DEALING WITH CYBERSECURITY THREATS RELATED TO AUTOMATED SYSTEMS IN AVIATION INDUSTRIES

Abstract

Cyber protection has been a big concern for the aviation industry, as most computerised computers are used in this field. The exponential development in technology has a direct impact on the networks and processes of the aviation industry. Nowadays cybersecurity vulnerabilities and challenges have advanced a great deal and thus an efficient and ongoing method of surveillance is needed to deter cyber attackers. In addition, automated systems are commonly used in the aviation industry. The cybersecurity threats of the aviation sectors have effectively been discussed in this dissertation. Along with that, the different forms of cyber hacks have also been represented in this work. The different methodological approaches along with the tools have also been outlined in this dissertation. Both primary and secondary data collection process has been used to source valuable information regarding cybersecurity threats in the aviation industries. The survey has been conducted with 100 people whereas 3 different cybersecurity experts of three different organisations have been interviewed to secure the primary quantitative and qualitative data collection method. Pie chart analysis has been used to analyse the collected information through the survey. At last, some of the recommendations have been provided that will help the aviation industries to strengthen the cybersecurity network and mitigate the risk.

Table of Contents

CHAPTER 1: Background and Objectives

Overview of the study

The aviation sectors contribute much to the economy of a nation. It is one of the safest forms of transportation. As it offers people to reach the destination at a short time, people have been using the flight to fly from one place to another not only within the country but also abroad. Many airports and airlines have been started in the last few decades. Moreover, many facilities are offered to the customers by the airport authorities such as user-friendly airlines, online baggage checking system, UBC (unnamed border controls) and online check-in (Lamb, 2018). Free Wi-Fi facilities are also offered to the customers which result in customers' satisfaction and when it comes to a comfortable journey, a flight has always been the priority for the customers. The technology has evolved much in the last few years and so as the risks of cyber threats. Information and communication technology (ICT) has been taken into consideration by the security engineers of airports to maintain the entire network and processes of the airport cybersecurity system (Kessler *et al.* 2018). ICT allows engineers to work and operate the internal network and if any major threat is detected then the alarm starts ringing within a fraction of second. The network infrastructure of the airports is critical as it has to handle a set of different operations at a single time frame to enhance the effectiveness of the air transport system. The US federal aviation administration (FAA's) in collaboration with JPDO (Joint planning and development office) has been working on Next-generation air transportation system which will benefit the airlines (Lykou *et al.* 2018). The advanced technology would provide a more short and precise route for the aeroplanes to reach the destination with a shorter time frame. Moreover, it offers enhanced flexibility and security. The air traffic control (ATC) would be handled from the satellite instead of ground which offers less risk to the data hack. Security is the most important thing for any airlines to be taken into consideration as millions of customers' data are processed each day through the networks.

Rationale

The cybersecurity has become the biggest concern for the airlines and airport authorities have been taking several security measures to mitigate this issue. It is one of the crucial factors that affect nearly all the transport modes. The rapid growth in the automation and digitalization in the fourth industrial revolution has enabled cyber attackers to cause damages to the aviation sectors (Lykou

et al. 2019). The most advanced and cutting edge technologies are used in the aviation networks to make it stronger and efficient agents the potential threats yet the advancement of technology has made the air transportation network more vulnerable to cyber-attacks. The diversified form of cyber-attacks harms the aircraft operations which could bring a disaster. It not only affects the operation of aircraft but also it has a significant impact on the passenger services, airport services, security and security of passengers and more significantly the economic steadiness of a nation. The aviation industry is globally interconnected and therefore the regulation and policies of cybersecurity in air transportation are decided and formed by international organisations (Urban, 2017). Each airport around the globe has to follow the regulations set by the parent organisations to make the operations working. This dissertation aims to critically identify and analyze the type of cybersecurity threats that exist for the aviation sectors that could damage the operations of the airports. Besides that, the cybersecurity policies and regulations for the aviation sectors will also be discussed in this dissertation work which will help the organisations to maintain the regulation act properly and mitigate the potential threats against cybersecurity. Moreover, this is one of the major topics to pay attention as security has become the most important part of any organisation. No major research has been conducted on this topic and it is very infrequent to find. The airport authorities must do a self-assessment to identify the weaker areas that are more likely vulnerable to cybersecurity threats (De Gramatica *et al.* 2015). This helps the organisations to build a strong system which could be able to resist the cybersecurity threats on the private data centres and networks and allow the business to be operated with success. Considering all the areas, this topic has been chosen to do extensive research on the topic and find some of the solutions to solve the issue related to the cybersecurity.

Problem statement

The cyber threats in the aviation sectors have become more evolved and persistent in the last few decades. The data breach is the most common factor of cyber threats and it can exploit the crucial information of an organisation (Duchamp *et al.* 2016). It has led the business organisations to develop a strong cybersecurity network that can offer maximum security against potential cyber threats. A computer glitch is one of the most famous forms of cyber-attack in which the attackers ensure that all the computer system of the target shuts down immediately and within a fraction of second the entire control is shifted to the attackers (Suciu *et al.* 2018). Many private and secure

information of customers is processed through the aircraft networks starting from booking tickets to the boarding. Therefore, the computer glitch can exploit a huge amount of customers' information just by a tap. Not only that but also they can regain the power to control the operations going on the aircraft systems. This could be the biggest threat, especially for the aviation industry. Social engineering is also an important form of cyber-attack to be taken onto account. Apart from that, malware and DDoS are common forms of cyber-attacks. Moreover, the wireless networks are broadly used in the aviation sectors and all the operations are performed using the wireless network. Cyber attackers can target only the parent wireless network to gain complete control over the entire system of the aviation sectors (Haass *et al.* 2016). The biggest cyber threats for the aviation sector are air trafficking control (ATC). ATC is the most vital part of the aviation sector which decides the route in the air for the aircraft by using the navigation. If the hackers manage to hack the server then this could be the biggest threats for the air transportation system. SDRs (software-defined radio technology) has been developed back in 1990 for the military and it was previously used for close communication. Using the COTS SDR hackers can easily steal the information of any flight. Because of these, all potential threats aviation industries seek to implement a strong cybersecurity network that will keep them away from this.

Research aim and objectives

The primary aim of this study is to identify the potential cybersecurity threats for the aviation industries and provide the remedies to mitigate the issues.

- To identify the potential threats for airport against cybersecurity
- To identify the challenges of ATC communication
- To identify the cyber threats for air transportation
- To provide the solution in order to mitigate the potential cybersecurity threats

Research hypothesis

H1: Malware threats positively impact the aviation sector

H0: Malware threats do not impact aviation sectors that much

H2: ATC communication issues have a positive impact on aviation sectors

H0: ATC communication issues do not have a positive impact on the aviation sectors.

H3: Cybersecurity policies and measures help mitigate the cybersecurity issues in the aviation sector

H0: Cybersecurity policies and measures do not help mitigate the cybersecurity issues in aviation sectors

H4: Advanced technologies contribute to mitigating the cybersecurity threats in aviation sectors

H5: Advanced technologies do not contribute to mitigating the cybersecurity threats in aviation sectors

Research questions

1. What are the potential threats for the airport against cybersecurity?
2. What communication challenges does Air traffic system face?
3. What can be the solutions to mitigate cybersecurity problems in airports?

Thesis outline

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

The cases and cyber-attacks have been exponentially increasing which has forced the organisations to incorporate a strong cybersecurity network and offer them immunity against the cyber threats. Cyber hackers have long been keeping their eyes on aircraft operations and many such cases of hijacking have been taken place using cyber-attack strategies. This could the biggest threat for the aviation industries and no such airlines expect this to happen. The significance of cybersecurity, conceptual framework, the importance of aviation industries and many other things have been assessed in this chapter that will help to identify the potential cyber threats for the aviation sectors. Not only identifying risk but also some of the security measures and policies have been discussed that ensures maximum security and security against cyber threats for the aviation sectors.

2.2 Conceptual framework

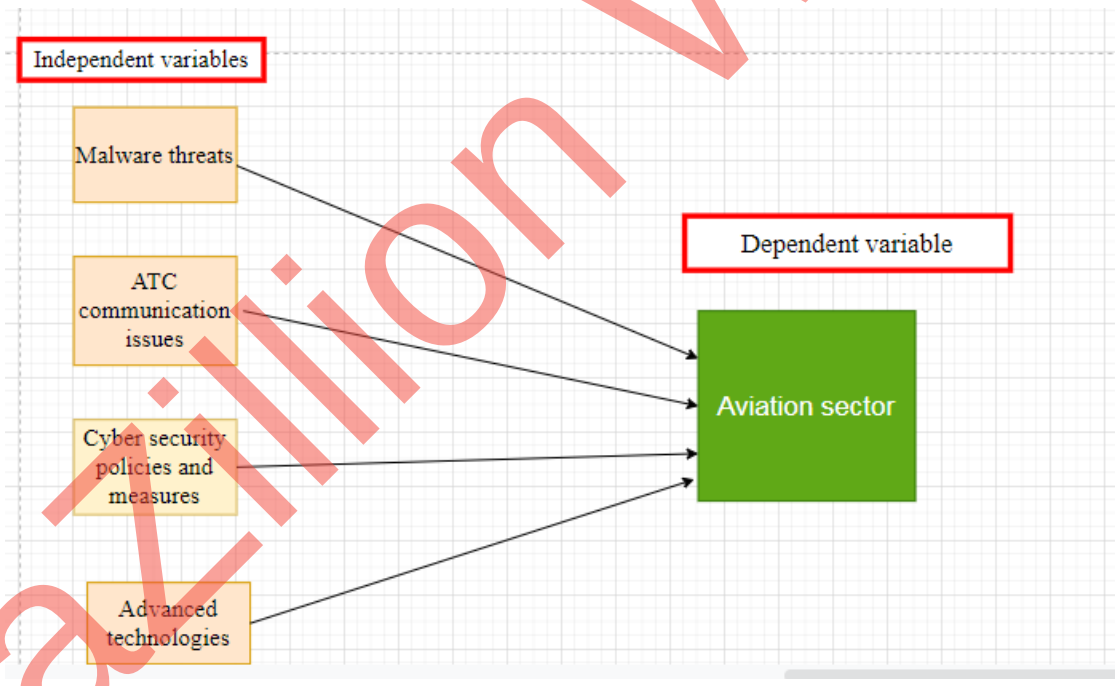


Figure 1: Conceptual framework

(Source: Learner)

The above picture represents the conceptual framework of the cybersecurity threats for the aviation sectors. The picture demonstrates that the aviation sector has been identified as the dependent

variable whereas the malware threats, ATC communication issues, cybersecurity measures and policies and advanced technologies have been identified as independent variables. The aviation sector is the centre focus of this study and providing the security and security for the aviation sectors is the main goal. As the aviation sector is dependent on some of the factors in terms of security and security that is why it has been represented as the dependent variable. On the other hand, malware threats are the individual factors that do not depend on the aviation sectors' security. For that reason, it has been represented as the independent variable. Besides that, ATC communication issues can cause the cybersecurity issues for the aviation sectors and for that reason the aviation sectors security is dependent on the ATC communication issue which is one of the important factors, this is the reason, and the ATC communication issue has been represented as the independent variable. Cybersecurity policies and measures likewise help mitigate the security issues for the aviation sectors and for that reason it has been identified as the independent variable. In addition, advanced technologies contribute to mitigating the cybersecurity threats for aviation sectors and there also the security factor of the aviation sector is dependent on the advanced technologies. This is why advanced technologies have also been represented as an independent variable.

2.3 Significance of cybersecurity and types of cyber threats

Cybersecurity has always been an important factor for business organisations to be taken onto consideration. It does not only affect the organisations but it has shown threats to human life. Because of that reason whether the individual or organisations seek to implement a strong cybersecurity architecture that can assure maximum security and protection against any type of cyber threats. Cybersecurity architecture contains some technological processes and control design that help protect the systems and networks so as to protect the data from cyber hackers (Shackelford and Russell, 2014). The network design of effective cybersecurity resists the cyber attacker to get into the network and steal information. Omnidirectional antennas are used to strengthen the signal frequencies. The control process of robust cybersecurity is based on the three factors such as processes, people and technology. These three factors help organisations to be safe from both the cyber-attacks performed by hackers and the accidental internal braches. The data integrity, confidentiality and availability are the three factors that are highly maintained in the strong cybersecurity controls.

The cybersecurity network has been invented keeping cyber threats in mind. There are lots of breaches taking place now and then. Much reputed organisation has also faced the consequences of data breaches because of poor cybersecurity design. Cybersecurity breaches not only affect the fund of an organisation but also puts the reputation of the organisation in danger in the marketplace (Lykou *et al.* 2020). A computer glitch is one of the common and framed attacks used by cyber attackers. DDoS (Distributed Denial of service) attack is such kind of attack in which the cyber attackers send multiple fake requests to a server in order to make it non-functional (Izuakor, 2016). The network is flooded with so many fake requests and it cannot work as usual. Sometimes the network shuts down immediately and that is the phase where the cyber attackers' stat stealing information form the network. One such incident took place in 2015 in which the networks and servers of the united airlines got hacked by cyber attackers the all the servers got turned off immediately for new few hours (Sans, 2020). Many flights have been cancelled during this time and it has caused the biggest trouble for the passengers. Although there was no report of property or life loss it leads to customer dissatisfaction.

