*, *40*, p.100361.

Chowdhury, N. and Gkioulos, V., 2021. Cyber security training for critical infrastructure protection: A literature review. *Computer Science Review*, *40*, p.100361.

Chung, K.C. and Tan, P.J.B., 2022. Options to improve service quality to enhance value co-creation for customers in the aviation industry in Taiwan. *Sage Open*, *12*(1), p.21582440221079926. https://doi.org/10.1177/21582440221079926

CIAB, 2024. *Polish Airline Hack Was Denial of Service Attack.* Available at: https://www.ciab.com/resources/polish-airline-hack-was-denialof-service-attack/ [Accessed on 20 June 2024]

Clarke, M. and Martin, K., 2024, January. Managing cybersecurity risk in healthcare settings. In *Healthcare Management Forum* (Vol. 37, No. 1, pp. 17-20). Sage CA: Los Angeles, CA: SAGE Publications.https://doi.org/10.1177%2F08404704231195804

Cremer, F., Sheehan, B., Fortmann, M., Kia, A.N., Mullins, M., Murphy, F. and Materne, S., 2022. Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva papers on risk and insurance. Issues and practice*, *47*(3), p.698. https://doi.org/10.1057/s41288-022-00266-6

Dave, G., Choudhary, G., Sihag, V., You, I. and Choo, K.K.R., 2022. Cyber security challenges in aviation communication, navigation, and surveillance. *Computers & Security*, *112*, p.102516.

Durst, S., Hinteregger, C. and Zieba, M., 2024. The effect of environmental turbulence on cyber security risk management and organizational resilience. *Computers & Security*, *137*, p.103591.https://doi.org/10.1016/j.cose.2023.103591

Ebert, J., Newton, O., O'Rear, J., Riley, S., Park, J. and Gupta, M., 2021. Leveraging aviation risk models to combat cybersecurity threats in vehicular networks. *Information*, *12*(10), p.390. https://doi.org/10.3390/info12100390

Edmonds, W., and Kennedy, T., 2017. *An applied guide to research designs*. SAGE Publications, Inc, https://doi.org/10.4135/9781071802779

Efe, A., Tuzlupınar, B. and Cavlan, A.C., 2021. Air traffic security against cyber threats. *Bilge International Journal of Science and Technology Research*, *3*(2), pp.135-143.

Eling, M., McShane, M. and Nguyen, T., 2021. Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, *24*(1), pp.93-125.https://doi.org/10.1111/rmir.12169

Elmarady, A.A. and Rahouma, K., 2021. Actual TDoA-based augmentation system for enhancing cybersecurity in ADS-B. *Chinese Journal of Aeronautics*, *34*(2), pp.217-228.

Esteki, M., Gandomani, T.J. and Farsani, H.K., 2020. A risk management framework for distributed scrum using PRINCE2 methodology. *Bulletin of Electrical Engineering and Informatics*, *9*(3), pp.1299-1310.

Fadziso, T., Thaduri, U.R., Dekkati, S., Ballamudi, V.K.R. and Desamsetti, H., 2023. Evolution of the cyber security threat: an overview of the scale of cyber threat. *Digitalization & Sustainability Review*, *3*(1), pp.1-12. http://dx.doi.org/10.6084/m9.figshare.24189921.v1

Faruk, M.J.H., Miner, P., Coughlan, R., Masum, M., Shahriar, H., Clincy, V. and Cetinkaya, C., 2021, December. Smart connected aircraft: towards security, privacy, and ethical hacking. In *2021 14th International Conference on Security of Information and Networks (SIN)* (Vol. 1, pp. 1-5). IEEE.

Filinovych, V. and Hu, Z., 2021, August. Aviation and the Cybersecurity Threats. In *International Conference on Business, Accounting, Management, Banking, Economic Security and Legal Regulation Research (BAMBEL 2021)* (pp. 120-126). Atlantis Press.

Florackis, C., Louca, C., Michaely, R. and Weber, M., 2023. Cybersecurity risk. *The Review of Financial Studies*, *36*(1), pp.351-407.