In regards to the three pillars of above-mentioned cybersecurity, people have been playing a major role in minimizing cyber threats. The security personnel must make sure that all the network and server protocols are being properly updated and latest technologies are used to strengthen the security and data privacy (Watkins, 2014). Moreover, the operations and ongoing processes must be evaluated at each time frame so as to find any fraudulent or suspicious activity. There are many reasons for the organisation to develop a strong cybersecurity network. Security breaches cause a great loss for any organisation. This does not only include the asset loss but also it entails the penalties for violating data protection regulation act, reputation and customers. Moreover, the cyber-attacks have been more sophisticated and social engineering is one of the reasons for it (Kagalwalla and Churi, 2019). Hackers send some malicious links to the customers' end and manipulate customers to click on it. Once it is done they will get access to the entire system. Therefore it is important for the security engineers to be updated with such things so as to prevent themselves and the organisations from it.

2.4 Importance of the aviation industry

The aviation industries have become an integral part of the economy. According to a report of 2013, the network of airport transportation had carried more than 2.6 billion passengers and 48

million consignments. It has contributed to enhancing the economic value by 2.2 trillion dollars (Duchamp *et al.* 2016). Any cybersecurity issues in such scenario impose the highest level of threats in terms of economic and social consequences. With the constant development of the internet, an extra amount of threats are coming from cyberspace on the aviation industries. The main purpose of the cyber-attacks is to expose political and private information and make a profit by decreasing the strength of an organisation from all the aspects (Lykou *et al.* 2019). There are many layers of an aviation industry staring from the aircraft manufacturer to the passenger boarding. Many stakeholders are also involved in each process. The layers have been categorized into four parts such as the parent international organisation, government, airlines trading organisations and security system and aircraft manufacturer.

The ICAO (international civil aviation organisation) is the part of the UN whose work is to form and redefine the international aviation standards. The standards made by ICAO must be maintained by the other aviation organisations which raising any question. The board of members also take part in the decision-making process of ICAO and when a decision is made related to the aviation standard then it is circulated in different aviation organisations of different countries (Strohmeier *et al.* 2018). Security agencies and investigation organisations are part of the government whose work is to get involved in any happened incident to find out the root cause of the problem on behalf of a nation. “Bureau d’Enquêtes et d’Analyses (BEA)” of France and “national transportation security board (NTSB)” of USA are the perfect examples of it. They have the authority to formulate additional security standards and make it included in the guidelines of ICAO such as smoke detector has been used in all the airlines of the US which has been developed by NTSB. On the other hand, IATA (International air transport association) has the authority to investigate the security standards of airlines at an industrial level (Simmons, 2017). The network of IATA is widely spread to all the airlines of the world. There are many organisations who manufacture aircraft and the security systems such as Dassault, Honeywell, Boeing and Thales. Their main work is to constantly upgrade the entire security systems to find novel security threats and find solutions to mitigate the issues. It ensures the maximum security and security in each aircraft.

As aviation sectors have become the most important part of the economy, breaking the security standards and stealing information can be a great challenge for cyber hackers (Żmigrodzka, 2020). In addition, the information and communication technology (ICT) is widely being used in the

aviation sectors as it offers the maximum security against threats and allows the engineering to work inside the network in order to customize the processes whenever they want. As air transportation is the safest mode of transportation, it is necessary for the stakeholders to effectively identify the upcoming threats and solve as early as possible for the betterment of the organisations, people and the nation.

2.5 Potential cyber threats for aviation sectors

The aviation industries are no safe against cyber threats like all other industries. Boeing 777 aircraft uses a complex network system which uses the transponders to communicate with the ATC. The ACARS (Aircraft Communications Addressing and Reporting System) and onboard radios are used in such aircraft to exchange the information using the strong encryption method. The voice transmission techniques are disregarded in the aircraft which makes it quite impossible to hack. If cyber hackers have an excellent knowledge of the aircraft's operations then only they can cause a serious issue. Although some of the researches have proved that the security system of ACARS can be manipulated using the strong network system (Andreades *et al.* 2017). The navigation system has been found as much vulnerable to cyber threats. If attackers can establish a secure connection to the internet server of the aviation sectors then they can do anything with it. Such incident took place in 2006 in which "US federal aviation administration" was forced to shut down the ATC unit and cancel many flights as the internet server of Alaska got hacked. The information regarding the flights time and the customers' information are shred through a common network to all the airports which increase the chance of hacking. Therefore the aviation authorities need to strengthen the security as much as possible although high-security measures are maintained properly. The computers, air navigation. ATC control, airport ground control such as security screening and flight information are majorly being used in the aviation sectors and all the things are highly vulnerable to the cyber-attacks. If attackers are able to hack it then can operate the entire system.

The use of wireless data networks and wireless communication has exponentially been increasing in the aviation sectors for ground and aircraft surveillance. The blessing of technology has allowed developing the COTS (commercial-off-the-shell) hardware which can affect the functionality of the wireless communication system in aviation sectors (Pollard and Clark, 2019). Experience ground staffs are able to effectively handle the information of the aviation protocols and offer

maximum privacy against the threats. The development of SDRs can also cause security issues for the aviation industry. Using the SDR anyone can manipulate and resign the program using the available resources on the internet. It also allows the people to create an undetected data link. Using the COTS SDR, attackers can track each detail of a flight by sending the undetected link to the internet protocols of the aviation sectors (Anaedevha and Ajibola, 2020). If hackers are able to manipulate the information about the flight then it will be the biggest threats for the aviation industries. The SDR also allows the individuals to manipulate the channels of wireless communication using the aviation protocols which can be the major disadvantage for the aviation industries. Some of the threats types of aviation industries have been discussed below.'

Threats	Resources	Type	Motivation
Passive observers	Very low	Passive	Personal o financial interest
Script kiddies	Low	Active	Thrill
Cybercrime	Moderate-high	Active	Blackmail or financial gains
Cyber terrorism	Low-moderate	Active	Political motivation

Table 1: Threat agents for aviation industries

(Source: Anaedevha and Ajibola, 2020)

Passive observers are those people who accumulate information about the flight timings and movements from the protocols of ATC. Passive observers have been using the SDR receivers or web applications to track the ATC instead of actively interfere (Tan, 2015). The real-time information of ATC movements are shown in this software and the collected information can be used for several reasons such as military operation detection or privacy concerns. On the other hand, the script kiddies use less sophisticated attacks to gain the connection of the aviation network. They use to find the gaps in the network protocols of the air transportation system and frame the attack on the weak areas. They do not have a proper goal but they have been seeking thrill and recognition through noticeable impacts. Cyber attackers use the sophisticated attack and they often use the UAV (unnamed aerial vehicles) and SDR software to get connected with the

aviation networks being undetected. Their main purpose is to cause optimum damage (Suchodolski, 2018). Their main target is the ATC so that they can control the aircraft's movement, their main motivation is money. They can also frame the attack by hacking aviation networks through the internet. The attack can be performed either way. On the contrary, cyber terrorists mainly target the physical security infrastructure of aviation sectors. The network design of the cyber-physical system is quite complex and next-generation engineering tools are used in this system. The cyber terrorists find the vulnerabilities in ATC ad perform the attack on that particular area. The attack is performed in the ground from a certain distance and damage the entire unit physically.

2.6 Challenges of communication security in ATC (Air traffic system)

Five primary reasons have been identified that cause communication challenge in the ATC which has been discussed below.

Long development cycles:

The development of new technologies and the certification processes in the aviation sectors require a long time frame and sometimes it takes more than 2 years (Mathew, 2019). There are several testing and certification process for the better improvement of security in the aircraft. Moreover, the security testing process includes several steps and until all the security tests are completed, the certification is not given. Because of this reason, the development and certification process in the aviation sectors need more time. Although this process ensures the maximum security factors yet some of the security threat models are not being taken into consideration. In addition, the negative impacts of wireless communication technology are also overlooked in the testing session.

Compatibility and legacy requirements

Civil aviation is the global industry which connects with all the airports in different countries. The procedures and security protocols of the organisation must be properly understood by the other organisations. However, all the airspaces are not able to launch and maintain the procedures and protocols at a single time frame because the infrastructure and the airport authorities are not the same in each airspace (Baghdasarin, 2019). Moreover, all the airspaces are not capable of adopting the advanced technologies that have been made musts by civil aviation. Therefore, the airports are bound to make use of the old technologies in order to minimize the compatibility issues for air

traffic communication around the world. The old technologies are being used by some of the airspaces as a backup service.

Costs

There is high competition in the aviation industry and the costs of the equipment are too high. Therefore, existing equipment alternation is often avoided due to the high price segment. It is only used if the price is reasonable and it offers extra benefits over the existing one. Regulatory directives influence to change some of the critical requirements which additionally require a lot of time than usual (Camilleri, 2014). For that reason, the old equipment is used in the aircraft unless it gets completely damaged.

Frequency overuse

The number of aircraft has been increasing with the progressing of time and all of them share the same frequency levels. Some of the Frequencies of ATC has been locked up for the detection of UAVs which are to enter the airports in the future. It leads to the data packet loss due to frequency mismatch (Tounsi and Rais, 2018). It also affects the encryption method used for strengthening data security using cryptography methods.

Preference for open systems

The "International civil organisation" has planned the future protocols which are set to be released for open purposes which means the protocols can be accessible by authorities. The security and security issues that may arise in the future has been disregarded by this organisation. In order to measure the security and security issues in the aviation sectors, ICAO has released SRPS (standards and recommended practices) which is close-ended and only be accessible by the authorized airspaces which offer optimum security and privacy against the ATC communication challenges (Bair *et al.* 2017).

2.7 Efforts made to mitigate the issues

The rise of software difficulty is one of the most important things to be taken into consideration for the aviation industries. The software is becoming much more complex although it does not guarantee complete security against the threats. Therefore dealing with vulnerability has been considered as the most important factor for this industry which can aid them from this drastic

situation. Besides that, every functional software needs to be updated properly so as to detect new threats and malware (Lonzetta *et al.* 2018). Security test of software needs to be operated regularly. The topology of the aviation industry is much complex and there are too many stakeholders associated with this industry. Because of these reasons the origins of data breaches and the numbers are substantial. Moreover, blaming the stakeholders for a particular data breach or security attack is not beneficial for the organisations as there can be a chance of losing stakeholders for a company in such a scenario. In previous cases when a data breach or suspicious activity within the network was detected, vendors did not manifest any positive sign to identify or fix the problem (Tedeschi and Sciancalepore, 2019). Stakeholders would be accountable for any sort of breach or attack. In such a scenario, the manufacturer blames the suppliers and the supplier blames the manufacturer for the attack. Cabin and critical system on an aircraft are not separated which make it vulnerable to the cybersecurity threats. AFXD (avionics full dupleX) is the primary communication protocol that is used in the aeroplanes. It has been found that poor security has been offered by this protocol which again makes the entire system vulnerable to the security breaches.

The cybersecurity threats for the aviation industries have considerably been increased therefore strengthening the cybersecurity network in the aviation sectors have become the major concern for the stakeholders associated with this industry. Their primary goal was to identify the nature of threats effectively so as to come up with a proper solution to resolve the problem. They have made some major efforts to resolve the problem yet that was not enough. The computer-based operations are used much in the aviation sector and for that reason, the cyber threats for this industry have increased a lot (Skorupski and Uchroński, 2017). ICAO wanted collaborative work amongst the stakeholders and identify as many risks and threats as possible. A conference meeting was organized by ICAO so as to explain the attributes of cybersecurity with its pros and cons in the aviation sectors. ICAO has encouraged many countries to develop a strong cybersecurity network that offers maximum protection against risks and cyber threats. In order to do that, setting strong management was highly recommended by the ICAO. The primary goal of this is to maintain cybersecurity security and measures as much as possible to be safe from the upcoming cyber threats. According to the guidelines of ICAO, organisations must follow the cybersecurity security measures and implement it to a wide extent to prevent the cyber attackers that can bring negative consequences for this industry (Tam and Jones, 2018). The ICAO recommendation has also been including business resilience and crisis management. After the discussion, more or less all

countries have given a major focus on the cybersecurity. Many airports started implementing cybersecurity security measures and policies to make the technical department strong. A major focus has also been given on the system that has been exposed before due to the cyber-attack. The security measures have been considered for future aviation projects as well to minimize the risks of a cyber-attack (Trimble *et al.* 2017). Security has become the top priority for air transportation organisations. Besides that, IATA has decided to carry out a yearly audit to all the aviation sector in order to check whether the cybersecurity measures are properly maintained or not. It has later been confirmed by the governments that organisations would receive the advanced toolkits during the audit with the traditional approach of risk assessment. Manufacturers have also made some extra sort of efforts to starting the security and prevent the hacking of computer systems in an aircraft.

Although many security measures and efforts have been made by the aviation industries with the help of the government yet they fail to resist the potential cybersecurity threats. With the improvements of the technology, the cyber attackers are also adopting some advanced approach to exploit the vulnerabilities of the aviation sectors.

2.8 Cybersecurity in Air transportation and airports

The aviation industry is considered as one of the safest modes of transportation therefore the stakeholders need to pay high attention to the cybersecurity and security for passengers. They must adopt as much security, measures as possible while considering the privacy and security of passengers. The new cybersecurity threats will lead to loosing of potential customers as passengers have always been looking for the safest mode of transport. In order to maintain privacy and a high level of confidentiality, the stakeholders associated with aviation industries must come forward to take the initiatives to minimize the perceived security threats (Hasratyan *et al.* 2020). A continuous effort is much needed that can ensure optimum security against the cyber-attack. In order to deal with the security threats, the aviation industries must maintain all the policies and security, measures that have been proposed by the global agencies and experts.

The aviation sectors must focus on adopting the new strong security tests against potential cyber threats. Before attaching any devices to the onboard planes a systematic check must be applied with various layers. Internal security test is also important for strengthening the security measures of the computerized systems (Dancy and Dancy, 2016). Security experts have been playing a major

role in strengthening the security of a component moreover they will check the security of reach component independently in a much more advanced way. Moreover, airports have been found vulnerable to cyber threats. An information security system is widely being used in all the airports and if any sort of security breach takes place then it will have a positive impact on the passengers. A sophisticated cyber-attack results in monetary loss.