Freeman, K. and Garcia, S., 2021. A survey of cyber threats and security controls analysis for urban air mobility environments. In *AIAA Scitech 2021 Forum* (p. 0660).

Galkovskaya, V. and Volos, M., 2022. Economic Efficiency of the Implementation of Digital Technologies in Energy Power. *Sustainability*, *14*(22), p.15382. https://doi.org/10.3390/su142215382

Ganin, A.A., Quach, P., Panwar, M., Collier, Z.A., Keisler, J.M., Marchese, D. and Linkov, I., 2020. Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Analysis*, *40*(1), pp.183-199.

Gebremeskel, B.K., Jonathan, G.M. and Yalew, S.D., 2023. Information security challenges during digital transformation. *Procedia Computer Science*, *219*, pp.44-51. https://doi.org/10.1016/j.procs.2023.01.262

Gnatyuk, S., Sydorenko, V., Polozhentsev, A., Fesenko, A., Akatayev, N. and Zhilkishbayeva, G., 2020. Method of Cybersecurity Level Determining for the Critical Information Infrastructure of the State. In *COAPSN* (pp. 332-341).

Government of the UK, 2024. *Cybersecurity breaches survey*, *2024.* Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024 [Accessed on 1 August 2024]

Habler, E., Bitton, R. and Shabtai, A., 2022. Evaluating the Security of Aircraft Systems. *arXiv preprint arXiv:2209.04028*.

Habler, E., Bitton, R. and Shabtai, A., 2023. Assessing Aircraft Security: A comprehensive survey and methodology for evaluation. *ACM Computing Surveys*, *56*(4), pp.1-40.

Hagen, R.A., 2023. *The Evolution of Malicious Intent in Cybercrime Since 1990*. Available at: https://www.linkedin.com/pulse/evolution-malicious-intent-cybercrime-since-1990-raymond-andr%C3%A8-hagen/ [Accessed on 20 July 2024]

Hilbert, M., 2020. Digital technology and social change: the digital transformation of society from a historical perspective. *Dialogues in clinical neuroscience*, *22*(2), pp.189-194. https://doi.org/10.31887%2FDCNS.2020.22.2%2Fmhilbert

IATA, 2023. *Aviation Cyber security.* Available at: https://www.iata.org/contentassets/f23f6fa53f6b4dff8178bf88102c9f09/acysec [Accessed on 17 June 2024]

IATA, 2023. *Aviation Cyber security.* Available at: https://www.iata.org/contentassets/f23f6fa53f6b4dff8178bf88102c9f09/acysec-industryposition-2023.pdf [Accessed on 17 June 2024]

IATA, 2024. *Aviation Cyber Security.* Available at: https://www.iata.org/en/programs/security/cyber [Accessed on 17 June 2024]

IATA, 2024. *Aviation Cyber security.* Available at: https://www.iata.org/en/programs/security/cyber-security/ [Accessed on 17 June 2024]

ICAO, 2024. *Aviation Cybersecurity.* Available at: https://www.icao.int/aviationcybersecurity/Pages/default.aspx [Accessed on 17 June 2024]

ICAO, 2024. *Aviation Cybersecurity.* Available at: https://www.icao.int/aviationcybersecurity/Pages/default.aspx [Accessed on 17 June 2024]

Industrial cybersecurity pulse, 2022. *Throwback Attack: Hack leaves 1,400 passengers of Polish airline LOT stranded.* Available at: https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attackhack-leaves-1400-passengers-of-polish-airline-lot-stranded/ [Accessed on 18 June 2024]

Industrial cybersecurity pulse, 2022. *Throwback Attack: Hack leaves 1,400 passengers of Polish airline LOT stranded.* Available at: https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-hack-leaves-1400-passengers-of-polish-airline-lot-stranded/ [Accessed on 18 June 2024]

International Civil Aviation Organisation, 2023. *Attack types targeting the aviation industry.* Available at: https://www.icao.int/MID/Documents/2023/Cybersecurity%20Symposium/3.3%20Oman%20-%20Navigating%20the%20Skies%20of%20Cybersecurity%20Unveiling%20Real-World%20Attacks%20and%20Risk%20Management%20in%20Aviation.pdf [Accessed on 1 August 2024]

James, A., 2023. *The importance of an incident response plan in today's cybersecurity landscape.* Available at: https://www.linkedin.com/pulse/importance-incident-response-plan-irp-todays-landscape-anish-james/ [Accessed on 20 July 2024]

Kabashkin, I., Misnevs, B. and Zervina, O., 2023. Artificial intelligence in aviation: New professionals for new technologies. *Applied Sciences*, *13*(21), p.11660. https://doi.org/10.3390/app132111660

Kadena, E. and Gupi, M., 2021. Human factors in cybersecurity: Risks and impacts. *Security science journal*, *2*(2), pp.51-64.DOI: 10.37458/ssj.2.2.3

Kalinin, M., Krundyshev, V. and Zegzhda, P., 2021. Cybersecurity risk assessment in smart city infrastructures. *Machines*, *9*(4), p.78.

Kamiya, S., Kang, J.K., Kim, J., Milidonis, A. and Stulz, R.M., 2021. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), pp.719-749. https://doi.org/10.1016/j.jfineco.2019.05.019

Kandasamy, K., Srinivas, S., Achuthan, K. and Rangan, V.P., 2020. IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process. *EURASIP Journal on Information Security*, *2020*, pp.1-18.https://doi.org/10.1186/s13635-020-00111-0

Kankam, P.K., 2020. Approaches in information research. *New Review of Academic Librarianship*, *26*(1), pp.165-183. https://doi.org/10.1080/13614533.2019.1632216

Karpiuk, M. and Kelemen, M., 2022. Cybersecurity in civil aviation in Poland and Slovakia. *Cybersecurity and Law*, *8*(2), pp.70-83.

Kaushik, R. and Thakur, A.K., 2022. A Brief Review on IoT, its Applications, Challenges & Future Aspects in Aviation Industry. *International Journal of Current Science*, *12*(2), pp.909-914.

Kayan, H., Nunes, M., Rana, O., Burnap, P. and Perera, C., 2022. Cybersecurity of industrial cyber-physical systems: A review. *ACM Computing Surveys (CSUR)*, *54*(11s), pp.1-35.

Khandker, S., Turtiainen, H., Costin, A. and Hämäläinen, T., 2022. Cybersecurity attacks on software logic and error handling within AIS implementations: A systematic testing of resilience. *IEEE Access*, *10*, pp.29493-29505.

Khandker, S., Turtiainen, H., Costin, A. and Hämäläinen, T., 2022. Cybersecurity attacks on software logic and error handling within AIS implementations: A systematic testing of resilience. *IEEE Access*, *10*, pp.29493-29505.

Kizilcan, L.S. and Mizrak, K.C., 2022. Cyber Attacks In Civil Aviation And The Concept Of Cyber Security. *Idea Studies Journal. International Journal*, *47*(8), pp.742-752. http://dx.doi.org/10.2922

Korba, P., Jenčová, E., Al-Rabeei, S., Koščáková, M. and Sekelová, I., 2023, October. Analysis of Serious Challenges Faced by the Aviation Industry. In *International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures* (pp. 37-49). Cham: Springer Nature Switzerland. http://dx.doi.org/10.1007/978-3-031-50051-0_3

Koroniotis, N., Moustafa, N., Schiliro, F., Gauravaram, P. and Janicke, H., 2020. A holistic review of cybersecurity and reliability perspectives in smart airports. *IEEE Access*, *8*, pp.209802-209834.

Lahiri, S., 2023. A Qualitative Research Approach is an Inevitable Part of Research Methodology: An Overview. *International Journal For Multidisciplinary Research*, *5*(3). https://doi.org/10.36948/ijfmr.2023.v05i03.3178

Lee, I., 2020. Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future internet*, *12*(9), p.157.https://doi.org/10.3390/electronics12183958

Lehto, M., 2020. Cyber security in aviation, maritime and automotive. *Computation and Big Data for Transport: Digital Innovations in Surface and Air Transport Systems*, pp.19-32.