Four types of cyber threats can create hindrance by affecting the operational efficacy of the airports such as political, commercial spying, disruption and cybercrime. Most of the cyber-attacks are performed in the aviation sectors by intelligence sources or foreign military (Best *et al.* 2020). The purpose of these attacks is to gain information about political or military activities. These are also conducted to destroy the reputation of the organisations. Another reason for that is to make people hate the entire system. Disrupting the operations and seek attention is also the reason for this type of cyber tacks. The primary focus is given on the information of public and government agencies to keep an eye on the movements of a nation. A cybersecurity threat can damage public trust in the national airspace system (Johnson, 2016). On the other hand. The commercial spying is another type of cyber threat for the aviation sectors which intends to destroy the confidential information of government and public agencies. Monetary gain is one of the primary reason for framing this type of cyber-attack. They target the airport construction, palling, government document and public.

Disruption is the third kind of cyber-attack that aims to create disturbance in the harmony of an operation. This type of attack disrupts accessing the resources. These attackers have a wide agenda and they aim to destroy the network and make it nonfunctional so that the system automatically rejects the user requests. DDoS is such type of attack which is mostly being used for the disruption. It floods the network of an organisation with so many fake requests and after a certain time, the server stops responding. Later the confidential information is stolen from the servers of the airports. More and more traffic is sent to the website of the airports which makes it non-operating. The fourth category is the cybercrime which is the most and common form of cyber-attack in the airports. In cybercrime, attackers aim to steal the personal information of the passengers such as credit card numbers, customers;' identification and the banking information (Chirichiello *et al.* 2017). This information is often sold by the attackers to the third parties to make money.

Cybercriminals have been targeting the airports as it contains many customers banking and personal information which are stored in the computer systems of the airports.

2.9 Cybersecurity measures and policies

The cybersecurity action plan was signed on 5th December 2014. The undersigned organisations were The airport council international (ACI), the civil air navigation services organisation(CANSO), IATA, ICAO, the international coordination council of aerospace industries associations (ICCAIA) and the aerospace and defence industries association of Europe (ASD) (Rodrigues *et al.* 2019). They all have agreed to sign some of the declarations and follow some commitments.

They all have agreed upon establishing a collective understanding of cybersecurity threats and risks in the aviation sectors. In addition, they all settled to share a common risk assessment. The common language and terminology were decided to implement a, amongst them. They have also decided to clarify joint positions and recommendations. A simple and comprehensive cybersecurity approach was decided to be implemented for normal people (Κοσσένα, 2019). Coordinated cybersecurity measures, policies and strategies were decided to be reintroduced for the industry and state-level aviation sectors. Dynamic cybersecurity measurements have been made mandatory. The older cybersecurity protection and standards will be kept functional and at the same time, new security standards must be created according to the decision. New sort of devices was decided to be introduced to facilitate communication and information forwarding (Alqushayri, 2020). Besides that, the threat identification, evaluation of the existing defence system and incident reports would be generated as per the collaborative decision. They have also decided to share the security-related information in order to create awareness amongst the employees in the aviation sectors. The existing security policies, principles and the defence system must be redesigned as per the requirements. The roadmap of the civil aviation security cyber plan has been discussed below.

Commitment	Short term	Midterm	Long term
Developing a common	Task: threats and risk matrices analysis	Develop a security panned paper	Review the existing cybersecurity to identify the threats

understanding of cybersecurity threats	Deliverables: evaluation of the identified risks		and update the risk evaluation
Share risk assignment	Contrasting risk analysis from the perspectives of different stakeholders	Sharing risk assessment report to every industrial level	Identify the high-level threats at the industrial level through the reviewing process and update the evaluation report
Common language and terminology	Promoting the frameworks and existing standards	Glossary of terms for ICAO guidance resources	Submit the updated communication report
Joint position and recommendations	Mutual agreement on the terms of cybersecurity action plan and sign the declaration paper		Deliver input for developing regulation standards.
Demonstrate a comprehensible cyber threats approach to the public	the format and the communication strategies must be agreed by all the stakeholders		Submit the updated communication report

Table 2: Roadmap of the civil aviation security cyber plan

(Source: Alqushayri, 2020)

Apart from that draft assembly resolution, ICAAT (ICAO civil aviation authority tools), ICARD (International codes and routes designators), implement, SIMS, (security information monitoring system), Declaration of cybersecurity in aviation sectors, global aviation security plan, first transport cybersecurity conference, aviation information sharing and analysis centre and

Eurocontrol are the important cybersecurity policies that have been implemented till date (Ian *et al.* 2019).

2.10 Security measures to mitigate cybersecurity issues

Some of the security measures have been proposed by the international aviation organisation in order to effectively detect and prevent cybersecurity threats for the aviation sectors. Some sort of mandatory baselines has been provided by the parent organisations which needs to be followed by the fellow aviation sectors so as to be safe from the cybersecurity threats and run the business with success (De Zan *et al.* 2016). The security measurement steps against cybersecurity threats have been discussed beneath.

Developing measurable baselines

Developing the measurable business norms for the aviation sectors are the most important thing to be taken into account for the aviation industries. The most important thing is to develop a baseline for the data volumes, data transmission and times (Shukla *et al.* 2019). It enables the airlines to detect a particular area where an event has taken place which is not included in the norms.

Develop training and education process

Ground staffs are one of the important aspects of aviation industries as the control of the ATC is done by them. The complete route map and the communication with the aircraft are maintained by the ground staffs (Nikolova, 2017). Therefore, it is important to teach them about the cybersecurity so that they can be able to detect any suspicious activities if occurs. The training and education on cybersecurity will not only help them to identify the upcoming threats but it also will help them to deal with the threats and find the possible solution to mitigate the aroused threats.

Priorities and scope assets

The most important thing is to give the priority to the assets. A high focus also needs to be paid on the capability detection technique such as personal data of customers which can be fetched from operational systems and the credit card information of passengers (Lewallen, 2020).

Internal collaboration

Aviation sectors must build a combined system within their organisations. The cross-functional operation model must be broken down and an incident response process must be entrenched into the operations (Emanuilov, 2019). It will help the organisations to work on a single goal and the detected issue will be solved in a much more effective way. If any breach is detected then all the organisations will be alerted and they all can help collectively the victim organisation to get over the situation. It will also enable them to react more proactively when a breaching issue is detected. The threat monitoring process will also be improved for all the aviation sectors using this particular step which will definitely help mitigate the cybersecurity threats in the aviation industries.

Hire quality expertise

The expert security analysts need to be hired in the aviation sectors. The experts can easily detect cybersecurity threats as compared to inexperience engineers. Moreover, the nature of the threat can easily be identified by the experienced security engineers (Hasratyan *et al.* 2020). It will be tough for the cyber attackers to manipulate the experience security analysts and collect the information from the existing cybersecurity network of the aviation sectors. The expertise has a deep knowledge of the cybersecurity network of the enterprise level, domains, and internet protocols. Therefore they can easily track the IP of the paired device which is connected with the cybersecurity network of the aviation sectors in real-time so as to effectively prevent the cybersecurity threats.

2.11 Contributions of technology to deal with cyber threats

SITA and airbus have recently presented a new customized service operation centre for meeting the specific needs of air transportation (Lamba and Kandwal, 2019). If any suspicious activity is found within the existing network of the aviation sectors then this security service will capture and detect the threat easily. It is beneficial for the aviation industries as well as for its stakeholders and airlines. Most of the aviation industries seek to implement this cutting edge technology so as to prevent the cyber attackers from entering the network and manipulate the private information. It has the capability of providing remedies for cybersecurity threat for the communication network used in the aviation sectors. Airbus is connected majorly with the government, defense and airline companies so as to prevent the intruders and it has even the ability to detect the sophisticated cyber-attacks. The expertise is appointed who has a deep knowledge of this new technology and

compatible with all its features. The technology and expertise together have been working to mitigating the cybersecurity risks for air transportation.

The multidirectional antennas of high-frequency level have been attached in the chip of the hardware that can cover the wider range of the wavelength and it provides the real-time monitoring facility for the communications and applications related to incident response and air transport. A dedicated portfolio of cybersecurity is being generated by SITA that helps the airlines to identify the nature of cyber threats and protect the company's assets from cyber threats (Aboti, 2019). Airbus cybersecurity is one of the important software to pay attention to. This software ensures the maximum protection against a cyber-threat for the airlines and the defenses. If any sort of disturbance in the network is found then it immediately responds and takes quick actions to resolve the issues related to cyber-attacks. SITA is the leading IT communication and transport specialist who provides the support for ICT to the aircraft, airlines and ground handlers. The infrastructure of the network and global services are thoroughly being taken care of by this software. In addition, it also takes care of passenger operations, commercial management, ATC communication, aircraft operations, baggage systems and transportation security. Besides that, the aviation industries seek to implement a sophisticated network architecture that can offer maximum data privacy. In order to do that, they are inclined to adopt the IoT (internet of things) security. Cloud storage is going to be accessed by the air transportation industries to store the sensitive information and there is a less chance of data leakage of data loss (Bhatia *et al.* 2016). Furthermore, multi-channel authentication and network access control technology is expected to be used by most of the aviation companies so as to strengthen the cybersecurity architecture.

2.12 Summary

Many technologies are being used in airports which are technically way advanced. The risk assessment programs are often held in the airport by the government of private major organisations so as to check the strength of the security at each level. All the possible security measures are thoroughly being checked yet still the airports are no immune against the cyber threats and the risks are increasing each day. Every airport organisation must follow the security measures as much as possible in order to prevent the cyber attackers. In this chapter, the cybersecurity threats for the aviation industry have been thoroughly discussed. The organisations are mainly facing issues with the ATC communication which is considered as the most vital things for an aircraft

operation. The challenges with air trafficking control system have also been outlined in this chapter. Cybersecurity security measures and policies that have been announced by the international aviation organisation has also been included in this study which ensures optimum security and protection against cyber threats. Furthermore, the contribution of the cutting edge technologies such as cloud computing and IoT to mitigate the cyber risks have also been discussed effectively in this chapter which will help the organisations to identify the cyber threats efficiently and resolve the issues as early as possible.

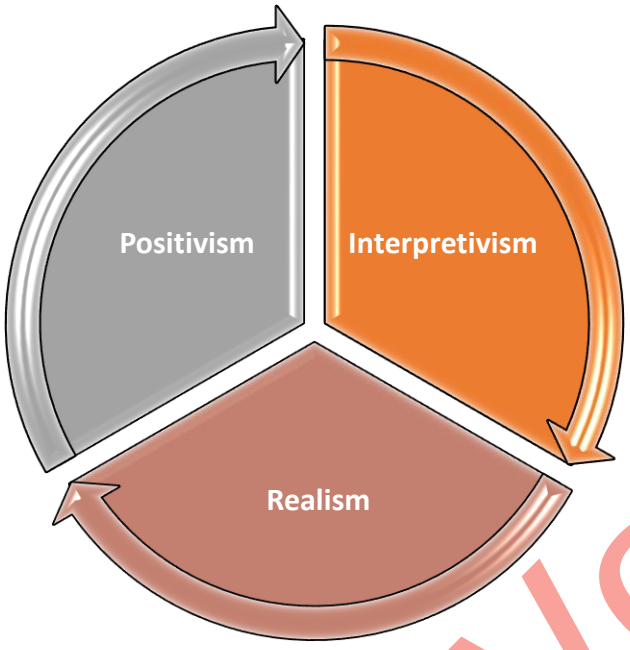
CHAPTER 3: Research plan

3.1 Introduction

For each research, the methodology is one of the vital things for the researchers. The biggest advantage of using the research methodology is that it provides a systematic approach to the data collection and data analysis process. It includes some sort of techniques and processes that helps in analyzing the information on the topic. It moreover helps in checking the overall reliability and validity of the paper by evaluating the study from all the aspects. In the research methodology section research philosophy, approach, design, data collection process, data analysis, sampling and population, validity and reliability has been outlined. Moreover, the ethical aspects related to this research have also been discussed in this chapter. Furthermore, the research constraints have also been included in this chapter.

3.2 Philosophy

Research philosophy helps the researcher to clarify the assumptions of the topic by gathering a vast knowledge about it (Ryan, 2018). All studies are conducted based on some of the broad assumptions therefore it is important for the researcher to filter the assumptions properly which helps in fostering the research. Research philosophy defines the belief of the researcher about the process of data collection based on which the data analysis would be done. Clarifying the research philosophy is the primary stage for the researchers while carrying out any research. There are mainly three types of research philosophy such as positivism, pragmatism and realism (Tumele, 2015).



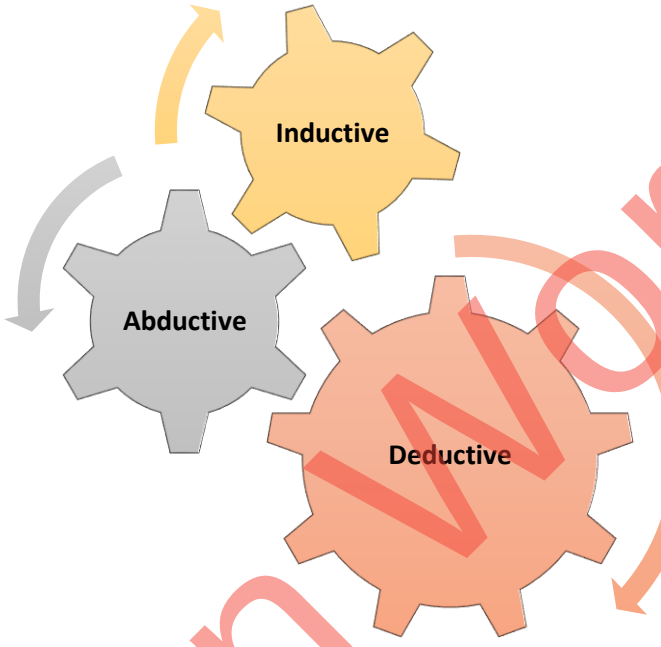
Justification

The positivism philosophy has been used to carry out this dissertation work. Positivism research philosophy depicts that only the factual data which has been collected through observation will be taken into account by the researchers while conducting any research. Therefore the positivism philosophy has helped in collecting only the factual information about the provided the topic. Moreover, no broad assumptions have been used while carrying out this dissertation work. This particular method limited the movements towards the effective data collection process and the research findings have been considered as quantifiable. In addition, positivism philosophy has helped in meeting the objective 1 which is "To identify the potential threats for airport against cybersecurity". While researching on identifying the threats and challenges for the aviation sectors, the observational data has been noted down. Only including the factual data has helped in making the research work much more compact and true to the source. Furthermore, the positivism philosophy has helped simplify the potential cybersecurity threats for the aviation industries.

3.3 Approach

The research approach includes a systematic plan and process that undertakes several broad assumptions to the detail data interpretation, collection and analysis (Woiceshyn and Daellenbach, 2018). It is one of the vital movement of the researchers to be taken into account while carrying out any sort of research. It moreover helps in choosing the simplest way of collecting the data

efficiently. However, the most important thing is to identify the nature of the problem form the current study as the whole process of approach depends majorly on it. The research approach is essentially divided into three parts such as inductive, abductive and deductive approach (Johnston, 2014).



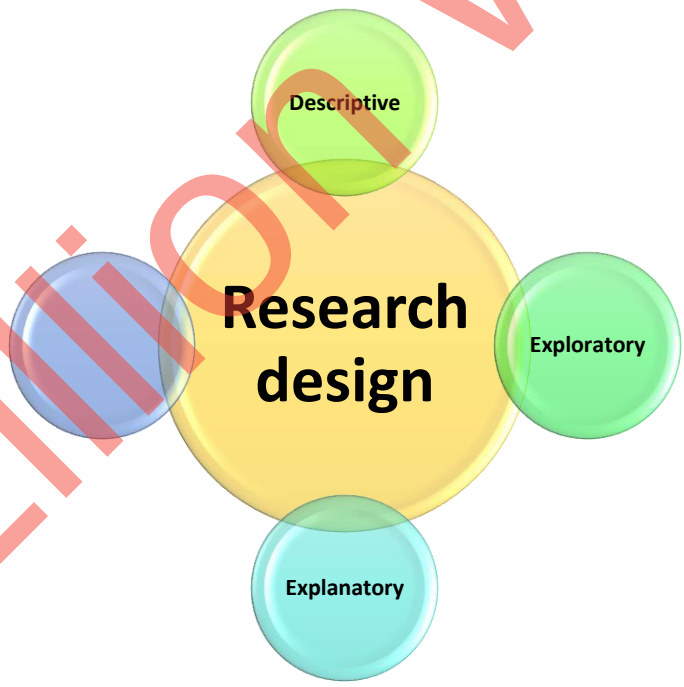
Justification

The deductive approach has been chosen so as to carry out the dissertation work with success. The deductive approach has helped in satisfying objective 3 which is "To identify the cyber threats for air transportation". In addition, it has helped in identifying the different variable that was used in objective 2 such as air transportation and cyberthreats. Moreover, it has guided to pick the proper information of the variables from the internet which is relevant to the topic. Some sort of the broad assumptions have been considered while conducting the study but as the research topic was "dealing cybersecurity threats of automated systems in the aviation sector", the assumption that was taken into consideration was relevant to the topic. No other major assumptions have been entertained while conducting the research and besides that, the deductive approach has helped in collecting observational data which later has helped much at the time of analysis the collected information. It has contributed a little to meet of the objectives so as to foster the dissertation work successfully and generate the best outcomes. As the deductive method has helped make the data

collection process easier, analysing the information has also been easier. Apart from that, no false information about the cybersecurity and the aviation sectors have been provided in this study that can mislead anyone. Because of all these benefits, the deductive approach was found to be suitable for this dissertation work and hence has been chosen to complete the research work.

3.4 Design

Research design includes all the strategies that are most important in terms of integrating the different components and variables involved in research in a logical and coherent way. However, identifying the research problem is one of the important parts before choosing the proper research design. Research design establishes a blueprint for the data interpretation, collection and analysis method (Nassaji, 2015). The research design is broadly classified into three parts such as exploratory design, explanatory design and descriptive design. Based on the nature of the research and the addressed problem, the research design is chosen by the researcher so as to carry out the research without any hassle and collect the desired outcomes.



Justification

The descriptive research design has been chosen to conduct the research work. As the descriptive approach directly indicates the aim and objectives of the research, it has helped to be aim and

objective oriented. The primary goal of any dissertation is to satisfy the aim and objective that has been addressed at the beginning of the work. Descriptive research design has made it possible and helped in making the research work more compact. Moreover, it has helped in satisfying the objective 2 and 4 which are" To identify the challenges of ATC communication" and "To provide the solution in order to mitigate the potential cybersecurity threats". Furthermore, the descriptive research design has helped in finding the detailed concept of cybersecurity threats through the data collection process. It has been discussed in detail in the data analysis chapter. The term "cybersecurity threats" has been addressed as the natural variable and other variables such as aviation sectors, ATC communication has been arranged sequentially by the help of descriptive research design. Additionally, it has helped in comprehending the research problem effectively and complete the rest work based on the problem statement. The deductive approach has helped in finding the solutions for mitigating the cybersecurity issues in the aviation sectors. Because of its wide range of benefits, the deductive approach was a suitable method to continue the research work further.

3.5 sampling and population

Sampling and population are also one of the important aspects of research which includes both individuals and the items. However, the objects are also considered as a part of samples. The population is the centre area from where the samples are chosen (Taherdoost, 2016). It has a great contribution to the data analysis and often a satisfactory amount of samples are chosen to do that. It helps provide real-time information.

Justification

Random sampling technique has been chosen to carry out this dissertation work. It provides the equal opportunity of being chosen as samples from a large population. Moreover, it allows the samples to be chosen in an unbiased way. As the online survey has been performed to secure the primary quantitative data collection method, the sample size is 101 and the population is 220. The 101 samples were chosen using the random sampling technique. On the other 3 security experts have been chosen using the random sampling technique in an unbiased way. It has helped include only the three consultants who have the experience of working as a security expert in the aviation sectors for more than 2 years. The newly joined employees have not been considered in this context and they have been discarded using the random sampling technique.

3.6 Validity and reliability

Validity and reliability offer the concepts of assessing the quality of the research. The method and the processes used in the research to evaluate the variable involved in it are checked by the validity and reliability. However, the validity indicates the legitimacy of the information fetched through the data collection process (Mohajan, 2017). Moreover, the authentic, real-time and valid information makes the overall research valid. It has been ensured that no false information is added. Only the appropriate information with proper in texting has been included in this study which indicates that the validity of this dissertation work is justified. On the other hand, the reliability checks whether the current research has used the same theory and models as compared to the previous papers or not. The outcomes of the research have also been compared with the previous studies and the similarities have been found in results with the previous papers which has made this dissertation work more reliable. Only the valid, tested and verified data has been used in this research work form the previous research papers. Furthermore, authentic data sources have been used to carry out this research paper and to make it more reliable as compared to others.

3.7 Ethical consideration

Ethical aspects are one of the vital things for the researcher so as to enhance data privacy. Ethical aspects have been put at the frontline of this research work. Ethical aspects moreover help in increasing the validity and authenticity of the research works. Confidentiality of information is the most important thing for a researcher to be taken into account. The collected responses from the participants have been kept securely for the analysis. As the study intends to use the online survey, human participants are engaged in this. Therefore, it has become too important to look after the data privacy. The responses have been collected after taking positive agreements from the participants. Besides that, before accessing the information positive agreements have also been considered. All the responses have been kept to maintain high data privacy and data are securely stored under the data protection act 2018. IATA and ICAO websites have been reviewed in order to source valid and authentic information about the cybersecurity security measurements in the aviation industries. It is also asserted that no unethical work has been done and no fake information has been provided in this research work. Private information of the participants would not be exposed outside and the collected information will bring no harm to any community or organisation.

3.8 Research gap

Time and budget constraints have been identified as important barriers for this research. The time for this dissertation was limited and it has to be completed within that limited timeframe. Therefore, it was difficult to explore the literature part of this topic and find more valuable and undiscoverable information about the cybersecurity issues in the aviation sectors. Moreover, due to less time, the data collection process could not be executed as effectively as it could have been. It has also affected the data analysis as well. If this constraint had not appeared in the way then the consequences could have been much improved. The second constraint was the budget limitation. Due to the low budget, some of the paid websites could not be accessed otherwise the data analysis could have been performed in a much effective way by including detailed information. In addition, top-notch technologies such as cloud storage and IoT could not be implemented in this research because of the low budget. The resources could not be used effectively because of the low budget. If these limitations never appear then there was a chance of generating much-improved output.

3.9 Summary

Different kinds of methodological tools and techniques have been discussed in this chapter which has contributed much in fostering this dissertation work. The positivism philosophy has been used which has helped in sourcing the factual data. In addition, the descriptive design has been chosen so as to identify the research problem and meet the objectives. Besides that, the deductive approach has been selected which has helped in taking some of the broad assumptions into account which is relevant to the cybersecurity issues. Moreover, the mixed data collection method has been used to frame the dissertation work. The online survey has been conducted to secure the primary quantitative data collection method and the for the secondary qualitative data collection method, thematic analysis has been carried out. SPSS tool has been used to analyse the data effectively. Random sampling technique has been selected to choose 101 participants out of 220 population in an unbiased way. Furthermore, the ethical aspects have been maintained throughout the dissertation work and all the responses have been kept under high security.

Chapter 4: Data Collection, Presentation, Analysis and Findings

4.1 Introduction

The primary data collection method has been used in this dissertation work. The survey has been carried out to secure the primary data collection method. The security personnel of the aviation sectors have been surveyed and the collected responses have been analyzed using the Likert scale. On the other hand, in order to secure the primary qualitative data collection method, 3 of the security personnel has been interviewed. The pie chart analysis and the interview has been performed in this chapter.

4.2 Data collection

The data collection process is considered as the most important mechanism of the research work. The most significant part of the data collection is that it has a huge contribution to the data analysis process (Choy, 2014). The more effectively data is collected the more efficiently the data analysis will be. The main focus of the data collection process is solving the research questions and the data is collected in such a way so that the researchers can meet the research questions. In order to do that, the first thing is collecting the authentic information and for that the sources from where the data is collected need to be authentic first. The data collection process is essentially classified into three parts such as primary data collection method, secondary data collection and mixed data collection method (Cyr, 2016). The primary data collection method is again divided into two parts such as quantitative and qualitative method whereas the secondary data collection is qualitative.

Justification

The primary data collection method has been chosen so as to foster this dissertation work. It has helped in collecting valuable information about the cyber threats in aviation sectors from the security consultants working in the aviation sectors. On the other hand, to secure the primary qualitative data collection method, 3 cybersecurity experts of 3 different aviation organisations have been interviewed face to face. They have been asked 10 questions related to the cybersecurity threats in the aviation sectors and all of the responses have been stored to foster this dissertation work. The interview process has helped collect the individual opinion from the security experts of the aviation sectors.

The effectiveness of data analysis completely relies on the effectiveness of the data collection process as discussed before. The mixed data collection method has been adopted to foster this research work. An online survey has been conducted to secure the primary quantitative data collection method. The Likert scale ranging from 1 to 5 has been used to analyse the collected responses from the participants and generate the best outcomes.

4.3 Quantitative data collection (Survey)

In the primary data collection method, a survey questionnaire has been prepared which comprises 14 questions related to the cybersecurity. The questionnaire has been sent to the different

cybersecurity experts of different aviation industries. The online survey has been conducted to collect the responses from the security consultants. Questions have been collected from Survey Monkey and some other websites. The questions which are relevant to the cybersecurity have only been added in the questionnaire. The Likert scale has been performed to analyse the responses. The responses from the participants have been stored electronically and pie chart analysis has been used to effectively analyse the collected information. The questions that have been asked, are presented below.