Lekota, F. and Coetzee, M., 2021, June. Aviation Sector Computer Security Incident Response Teams: Guidelines and Best Practice. In *European Conference on Cyber Warfare and Security* (pp. 507-XII). Academic Conferences International Limited.

Li, Y. and Liu, Q., 2021. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Lim, W.M., 2023. Philosophy of science and research paradigm for business research in the transformative age of automation, digitalization, hyperconnectivity, obligations, globalization and sustainability. *Journal of Trade Science*, *11*(2/3), pp.3-30. https://doi.org/10.1108/JTS-07-2023-0015

Liu, X., Ahmad, S.F., Anser, M.K., Ke, J., Irshad, M., Ul-Haq, J. and Abbas, S., 2022. Cyber security threats: A never-ending challenge for e-commerce. *Frontiers in psychology*, *13*, p.927398.https://doi.org/10.3389/fpsyg.2022.927398

Loura, J. and Singh, K.D., 2021. Emerging Trends in Aviation Cyber-Security: Study of European Air Traffic Control (Euro-Control). *Indian JL & Just.*, *12*, p.1.

Lu, X. and Wu, Z., 2022. ATMChain: Blockchain-Based Security Framework for Cyber-Physics System in Air Traffic Management. *Security and Communication Networks*, *2022*(1), p.8542876.

Lykou, G., Anagnostopoulou, A. and Gritzalis, D., 2018. Smart airport cybersecurity: Threat mitigation and cyber resilience controls. *Sensors*, *19*(1), p.19. https://doi.org/10.3390%2Fs19010019

Maalem Lahcen, R.A., Caulkins, B., Mohapatra, R. and Kumar, M., 2020. Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, *3*, pp.1-18.https://doi.org/10.1186/s42400-020-00050-w

Matta, C., 2022. Philosophical paradigms in qualitative research methods education: What is their pedagogical role?. *Scandinavian Journal of Educational Research*, *66*(6), pp.1049-1062. https://doi.org/10.1080/00313831.2021.1958372

Mäurer, N., Guggemos, T., Ewert, T., Gräupl, T., Schmitt, C. and Grundner-Culemann, S., 2022. Security in digital aeronautical communications a comprehensive gap analysis. *International Journal of Critical Infrastructure Protection*, *38*, p.100549.

Mauthner, N.S., 2020. Research philosophies and why they matter. In *How to Keep your Doctorate on Track* (pp. 76-86). Edward Elgar Publishing. http://dx.doi.org/10.4337/9781788975636.00018

Mbedzi, M.D., van der Poll, H.M. and van der Poll, J.A., 2020. Enhancing a decision-making framework to address environmental impacts of the South African coalmining industry. *Energies*, *13*(18), p.4897. https://doi.org/10.3390/en13184897

Meshkat, L. and Miller, R.L., 2022, January. A Systems Approach for Cybersecurity Risk Assessment. In *2022 Annual Reliability and Maintainability Symposium (RAMS)* (pp. 1-9). IEEE. https://doi.org/10.1109/RAMS51457.2022.9893966

Mishra, A., Alzoubi, Y.I., Gill, A.Q. and Anwar, M.J., 2022. Cybersecurity enterprises policies: A comparative study. *Sensors*, *22*(2), p.538.

Mızrak, F., 2023. Integrating cybersecurity risk management into strategic management: a comprehensive literature review. *Research Journal of Business and Management*, *10*(3), pp.98-108.http://dx.doi.org/10.17261/Pressacademia.2023.1807

Najaf, K., Mostafiz, M.I. and Najaf, R., 2021. Fintech firms and banks sustainability: why cybersecurity risk matters?. *International Journal of Financial Engineering*, *8*(02), p.2150019.

Ohrimenco, S. and Cernei, V., 2024. Cybersecurity risk.http://dx.doi.org/10.53486/escst2023

Onwubiko, C., 2022. CyberOps: Situational Awareness in Cybersecurity Operations. *arXiv preprint arXiv:2202.03687*.