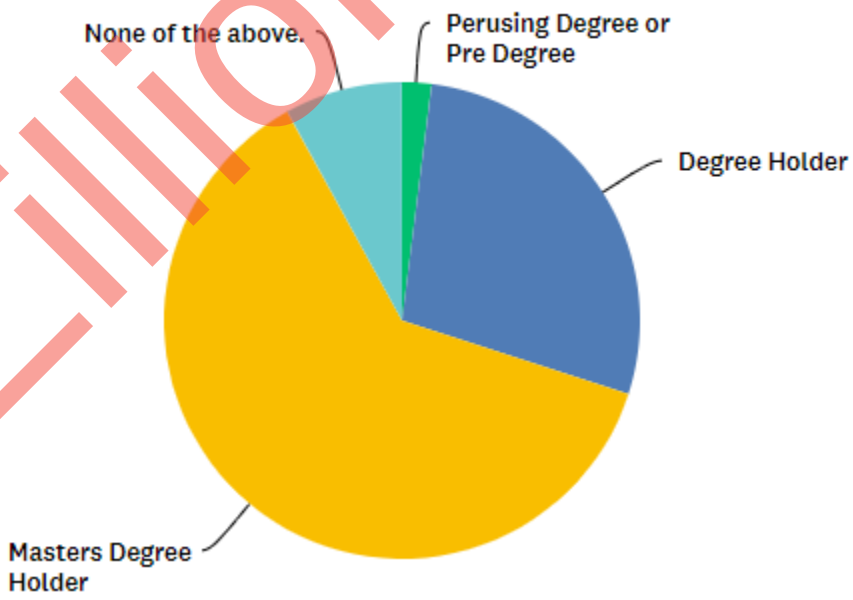
Question 1	**What is your educational qualification?**
Question 2	**In which operational area you are currently working with?**
Question 3	**For how long have you been working as security personnel in the aviation sector?**
Question 4	**In which operational area you are working in the aviation industry?**
Question 5	**Do you, as a registered aircraft operator, consider cybersecurity as a risk in terms of your airline operations (i.e., flight operations, ground operations, airport operations, maintenance, and engineering)?**
Question 6	**If you, as a registered aircraft operator, consider cybersecurity as a risk in terms of your airline operations, please indicate the risk level frequency by using the three-point scale:**
Question 7	**What kind of support would you, as a registered aircraft operator, find it useful for your airline operations?**
Question 8	**The use of approved, independent companies to objectively assess the cybersecurity of aviation products and services is useful to gain insight into risk**
Question 9	**Is it not possible to 'hack' aviation systems?**
Question 10	**How often does your organization conduct exercises replicating aviation cybersecurity incidents?**
Question 11	**Is it easy to incorporate cybersecurity best practice into purchasing aviation-related hardware/software/services?**

Question 12	**Are your operational staffs enough trained to recognize a potential aviation cybersecurity incident?**
Question 13	**Does your organization include cyber insurance as an element of managing our aviation cybersecurity risk?**

4.4 Analysis of survey

Question 1: What is your educational qualification?

Option	Responses	Responses%	Total respondents
Perusing Degree or Pre Degree	2	2%	100
Degree Holder	28	28%	100
Master's Degree Holder	62	62%	100
None of the above	8	8%	100

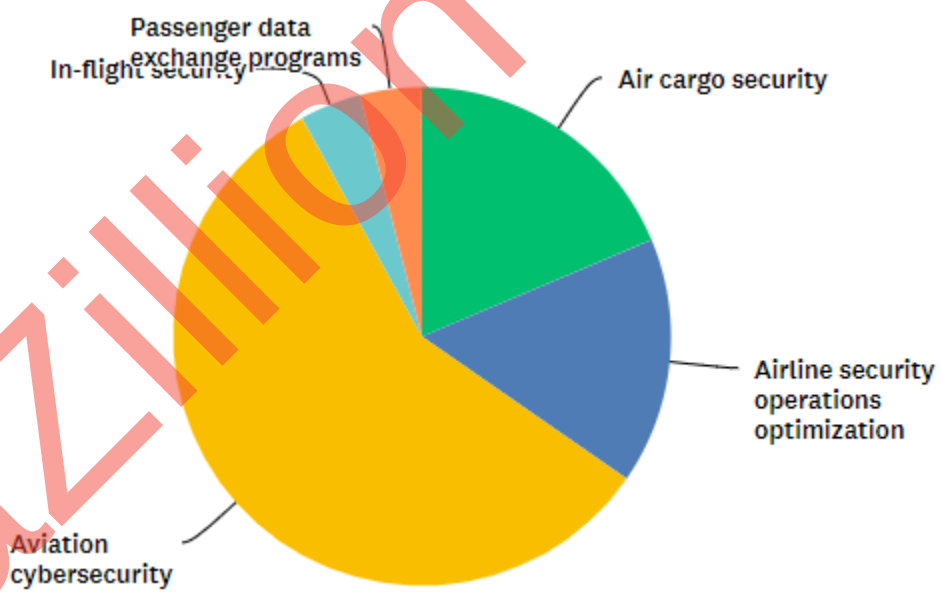


Question 1: What is your educational qualification?

Findings: As per the above graph and table, 62% of the respondents have the educational qualification of master degree and 28% of the respondents are the degree holder.

Question 2: In which operational area you are currently working with?

Option	Responses	Responses%	Total respondents
Air cargo security	14	18.67%	100
Airline security operations optimization	12	16%	100
Aviation cybersecurity	43	57.33%	100
In-flight security	3	4%	100
Passenger data exchange programs	3	4%	100

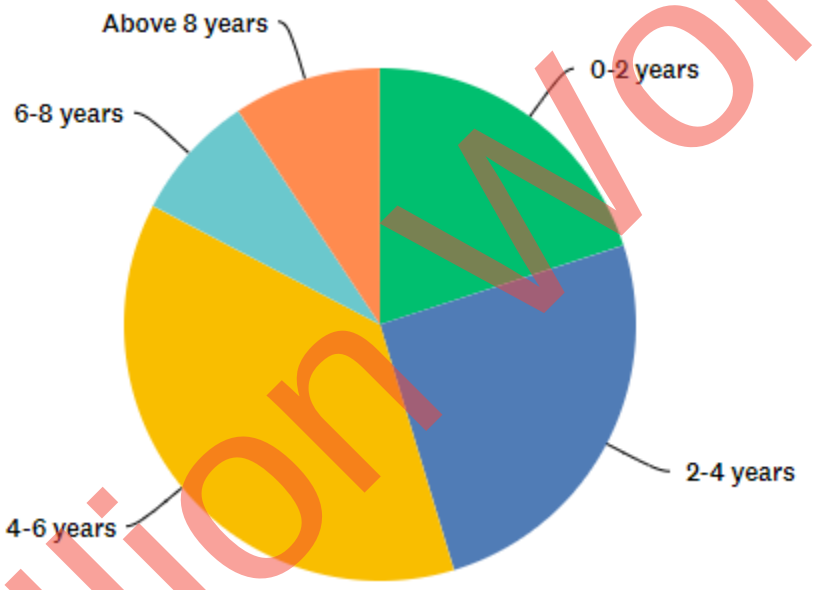


Question 2: In which operational area you are currently working with?

Findings: As per the above graph and table, 57.33% of the respondents work in the aviation cybersecurity sectors and 18.67% of the respondents work in air cargo security.

Question 3: For how long have you been working as security personnel in the aviation sector?

Option	Responses	Responses%	Total respondents
0-2 years	15	20%	100
2-4 years	19	25.33%	100
4-6 years	28	37.33%	100
6-8 years	6	8%	100
Above 8 years	7	9.33%	100

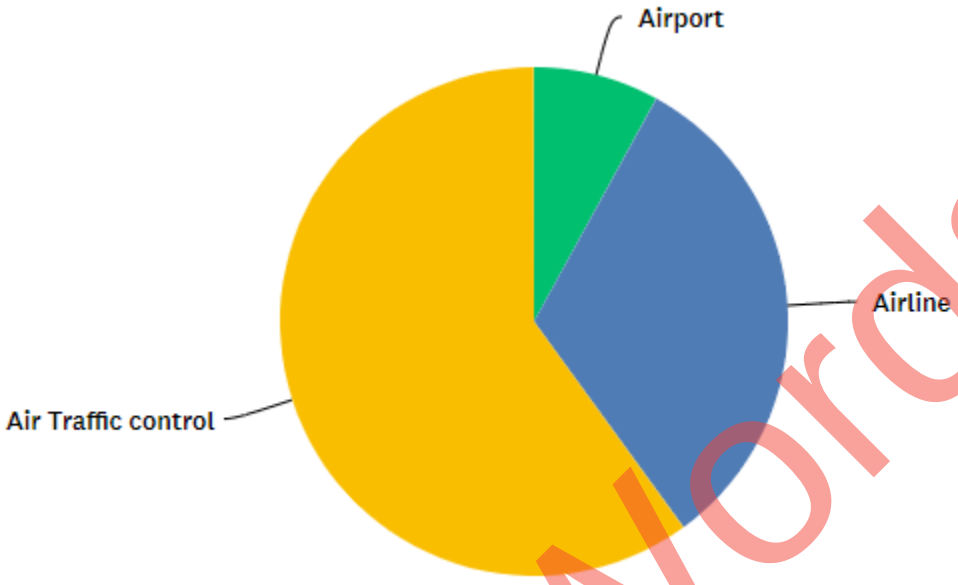


Question 3: For how long have you been working as security personnel in the aviation sector?

Findings: As per the above graph and table, 37.33% of the respondents have been working as security personnel in the aviation sector for 4 to 6 years whereas 25.33% of the respondents have been working as security personnel in the aviation sector for 2 to 4 years.

Question 4: In which operational area you are working in the aviation industry?

Option	Responses	Responses%	Total respondents
Airport	6	8%	100
Airline	24	32%	100
Air Traffic control	45	60%	100

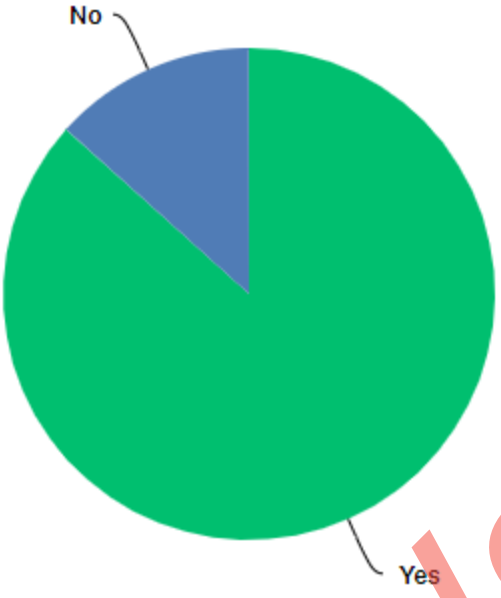


Question 4: In which operational area you are working in the aviation industry?

Findings: As per the graph and table, 60% of the respondents have been working in the air traffic control whereas 32% of the respondents have been working in the airlines.

Question 5: Do you, as a registered aircraft operator, consider cybersecurity as a risk in terms of your airline operations (i.e., flight operations, ground operations, airport operations, maintenance, and engineering)?

Option	Responses	Responses%	Total respondents
Yes	52	86.67%	100
No	8	13.33%	100

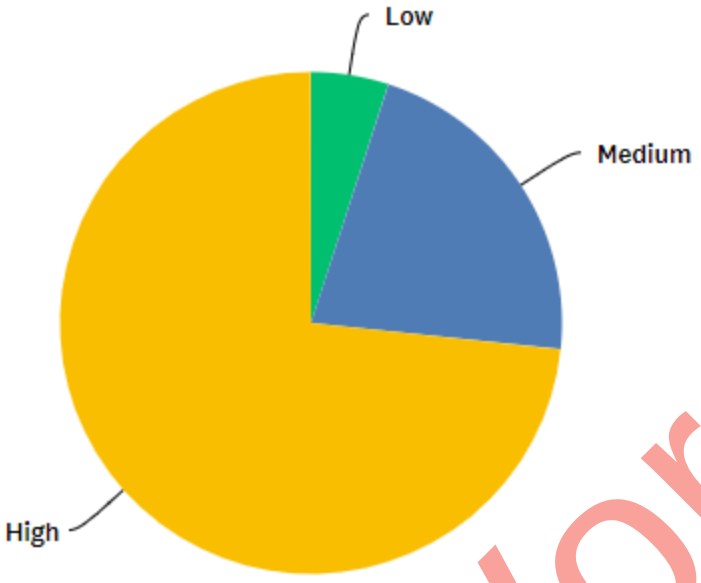


Question 5: Do you, as a registered aircraft operator, consider cybersecurity as a risk in terms of your airline operations (i.e., flight operations, ground operations, airport operations, maintenance, and engineering)?

Findings: As per the graph and table, 86.67% of the respondents believe that cybersecurity is the risk for the aircraft operation whereas 13.33% of the respondents believe that cybersecurity is not a real risk for the aircraft operation.

Question 6: If you, as a registered aircraft operator, consider cybersecurity as a risk in terms of your airline operations, please indicate the risk level frequency by using the three-point scale:

Option	Responses	Responses%	Total respondents
Low	3	5%	100
Medium	13	21.67%	100
High	44	73.33%	100



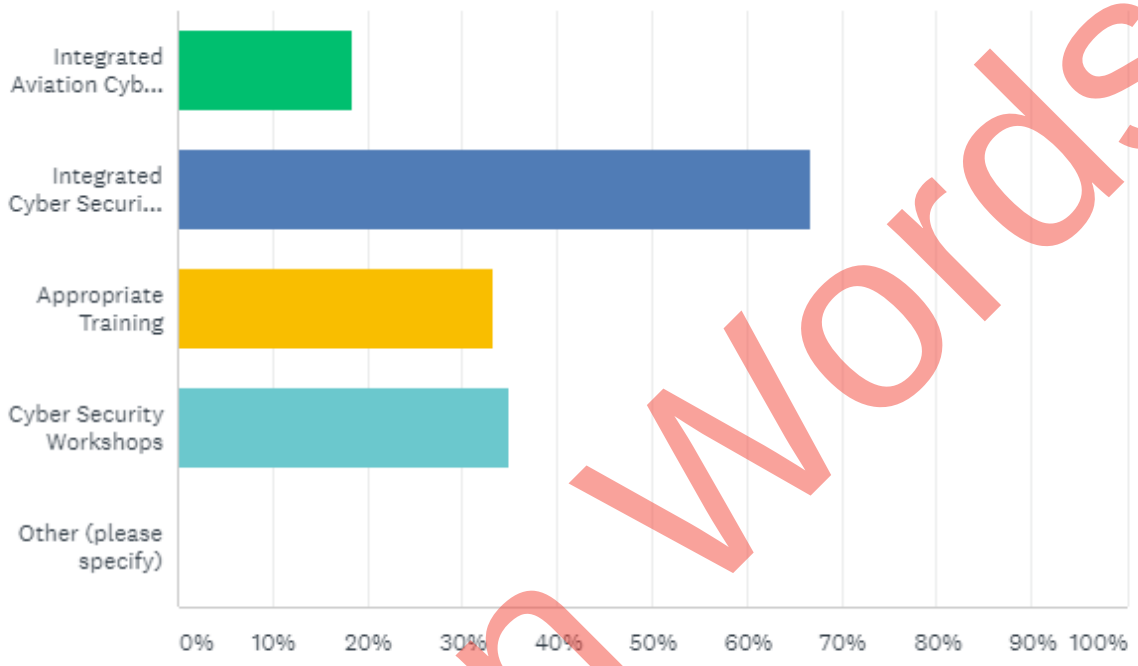
Question 6: If you, as a registered aircraft operator, consider cybersecurity as a risk in terms of your airline operations, please indicate the risk level frequency by using the three-point scale:

Findings: As per the above graph and table, 73.33% of the respondents consider cybersecurity as a risk in terms of your airline operations whereas 21.67% of the respondents consider cybersecurity as a risk in terms of your airline operations.

Question 7: What kind of support would you, as a registered aircraft operator, find it useful for your airline operations?

Option	Responses	Responses%	Total respondents
Integrated Aviation Cyber Security Strategy	11	18.33%	100
Integrated Cyber Security Risk Management System	40	66.67%	100
Appropriate Training	20	33.33%	100

Cyber Security Workshops	21	35.00%	100
Other (please specify)	0	0.00%	100



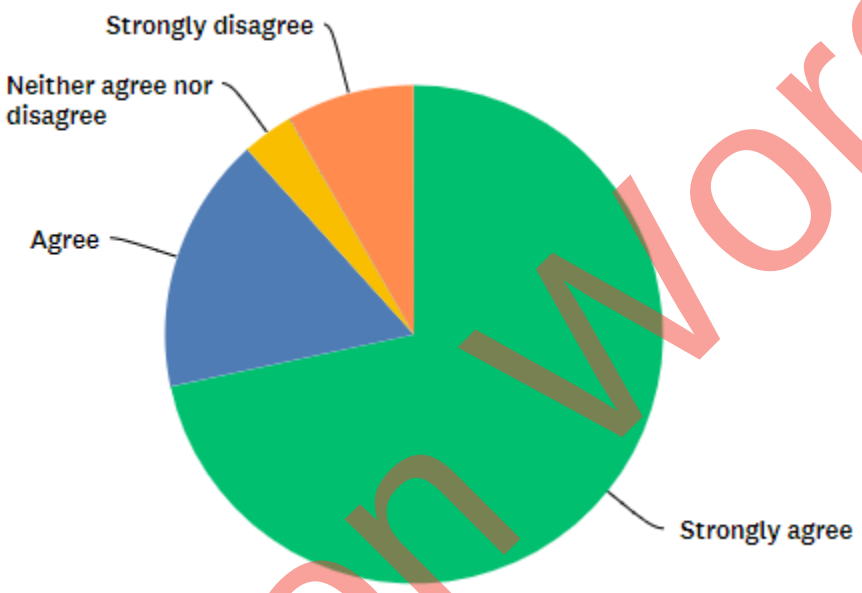
Question 7: What kind of support would you, as a registered aircraft operator, find it useful for your airline operations?

Findings: As per the above graph and table, 66.67% of the respondents believe that Integrated Cyber Security Risk Management System is the best security system for the airline operations whereas 35% of the respondents consider cyber Security workshops are the best security system for the airline operations.

Question 8: The use of approved, independent companies to objectively assess the cybersecurity of aviation products and services is useful to gain insight into risk

Option	Responses	Responses%	Total respondents
Strongly agree	43	71.67%	100

Agree	10	16.67%	100
Neither agree nor disagree	2	3.33%	100
Disagree	0	0	100
Strongly disagree	5	8.33%	100



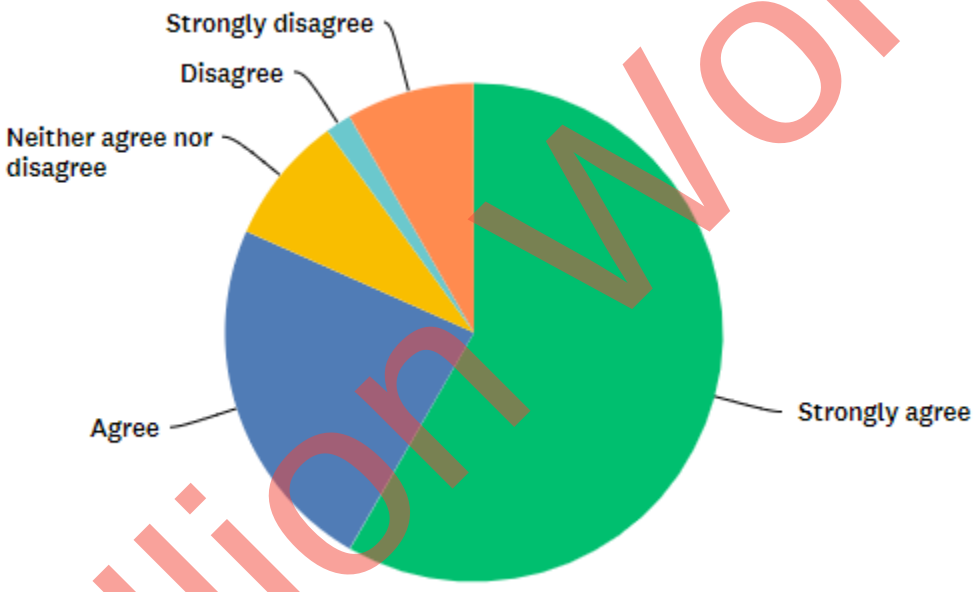
Question 8: The use of approved, independent companies to objectively assess the cybersecurity of aviation products and services is useful to gain insight into risk

Findings: As per the above graph and table, 71.67% of the respondents strongly agrees that the use of approved, independent companies to objectively assess the cybersecurity of aviation products and services is useful to gain insight into risk whereas 16.67% of the respondents agrees that the use of approved, independent companies to objectively assess the cybersecurity of aviation products and services is useful to gain insight into risk.

Question 9: It is not possible to 'hack' aviation systems

Option	Responses	Responses%	Total respondents

Strongly agree	35	58.33%	100
Agree	14	23.33%	100
Neither agree nor disagree	5	8.33%	100
Disagree	1	1.67%	100
Strongly disagree	5	8.33%	100



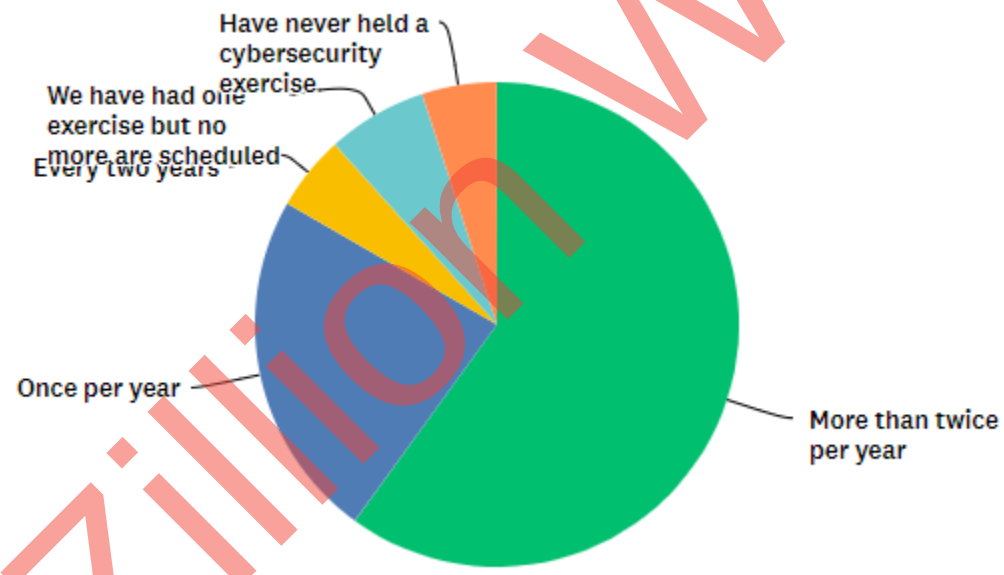
Question 9: It is not possible to 'hack' aviation systems

Findings: As per the above graph and table, 58.33% of the respondents strongly believes that hacking aviation security is possible whereas 23.33% of the respondents also agrees that hacking aviation security is possible.

Question 10: Your organization conducts exercises replicating aviation cybersecurity incidents

Option	Responses	Responses%	Total respondents

More than twice per year	36	60.00%	100
Once per year	14	23.33%	100
Every two years	3	5.00%	100
We have had one exercise but no more are scheduled	4	6.67%	100
Have never held a cybersecurity exercise	3	5.00%	100

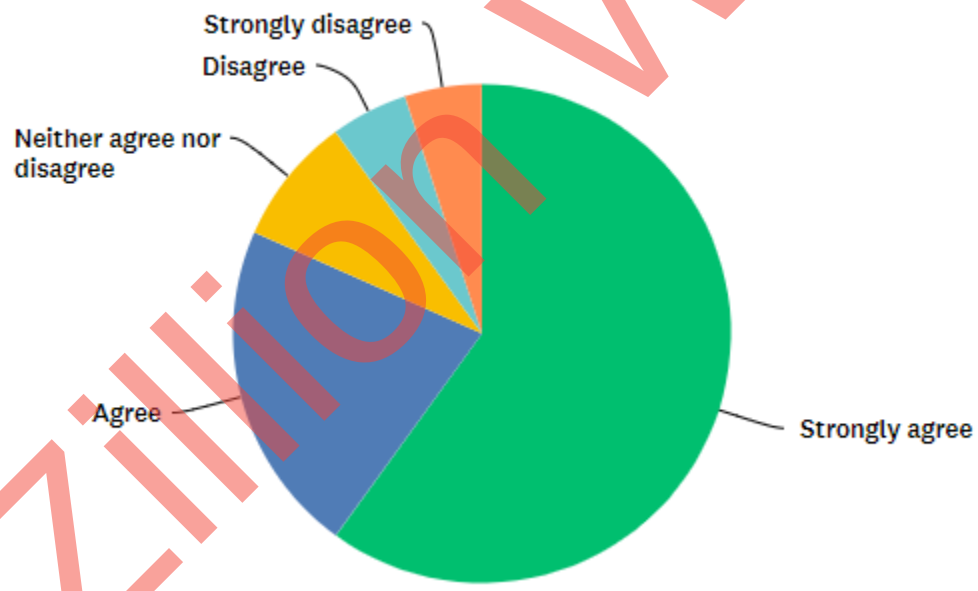


Question 10: Your organization conducts exercises replicating aviation cybersecurity incidents

Findings: As per the above graph and table, 60% of the respondents believe that their organisation conduct exercises replicating aviation cybersecurity incidents more than twice per year whereas 23.33% of the respondents told that their organisation conducts exercises replicating aviation cybersecurity incidents once per year.

Question 11: It is easy to incorporate cybersecurity best practice into purchasing aviation-related hardware/software/services

Option	Responses	Responses%	Total respondents
Strongly agree	36	60.00%	100
Agree	13	21.67%	100
Neither agree nor disagree	5	8.33%	100
Disagree	3	5.00%	100
Strongly disagree	3	5.00%	100

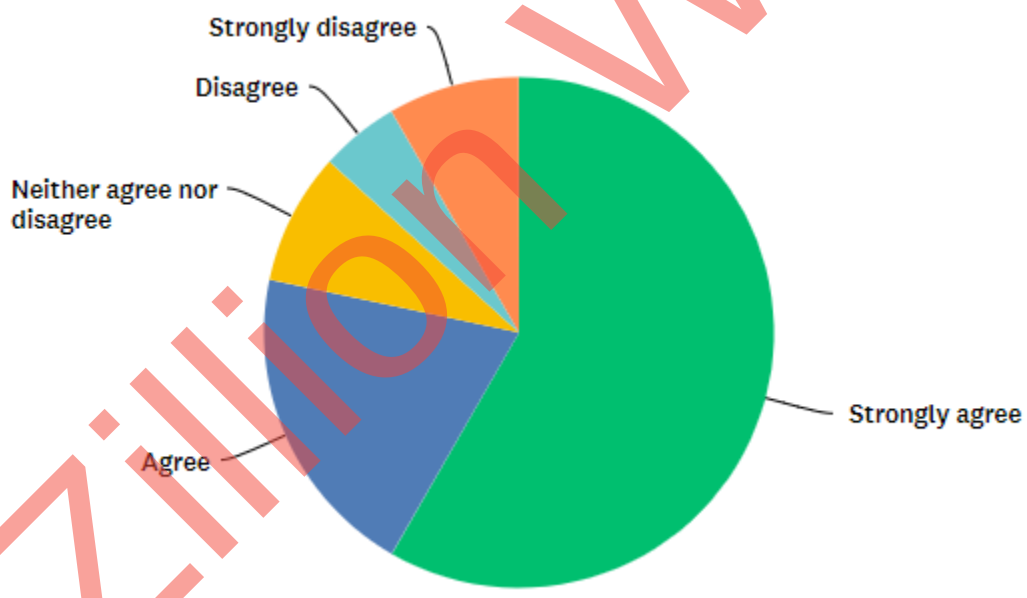


Question 11: It is easy to incorporate cybersecurity best practice into purchasing aviation-related hardware/software/services

Findings: As per the above graph and table, 60% of the respondents strongly believe that incorporating cybersecurity best practices into purchasing aviation-related hardware/software/services is good whereas 21.67% of the respondents agree that incorporating cybersecurity best practices into purchasing aviation-related hardware/software/services is better.