Osuagwu, L., 2020. Research methods: Issues and research direction. *Business and Management Research*, *9*(3), pp.46-55. http://dx.doi.org/10.5430/bmr.v9n3p46

Oztemel, E. and Gursev, S., 2020. Literature review of Industry 4.0 and related technologies. *Journal of intelligent manufacturing*, *31*(1), pp.127-182.

Oztemel, E. and Gursev, S., 2020. Literature review of Industry 4.0 and related technologies. *Journal of intelligent manufacturing*, *31*(1), pp.127-182.

Palko, Dmytro, Tetiana Babenko, Andrii Bigdan, Nikolay Kiktev, Taras Hutsol, Maciej Kuboń, Hryhorii Hnatiienko, Sylwester Tabor, Oleg Gorbovy, and Andrzej Borusiewicz. 2023. "Cyber Security Risk Modeling in Distributed Information Systems" *Applied Sciences* 13, no. 4: 2393. https://doi.org/10.3390/app13042393

Pandey, S., Singh, R.K., Gunasekaran, A. and Kaushik, A., 2020. Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing*, *13*(1), pp.103-128.https://doi.org/10.1108/JGOSS-05-2019-0042

Pyzynski, M. and Balcerzak, T., 2021. Cybersecurity of the unmanned aircraft system (UAS). *Journal of Intelligent & Robotic Systems*, *102*(2), p.35.

Ranganathan, P., 2019. Understanding research study designs. *Indian journal of critical care medicine: peer-reviewed, official publication of Indian Society of Critical Care Medicine*, *23*(Suppl 4), p.S305. https://doi.org/10.5005%2Fjp-journals-10071-23314

Rouder, J., Saucier, O., Kinder, R. and Jans, M., 2021. What to do with all those open-ended responses? Data visualization techniques for survey researchers. *Survey Practice*. https://doi.org/10.29115/SP-2021-0008

Saeed, S., Altamimi, S.A., Alkayyal, N.A., Alshehri, E. and Alabbad, D.A., 2023. Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, *23*(15), p.6666.https://doi.org/10.3390%2Fs23156666

Sagnier, C., Loup-Escande, E., Lourdeaux, D., Thouvenin, I. and Valléry, G., 2020. User acceptance of virtual reality: an extended technology acceptance model. *International Journal of Human–Computer Interaction*, *36*(11), pp.993-1007.

Sagnier, C., Loup-Escande, E., Lourdeaux, D., Thouvenin, I. and Valléry, G., 2020. User acceptance of virtual reality: an extended technology acceptance model. *International Journal of Human–Computer Interaction*, *36*(11), pp.993-1007.

Scholl, M., Scholl, M. and Suloway, T., 2023. *Introduction to cybersecurity for commercial satellite operations*. US Department of Commerce, National Institute of Standards and Technology.

Scholl, M., Scholl, M. and Suloway, T., 2023. *Introduction to cybersecurity for commercial satellite operations*. US Department of Commerce, National Institute of Standards and Technology.

Scholtz, S.E., de Klerk, W. and de Beer, L.T., 2020. The use of research methods in psychological research: A systematised review. *Frontiers in research metrics and analytics*, *5*, p.1. https://doi.org/10.3389/frma.2020.00001

Shafik, W., Matinkhah, S.M. and Shokoor, F., 2023. Cybersecurity in unmanned aerial vehicles: A review. *International Journal on Smart Sensing and Intelligent Systems*, *16*(1).

Shafik, W., Matinkhah, S.M. and Shokoor, F., 2023. Cybersecurity in unmanned aerial vehicles: A review. *International Journal on Smart Sensing and Intelligent Systems*, *16*(1).

Shaikh, F.A. and Siponen, M., 2023. Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*, *124*, p.102974. https://doi.org/10.1016/j.cose.2022.102974

Shaikh, F.A. and Siponen, M., 2023. Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*, *124*, p.102974.