Question 12: Your operational staffs are trained to recognize a potential aviation cybersecurity incident

Option	Responses	Responses%	Total respondents
Strongly agree	35	58.33%	100
Agree	12	20.00%	100
Neither agree nor disagree	5	8.33%	100
Disagree	3	5.00%	100
Strongly disagree	5	8.33%	100

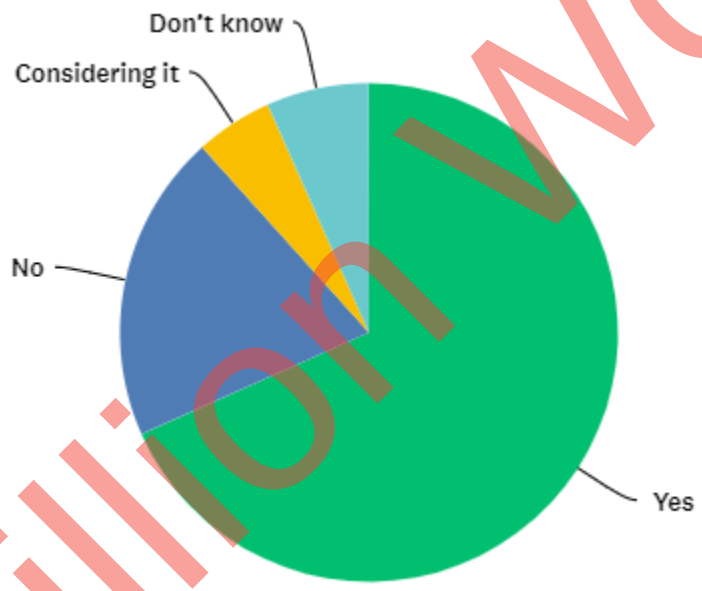


Question 12: Your operational staff are trained to recognize a potential aviation cybersecurity incident

Findings: As per the above graph and table, 58.33% of the respondents strongly agree that the operational staffs are trained enough to recognize a potential aviation cybersecurity incident whereas 20% of the respondents agrees that operational staffs are well trained to recognize a potential aviation cybersecurity incident.

Question 13: Your organization includes cyber insurance as an element of managing our aviation cybersecurity risk

Option	Responses	Responses%	Total respondents
Yes	41	68.33%	100
No	12	20.00%	100
Considering it	3	5.00%	100
Don't know	4	6.67%	100



Question 13: Your organization includes cyber insurance as an element of managing our aviation cybersecurity risk

Findings: As per the above graph and table, 68.33% of the respondents told that their organization includes cyber insurance as an element of managing the aviation cybersecurity risk whereas 20% of the respondents told that organization does not include cyber insurance as an element of managing the aviation cybersecurity risk.

Analysis

The above findings have been obtained from the responses collected through the online survey. It is quite evident from the generated report that aviation sectors have been taking great measures of security against the cybersecurity threats as it can disrupt the operations of the aviation sectors. It has been identified from the survey that 57.33% of the respondents have been associated with the aviation sectors as a cybersecurity consultant. 86.67% of the total respondents told that cybersecurity has held the highest risk for the aviation sectors. Social engineering is widely being used by the hackers which have given them many opportunities to hack the central server of the ATC communication system and it is considered as the core device of the entire communication in the aviation sectors. Therefore, it is quite evident that cybersecurity risk has got the highest priority for the aviation sectors.

In essence, 73.3% of the respondents believed that the cybersecurity risk in the aviation sector is too high. The cybersecurity threats not only harm the operations of the airlines' but it also imposes a great threat to the airports. The wireless network system is widely being used in the aviation sectors which makes it more vulnerable to the cybersecurity threats. A strong encryption method is used in the aviation sectors so as to strengthen the overall security of the central server but the COTS SDR has allowed the hackers to easily break the security code of the ATC and enter the server. It could be the biggest threat to the aviation industries. Several security guidelines have been proposed by the IATA still is not completely safe from the threats of cybersecurity. As per the survey report, it has been identified that the integrated cybersecurity risk management system could be the best option to prevent cyber hackers from entering the network. 60% of the respondents have told that aviation organisations often conduct cybersecurity risk management and it is done more than twice per year because it has been made compulsory by the IATA and ICAO. The cybersecurity practices have been made in such a way so that it becomes easy for the aviation sectors in terms of incorporating the practices in the day to day operation. 58.335 of the respondents have agreed that the operational staffs are trained enough to identify the cybersecurity risks and often they are provided with the training so as to make them effective in terms of increasing the cybersecurity awareness.

4.5. Qualitative data collection (Interview)

The interview has been carried out so as to secure the primary qualitative data collection method. Two security personnel of Dubai airport and Abu Dhabi airport of UAE has been interviewed. They have been asked 10 questions and the collected responses have been critically so as to meet the research objectives and to make the study more attractive and true to the source.

Interview transcript 1

S1= security personnel of Dubai airport, I= Interviewer

I: Hello sir, hope you have gone through the ethical policies, terms and conditions of this interview?

S1: Oh yes, I did. You may proceed now.

I: Okay then let us start the interview. Tell me one thing sir, how long you have been working in Dubai airport as a cybersecurity expert?

S1: I have been working with them for 11 years.

I: In your opinion, what are the potential threats for aviation industries against cybersecurity?

S1: Cybercrime and cyber terrorism obviously.

I: Do you think that ATC is more vulnerable to cyber threats?

S1: Yes it is indeed.

I: Do your organisations follow all the cybersecurity policies and measures?

S1: Definitely, being a reputed organisation we have to follow.

I: Have your organisation ever faced any issue with the cybersecurity threats?

S1: No, never

I: What efforts will you make if any breach attack takes place at your organisation?

S1: In order to be safe from such threats, Firewall and advanced encryption technique is widely being followed in our organisation.

I: What could be the best solution to strengthen the security parameters of ATC communication?

S1: See the thing is nothing can guarantee your safety against cybersecurity especially in the aviation industry. Still, we have been following some of the safety parameters of IATA so as to safeguard the ATC from cyber threats and strengthen the overall security of the air transmission.

I: How can technology help in lower the cybersecurity threats in aviation sectors?

S1: As per the guidelines of IATA, the most emerging technology which is STA cybersecurity is used in our organisation. Thus the advancement of technology may offer us some advanced tools in the future that can mitigate the cybersecurity threats.

I: In your opinion, what kind of potential threats does cybersecurity offer to airports?

S1: Commercial and political influence may cause cybercrime activities to the airports.

I: Are employees trained enough to detect any cybersecurity threat?

S1: Yes, they are.

I: Do your organisation follow cybersecurity risk Management?

S1: Obviously, we do.

Interview transcript 2

S2= security personnel of Abu Dhabi airport, I= Interviewer

I: Hello sir, hope you have gone through the ethical policies, terms and conditions of this interview?

S2: yes. You may proceed.

I: Okay then let us start the interview. Tell me one thing sir, how long you have been working in Abu Dhabi airport as a cybersecurity expert?

S2: I have been working with them for more than 12 years.

I: In your opinion, what are the potential threats for aviation industries against cybersecurity?

S2: Cyber-terrorism and Cybercrime.

I: Do you think that ATC is more vulnerable to cyber threats?

S2: Yes it is indeed.

I: Do your organisations follow all the cybersecurity policies and measures?

S2: Definitely, we have to follow all the cybersecurity rules made by IATA and ICAO.

I: Have your organisation ever faced any issue with the cybersecurity threats?

S2: No.

I: What efforts will you make if any breach attack takes place at your organisation?

S2: Cloudfare and VPN's.

I: What could be the best solution to strengthen the security parameters of ATC communication?

S2: We have always been trying to strengthen our overall cybersecurity network as this is currently the best option to safeguard the ATC.

I: How can technology help in lowering the cybersecurity threats in aviation sectors?

S2: Technology plays a crucial role in that. However, the SITA cybersecurity network which is widely being used in most of the aviation sectors is the invention of technology.

I: In your opinion, what kind of potential threats does cybersecurity offer to airports?

S2: Spying and cybercrime.

I: Are employees trained enough to detect any cybersecurity threat?

S2: Indeed they are.

I: Do your organisation follow cybersecurity risk Management?

S2: Yes we do.

4.6 Analysis of the interview

The interview has been conducted to secure secondary qualitative data analysis. 2 security experts of Dubai airport and Abu Dhabi airport have been interviewed to collect some important

information about the cybersecurity threat in the aviation sectors. The interview transcript has been used to ask the questions

The first question was about the potential threats for aviation industries against cybersecurity. 2 of the security experts consider that cybercrime and cyber terrorism are the primary threats for the aviation sectors. Onboard radios and the ACARS are widely being used in the aviation sectors in order to communicate with the ground staff. Although a strong encryption method is used to shield these devices against cybersecurity threats, still these are not safe from hackers. The security system of the ACARS can be bypassed using the strong network system. Along with that, wireless communication has widely been adopted by the air transmission sectors. Social engineering is a common field of cyber attacks and most of the hackers have a deep knowledge of COTS SDR which makes the strong cybersecurity architecture of ACARS vulnerable to cybersecurity threats.

The second question was asked about the potentiality of ATC communication against cyber threats. Both have agreed that ATC communication is more vulnerable to cybersecurity threats. Air traffic control is considered as the central system of air transmission and a single issue in the ATC can offer a major disruption in the effectiveness of air transportation. The technology is being evolved now and then but the research and development process takes quite a long time to implement. Developing new technologies and implement them in the aircraft require a couple of years. Therefore improving the security measures in the aircraft has become too complex. For that reason, ATC is also not safe from cybersecurity threats.

The third question was asked about the cybersecurity measures of the aviation sectors and to what extent it is being followed in the civil aviation sectors. Both security experts have replied that the cybersecurity measures formulated by IATA and ICAO are thoroughly being followed in the aviation organization and most importantly each aviation sector needs to follow the guidelines of IATA in terms of cybersecurity measures.

The fourth question was whether their organisation has ever faced any cybersecurity challenges or not. Both disagreed and they replied that they have not received any sort of cybersecurity challenges to date. However, aviation sectors are too much concerned about the cybersecurity issues and they have been taking several security measures so as to mitigate the threats of cybersecurity as much as possible.

The fifth question was about the security measure that they will take if they encounter any sort of breach attack. They have told that the strong firewall and advanced encryption standard (AES) is used in the aviation sectors which helps stop the unwanted rack and DDoS break attack. HTTP proxy server of Cloudflare is used in the aviation sectors in order to detect any suspicious activity and when any sort of breach attack is found then the network of the attacking server is bypassed using the proxy server which again stops the hackers to reach the central server of the aviation sectors.

The sixth question was about strengthening the security parameters of ATC communication. As per the reply of the 2 security engineers of Dubai airport and Abu Dhabi airport, it has been identified that no specific security has been invented to date which can offer maximum security to the ATC communication channel. If the overall security of the aviation sectors is strong enough to protect the cybersecurity threats then the ATC communication channel will automatically be safe from the cybersecurity threats. Strong data encryption technique is the best possible way to strengthen the security parameters of ATC communication.

The seventh question was about the role of technology in mitigating cybersecurity threats. According to the responses of the 2 security experts, the technology has been playing the most significant role in solving the cybersecurity risks in the aviation sectors. According to the guideline of IATA, the strong cybersecurity architecture offered by SITA and airbus is a must for all the aviation sectors. The sophisticated architecture of SITA cybersecurity can offer optimum security as it is capable enough to detect any suspicious activities with the central server of aviation. Not only has the detection had it also offered remedies according to the nature of the cyber threats.

The eighth question was regarding the cybersecurity threats for the airports. As per the reply of the security experts, it has been identified that there are five factors that can hinder the operational efficacy of the airports such as commercial, political, spying, and cybercrime.

The ninth question was asked about the employee training on cybersecurity. As per the responses of the security experts, all of the employees are trained enough to detect any intention of the breach. They are being provided quality training on cybersecurity as they are also an integral part of the aviation community. The ground staffs are highly trained and they have the depth knowledge of cybersecurity so that they can cope up with the cybersecurity threats without panicking if they find

any. Cybersecurity training is provided to the employees on cybersecurity awareness based on the company policy.

The last question was about cybersecurity risk management. As per the reply of the security consultants it has been identified that the cybersecurity risk management is a must for the aviation sectors. There is too much cybersecurity risk associated with the aviation sectors therefore the urgency of conducting security risk management has become compulsory for the aviation sectors as per the guidelines of IATA. The threat detection, endpoint monitoring, real-time analytics have become the core part of the cybersecurity risk management for the aviation sectors. Cybersecurity risk prevention and assessment programs are often being conducted in the aviation industries so as to be safe from the upcoming cybersecurity threats.

However, due to the ongoing pandemic, the interview has been conducted with the Microsoft teams instead of one to one interview.

Chapter 5: Conclusion and recommendations

5.1 Conclusion

It can be concluded that the cybersecurity has become the major issue for the aviation industries as most of the computerized devices are used in this industry. The rapid growth of technology has a significant impact on the networks and systems of aviation sectors. Nowadays the cybersecurity risks and threats have progressed much and therefore effective and continuous monitoring process is much required to prevent the cyber attackers. Moreover, automated systems are used much in the aviation sectors. The aircraft operations, network, Wi-Fi connectivity and baggage system checking are made automated and therefore these all things are much vulnerable to the cybersecurity threats. Besides, most of the systems are interconnected with the other devices and the devices communicate with each other so as to provide the service. This is how automated devices work. If hackers can grasp one of the networks then they can have remotely access the entire networks of the aviation sectors. For this reason, strengthening cybersecurity architecture has become the topmost priority for the authorities of the aviation sectors. Besides that, the remotely controlled services, devices and the internet connection is widely being used in the aviation sectors which makes it more vulnerable to the cybersecurity threats. There is also high risk with data confidentiality and if it gets exposed in any condition then it could be the disaster for the aviation industries as much private information of the passengers and operations are included in the database. All the airports and the aviation industries are connected sides by sides, therefore, it is too important for the stakeholders to take the cybersecurity issues seriously and focus on establishing a strong cybersecurity network that ensures the maximum security against the cyber threats.