Shaikh, F.A. and Siponen, M., 2023. Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity. *Computers & Security*, *124*, p.102974.

Shevchenko, P.V., Jang, J., Malavasi, M., Peters, G.W., Sofronov, G. and Trück, S., 2023. The nature of losses from cyber-related events: risk categories and business sectors. *Journal of Cybersecurity*, *9*(1), p.tyac016.https://doi.org/10.1093/cybsec/tyac016

Sileyew, K.J., 2019. *Research design and methodology* (Vol. 7). Cyberspace. https://doi.org/10.5772/intechopen.85731

Sleem, A., 2022. A Comprehensive Study of Cybersecurity Threats and Countermeasures: Strategies for Mitigating Risks in the Digital Age. *Journal of Cybersecurity & Information Management*, *10*(2).https://doi.org/10.54216/JCIM.100204

Stansbury, R.S., Akbas, M.I., Craiger, P. and Verleger, M.A., 2022. Enhancing STEM ROTC Training in Aviation Cybersecurity.

Stansbury, R.S., Akbas, M.I., Craiger, P. and Verleger, M.A., 2022. Enhancing STEM ROTC Training in Aviation Cybersecurity.

Stastny, P. and Stoica, A.M., 2022, February. Protecting aviation safety against cybersecurity threats. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1226, No. 1, p. 012025). IOP Publishing. doi:10.1088/1757-899X/1226/1/012025

Stastny, P. and Stoica, A.M., 2022, February. Protecting aviation safety against cybersecurity threats. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1226, No. 1, p. 012025). IOP Publishing.

Stastny, P. and Stoica, A.M., 2022, February. Protecting aviation safety against cybersecurity threats. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1226, No. 1, p. 012025). IOP Publishing.

Stine, K., Quinn, S., Ivy, N., Barrett, M., Witte, G., Feldman, L. and Gardner, R., 2021. Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management.https://doi.org/10.6028/NIST.IR.8286A

Strohmeier, M., Tresoldi, G., Granger, L. and Lenders, V., 2022, August. Building an avionics laboratory for cybersecurity testing. In *Proceedings of the 15th Workshop on Cyber Security Experimentation and Test* (pp. 10-18).

Strohmeier, M., Tresoldi, G., Granger, L. and Lenders, V., 2022, August. Building an avionics laboratory for cybersecurity testing. In *Proceedings of the 15th Workshop on Cyber Security Experimentation and Test* (pp. 10-18).

Taherdoost, H., 2022. What are different research approaches? Comprehensive Review of Qualitative, quantitative, and mixed method research, their applications, types, and limitations. *Journal of Management Science & Engineering Research*, *5*(1), pp.53-63. http://dx.doi.org/10.30564/jmser.v5i1.4538

Taylor, A.K. and Steven Cotter, T., 2020. Pilots' Role in the Critical Infrastructure of Aviation. In *Advances in Human Factors and Systems Interaction: Proceedings of the AHFE 2019*

International Conference on Human Factors and Systems Interaction, July 24-28, 2019, Washington DC, USA 10 (pp. 349-360). Springer International Publishing.

Taylor, A.K. and Steven Cotter, T., 2020. Pilots' Role in the Critical Infrastructure of Aviation. In *Advances in Human Factors and Systems Interaction: Proceedings of the AHFE 2019 International Conference on Human Factors and Systems Interaction, July 24-28, 2019, Washington DC, USA 10* (pp. 349-360). Springer International Publishing.

Thakur, M., 2024. Cyber security threats and countermeasures in digital age. *Journal of Applied Science and Education (JASE)*, *4*(1), pp.1-20.https://doi.org/10.54060/a2zjournals.jase.42

Tong, L. and Kwan, M., 2022. ENSURING CYBER SECURITY IN AIRLINES TO PREVENT DATA BREACH. *Computer Science & IT Research Journal*, *3*(3), pp.66-73. http://dx.doi.org/10.51594/csitrj.v3i3.426

Torens, C., 2020. Safety versus security in aviation, comparing DO-178C with security standards. In *AIAA Scitech 2020 Forum* (p. 0242).

Tran, T.D., Thiriet, J.M., Marchand, N. and El Mrabti, A., 2022. A cybersecurity risk framework for unmanned aircraft systems under specific category. *Journal of Intelligent & Robotic Systems*, *104*(1), p.4.

Turner, D.P., 2020. Sampling Methods in Research Design. *Headache: The Journal of Head & Face Pain*, *60*(1). https://doi.org/10.1111/head.13707

Turtiainen, H., Costin, A., Khandker, S. and Hämäläinen, T., 2022. Gdl90fuzz: Fuzzing-gdl-90 data interface specification within aviation software and avionics devices–a cybersecurity pentesting perspective. *IEEE Access*, *10*, pp.21554-21562.

Ukwandu, E., Ben-Farah, M.A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., Andonovic, I. and Bellekens, X., 2022. Cyber-security challenges in aviation industry: A review of current and future trends. *Information*, *13*(3), p.146. https://doi.org/10.3390/info13030146

Vaughn, L.M. and Jacquez, F., 2020. Participatory research methods–choice points in the research process. *Journal of Participatory Research Methods*, *1*(1). https://doi.org/10.35844/001c.13244

Vu, C. and Rajaratnam, S., 2022. *Cyber security in Singapore*. S. Rajaratnam School of International Studies..

Williams, C.M., Chaturvedi, R. and Chakravarthy, K., 2020. Cybersecurity risks in a pandemic. *Journal of medical Internet research*, *22*(9), p.e23692. https://doi.org/10.2196/23692

Woods, D.W. and Seymour, S., 2023. Evidence-based cybersecurity policy? A meta-review of security control effectiveness. *Journal of Cyber Policy*, pp.1-19.https://doi.org/10.1080/23738871.2024.2335461

Xie, Y., Gardi, A. and Sabatini, R., 2022, September. Cybersecurity trends in low-altitude air traffic management. In *2022 IEEE/AIAA 41st Digital Avionics Systems Conference (DASC)* (pp. 1-9). IEEE.

Żmigrodzka, M., 2020. Cybersecurity–One of the Greatest Challenges for Civil Aviation in the 21st Century. *Safety & Defense*, *6*(2), pp.33-41.

CIAB, 2024. *Polish Airline Hack Was Denial of Service Attack.* Available at: https://www.ciab.com/resources/polish-airline-hack-was-denial-of-service-attack/ [Accessed on 20 June 2024]

Appendices

Appendix 1: Interview Questionnaire

Question 1: Can you describe any instance associated with the issue of "cyber security attack"?

Question 2: How did this incident impact the overall airline?

Question 3: What measures are implemented by your airline to address such negative incidents?

Question 4: Were those measures effective in addressing such incidents?

Question 5: Have you encountered any issues while incorporating these measures?

Appendix 2: Interview transcripts

Interview transcript 1

Can you describe any instance associated with the issue of "cyber security attack"?	*"Yes! There was a breach in the security system of outline, where the "cyber attackers" have muddled through our system and gained access to our confidential information such as passengers' data."*
How did this incident impact the overall airline?	*"This incident has imposed a negative impact on our operability. Customers seem losing trust in us eventually reducing our annual revenue."*
What measures are implemented by your airline to address such negative incidents?	*"We implemented stringent metrics for ascertaining malicious activities earlier. Additionally, we increased the security of our authentication along with regular assessments of the overall scenario for determining risks and threats".*
Were those measures effective	*"Yes, the methods that we have implemented have proven to*

in addressing such incidents?	*be effective. These methods have allowed us to address such negative incidents effectively. Additionally, the implemented measures have allowed in mitigating such incidents".*
Have you encountered any issues while incorporating these measures?	*"Yes, we have faced certain challenges while implementing these measures. First, we found that the employees were reluctant to implement the new methods of maintaining security for the database. Secondly, the incorporation of security measures was a complex method and also a tedious method.*

Interview Transcript 2

Can you describe any instance associated with the issue of "cyber security attack"?	*"In recent years, we were exposed to a ransomware attack, where our vital information was acquired by the attackers, and they commanded a significant amount as a ransom for releasing back the data to us".*
How did this incident impact the overall airline?	*"It impacted negatively on our operations, finances and even customers. We found that our relationship with the customers weakened after this incident".*
What measures are implemented by your airline to address such negative incidents?	*"We have increased the security of our database, along with ensured that we have a secured security system and implemented a quick response system for addressing such incidents in the future".*
Were those measures effective in addressing such incidents?	*"Yes, the measures that the company has implemented, are found to be effective. However, according to my perception, I assume that these measures can be further improved."*

Have you encountered any issues while incorporating these measures?	*"Yes, we have faced significant challenges while incorporating the aforementioned strategies. Firstly, a limited budget is a significant challenge that we faced. Second, the company also faced challenges in terms of meeting legal obligations".*

Interview Transcript 3

Can you describe any instance associated with the issue of "cyber security attack"?	*"Two years back, our company faced a breach, where some of the employees received a fake email from our official site, which demanded some critical information regarding our organisation".*
How did this incident impact the overall airline?	*"It negatively affected our organisation, where we had lost severe data about our company and customers. Additionally, it disturbed the entire operability of our organisation and imposed severe financial costs.*
What measures are implemented by your airline to address such negative incidents?	*"We have provided training to all the employees to determine such incidents and the methods to encounter those. We always try to inform our customers to ensure that they are aware of such incidents. Apart from these, we have incorporated a robust system for identifying these incidents at the earliest".*
Were those measures effective in addressing such incidents?	*"With respect to the measures that have been implemented by the company are found to be effective and sound. These measures have helped the organisation in mitigating the negative incidents associated with cyber security attacks".*
Have you encountered any	*"We faced a major issue while meeting the legal obligations*

issues while incorporating these measures?	*while incorporating security measures and training sessions for the employees. Incorporation of such measures required significant financial resources, which created a major challenge for us".*

Interview Transcript 4

Can you describe any instance associated with the issue of "cyber security attack"?	*"In the year 2022, our organisation encountered a DDoS issue, which led our website to malfunction for several hours".*
How did this incident impact the overall airline?	*"It impacted our overall strategy and imposed a significant impact on our relationship with our customers and employees".*
What measures are implemented by your airline to address such negative incidents?	*"We have implemented a robust security framework for safeguarding our database and systems. It helps us in securing data and eliminating incidents of data breach".*
Were those measures effective in addressing such incidents?	*"In the context of the measures implemented within our organisation, I would like to inform you that yes, these measures are effective in addressing the incidents associated with data breach and helped us in eliminating further incidents in the organisation".*
Have you encountered any issues while incorporating these measures?	*"Yes, we have encountered certain challenges while incorporating the mitigating measures for addressing the cyber security attacks in the company. In this regard, we have faced a major financial limitation. Further, we also faced a*

	significant backlash from our existing employees as they had to shift to a new software for carrying out their organisational activities".

Interview Transcript 5

Can you describe any instance associated with the issue of "cyber security attack"?	*"We faced a breach, where crucial information regarding our loyal customers and others were accessed by the attackers".*
How did this incident impact the overall airline?	*"This incident led our company to face severe financial losses and disturbed our entire operational capabilities. Our relationship with our customers was also negatively affected".*
What measures are implemented by your airline to address such negative incidents?	*"We have implemented an inclusive framework for overseeing and managing critical information. Additionally, we also ensured that a continuous development framework is in place".*
Were those measures effective in addressing such incidents?	*"Yes, the implemented measures have proven to be effective in terms of addressing such negative incidents within the company. However, I found that we need to emphasise providing training to our employees to enhance the effectiveness of these measures implemented within the organisation".*
Have you encountered any issues while incorporating these measures?	*"Yes, we have faced certain challenges. Firstly, we found that the employees did not have sufficient skills to implement the mitigating measures. The organisation also struggled while minimising the gap between the safety of consumer data and*

	user interface while utilising the framework".