The aviation associations and the organisation such as ICAO, IATA, CANSO (Civil air navigation services organisations) and many others have developed some security measures and policies in order to prevent the cybersecurity risks. Aviation sectors must comply with the security measures and focus on implementing the policies as much as possible so as to mitigate the cybersecurity threats. It will not only help the, to protect the potential infrastructure but the strong network also ensures the security of the aircraft operation, employees and passengers. The DDoS and the ransomware attack has been identified as the common form of cyber threats which is being used by most of the cyber attackers to disable the security network of the aviation sectors and steak the

information, Attacks can be performed on the mobile and tablets which are being carried by almost all the passengers and employees and they can also fuel the process of data exploitation and make the work easier for the cyber attackers. Therefore a strong collaborative work amongst the stakeholders is much needed to prevent the cyber attackers from breaching the private information of the aviation sectors.

5.2 Linking with objectives

Objective 1: To identify the potential threats for the airports against cybersecurity

Airports have been located prone to cyber threats which have been mentioned on this observe. Internal security test is essential for strengthening the security measures of the computerized structures. Security specialists have the major responsibility in strengthening the security of a factor moreover they will check the security of reach factor independently in a far greater superior way. An information protection system is broadly being used in all of the airports and if any type of security breach takes vicinity then it'll have a positive effect at the passengers. A sophisticated cyber-attack consequences in monetary loss. *Four kinds of cyber threats have been identified from the survey that can create predicament via affecting the operational efficacy of the airports along with*

1. political

2. business spying

3. disruption

4. cybercrime.

Along with that 5. cyber crimes and 6. cyber terrorism are the potential threats for the aviation sectors. These things have been covered in this study and hence the objective 1 is justified.

Objective 2: To identify the challenges of ATC communication

Five reasons for ATC communication issues have been presented in this study such as long development cycle, legacy and compatibility requirements, costs, frequency overuse and the preferences for an open system. Development of new technologies and the certification process in the aviation sectors take too much time to be implemented. This is one of the primary reason for ATC communication issue. Besides that, civil aviation is the main organisation that create security

protocols and for the other aviation industries, the language barrier has become one of the primary issues. Apart from that due to the complexity of the security protocols, aviation industries of different countries fail to understand the processes and the security protocols. Moreover, due to the high costs of the machinery, aviation sectors avoid changing the parts of the aircraft till it becomes of no use. *Frequency overuse is one of the main reasons for ATC communication challenges as the frequency for all the aircraft are maintained by the ATC and the some of the frequency levels is stored for the future purpose which causes frequency mismatch*. All the above-mentioned things have been discussed in detail in this study and hence the objective 2 is satisfied.

Objective 3: To identify the cyber threats for air transportation

Much private information of passengers is stored in the database of the aviation industries. A potential data breach can exploit all the private information which can be the biggest threat for the aviation sectors. Therefore, the stakeholders of the air transport industries must address the issues earlier so as to minimize the level of threats which has been demonstrated in this study. Hence the objective 3 is also satisfied.

Objective 4: To provide the solution in order to mitigate the potential cybersecurity threats

The security measure and policies introduced by the global aviation organisations must be maintained and followed by the airport authorities of different countries so as to shield the air transportation from cyber threats. All the security measures have also been discussed in this study. Hence the objective 4 is satisfied.

5.3 Recommendations

Due to the increased automation in the aviation industries, cybersecurity threats have increased. Therefore, following and implementing the security and security policies are the best way to be safe from the cyber threats by the airports. Keeping the security policies and measures in mind, some of the beneficial recommendations have been provided below which will help the aviation sectors to deal with the cyber hackers proactively and mitigate the issues. *Cloud computing, virtualization, virtual networks and data recovery system can help a lot in mitigating the cybersecurity threats in the aviation sectors.* All the things have been elaborated deeply below.

Cloud computing

Cloud computing is the best tool for the aviation industries which will enable the authorities to store the confidential information in remotely accessed storage. It also offers the maximum security and the security layers of cloud can not be penetrated by the cyber hackers, Cloud storage also offers a backup unit where the information of passengers and the aircraft can be stored without any worry. Moreover, the hybrid could model can be implemented in the aviation sectors in which the internal operations of the airports will be managed using the private cloud infrastructure and the external operations such as customer management and employee management will be done using the infrastructure of the public cloud. It offers the maximum data security and security and the individual aviation industry can manage the entire cloud infrastructure on their own. In addition, the infrastructure of the cloud service is maintained by the third parties who provide the assurance of data confidentiality and they are also industrial level expert.

Virtualization

Virtualization is a cloud-based service that will allow the higher authorities to use each computer with multiple functions. Each of them will be provided with the different interfaces and the portable devices will be connected to each. When a unit will be attacked by the cyber hackers then they cannot reach the other devices as one main unit is segmented into many. Therefore other units including the central server remain unharmed.

Virtual networks

Virtual networks provide dynamic IP addresses with different domain names to the customers. Each time customers get connected with the central server, the IP addresses keep changing. Therefore, cyber attackers cannot locate the IP addresses of the customers along with the domain name. Therefore virtual networks will facilitate the process of intrusion free operations for the customers.

Data recovery system

A data recovery plan is also as important as other factors. A set of data may get disappeared but the organisations must have the plan that can restore the lost information. The databases of the aviation sectors are filled with the customers' information, aircraft operations, and flight time and so on. If these crucial information gets lost then it will cause cancellation and delays of flights. The entire thing will lead to passenger dissatisfaction. In order to avoid that, a strong backup and

restore plan must be introduced in the aviation sectors. Some of the measures can be taken to mitigate the negative impacts. The information must be stored in a remote location with preferred domain names and proper maintenance is required to that backup system. For the physical devices, the proper power sources and batteries must be used. Power generators must be installed in the remote areas for the security of the backup storage.

5.4 Future work

This research paper can be of great help for future researchers who are interested in researching on the near about the same topic. This paper has covered almost all the areas of cybersecurity in the aviation sectors which will help the future peers to understand the fundamentals of the cybersecurity issues in the aviation industries. This study has set a benchmark for future researchers. This study also helps in understanding the importance of establishing a strong cybersecurity network. It is mainly beneficial for the aviation industries who can find different cybersecurity threats to air transportation along with the mitigation techniques. Moreover, some of the recommendations have been included in this study as well which will help the aviation industries to mitigate the cyber threats easily and operate the business with success.

References

Aboti, C.D., 2019. Survey on IoT: Challenges and cyber risks in commercial aviation.

Alqushayri, D.F., 2020. Cybersecurity Vulnerability Analysis and Countermeasures of Commercial Aircraft Avionic Systems.

Anaedevha, R.N. and Ajibola, A., 2020. CYBER SECURITY FRAMEWORK FOR NIGERIAN CIVIL AVIATION AUTHORITY, HEADQUARTERS.

Andreades, C., Kendrick, J., Poresky, C. and Peterson, P., 2017. *Cyber Security in Civilian Aviation: Insights for Advanced Nuclear Technologies*. UCBTH-17-001, Berkeley, CA.

Baghdasarin, D., 2019. MRO Cybersecurity SWOT. *International Journal of Aviation, Aeronautics, and Aerospace*, *6*(1), p.9.

Bair, J., Bellovin, S.M., Manley, A., Reid, B. and Shostack, A., 2017. That was close: Reward reporting of cybersecurity near misses. *Colo. Tech. LJ*, *16*, p.327.

Best, K.L., Schmid, J., Tierney, S., Awan, J., Beyene, N.M., Holliday, M.A., Khan, R. and Lee, K., 2020. *How to Analyze the Cyber Threat from Drones*. RAND ARROYO CENTER SANTA MONICA CA SANTA MONICA United States.

Bhatia, J., Breaux, T.D., Friedberg, L., Hibshi, H. and Smullen, D., 2016. Privacy risk in cybersecurity data sharing. In *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security* (pp. 57-64).

Camilleri, S., 2014. The Current State of Cyber Security Readiness in the Aviation Industry. *Floriana: Durasee Services*, p.9.

Chirichiello, A., Porretti, C. and Berardi, A., 2017. Cyber Threat Intelligence for Supporting the ATM Security Management. In *ITASEC* (pp. 253-257).

Choy, L.T., 2014. The strengths and weaknesses of research methodology: Comparison and complimentary between qualitative and quantitative approaches. *IOSR Journal of Humanities and Social Science*, *19*(4), pp.99-104.

Cyr, J., 2016. The pitfalls and promise of focus groups as a data collection method. *Sociological methods & research*, *45*(2), pp.231-259.

Dancy, J.R. and Dancy, V.A., 2016. Terrorism and oil & gas pipeline infrastructure: vulnerability and potential liability for cybersecurity attacks. *ONE J*, *2*, p.579.

De Gramatica, M., Massacci, F., Shim, W., Tedeschi, A. and Williams, J., 2015. IT interdependence and the economic fairness of cybersecurity regulations for civil aviation. *IEEE Security & Privacy*, *13*(5), pp.52-61.

De Zan, T., d'Amore, F. and Di Camillo, F., 2016. The defence of civilian air traffic systems from cyber threats. *Istituto Affari Internazionali*.

Duchamp, H., Bayram, I. and Korhani, R., 2016. Cyber-Security, a new challenge for the aviation and automotive industries. In *Seminar in Information Systems: Applied Cybersecurity Strategy for Managers* (pp. 1-4).

Emanuilov, I., 2019. International (Cyber) security of the Global Aviation Critical Infrastructure as a Community Interest.

Haass, J., Sampigethaya, R. and Capezzuto, V., 2016. Aviation and cybersecurity: opportunities for applied research. *TR News*, (304), p.39.

Hasratyan, N., Olesen, N., Becue, A., Seldeslachts, U., Bâ, S., Chiappetta, A., Costin, A., Dobelmann, J., Henny, C., Khodashenas, P.S. and Rizzo, G., 2020. ECSO Transportation Sector Report, Cyber security for road, rail, air, and sea. WG3 I Sectoral Demand.

Hasratyan, N., Olesen, N., Becue, A., Seldeslachts, U., Bâ, S., Chiappetta, A., Costin, A., Dobelmann, J., Henny, C., Khodashenas, P.S. and Rizzo, G., 2020. ECSO Transportation Sector Report, Cyber security for road, rail, air, and sea. WG3 I Sectoral Demand.

Ian, M., Elena, V. and Michael, J., 2019. Artificial Intelligence in the Aviation Manufacturing Process for Complex Assemblies and Components. In *IOP Conference Series: Materials Science and Engineering* (Vol. 689, No. 1, p. 012022). IOP Publishing.

Icao, 2020. Available at: https://www.icao.int/NACC/Documents/Meetings/2018/CSEC/D12b-AirTransportCybersecurityInsights2018-SITA.pdf. Accessed on 5th November 2020.

Izuakor, C., 2016. Understanding the Impact of Cyber Security Risks on Security. In *ICISSP* (pp. 509-513).

Johnson, C., 2016. Securing the participation of security-critical SCADA systems in the industrial internet of things.

Johnston, A., 2014. Rigour in research: theory in the research approach. *European Business Review*.

Kagalwalla, N. and Churi, P.P., 2019. Cybersecurity in Aviation: An Intrinsic Review. In *2019 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA)* (pp. 1-6). IEEE.

Kessler, G.C., Craiger, J.P. and Haass, J.C., 2018. A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System. *TransNav: International Journal on Marine Navigation and Security of Sea Transportation*, *12*(3), p.429.

Lamb, K., 2018. Challenges of Digitalisation in the Aerospace and Aviation Sectors.

Lamba, T. and Kandwal, S., 2019. Study on Cyber Security and Malware Protection. *BLOOMSBURY INDIA*, p.127.

Lewallen, J., 2020. Cybersecurity Information Sharing and Congress's Oversight Role. *Wayne L. Rev.*, *66*, p.151.

Lonzetta, A.M., Cope, P., Campbell, J., Mohd, B.J. and Hayajneh, T., 2018. Security vulnerabilities in Bluetooth technology as used in IoT. *Journal of Sensor and Actuator Networks*, *7*(3), p.28.

Lykou, G., Anagnostopoulou, A. and Gritzalis, D., 2018. Implementing cyber-security measures in airports to improve cyber-resilience. In *2018 Global Internet of Things Summit (GIoTS)* (pp. 1-6). IEEE.

Lykou, G., Anagnostopoulou, A. and Gritzalis, D., 2019. Smart airport cybersecurity: Threat mitigation and cyber resilience controls. *Sensors*, *19*(1), p.19.

Lykou, G., Iakovakis, G. and Gritzalis, D., 2019. Aviation Cybersecurity and Cyber-Resilience: Assessing Risk in Air Traffic Management. In *Critical Infrastructure Security and Resilience* (pp. 245-260). Springer, Cham.

Lykou, G., Moustakas, D. and Gritzalis, D., 2020. Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies. *Sensors*, *20*(12), p.3537.

Mathew, A.R., 2019. Airport Cyber Security and Cyber Resilience Controls. *arXiv preprint arXiv:1908.09894*.

Mohajan, H.K., 2017. Two criteria for good measurements in research: Validity and reliability. *Annals of Spiru Haret University. Economic Series*, *17*(4), pp.59-82.

Nassaji, H., 2015. Qualitative and descriptive research: Data type versus data analysis.

Nikolova, I., 2017. Best Practice for Cybersecurity Capacity Building in Bulgaria's Public Sector. *Information & Security*, *38*, pp.79-92.

Pollard, T. and Clark, J., 2019. Connected aircraft: Cyber-security risks, insider threat, and management approaches. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*.

Rodrigues, B., Franco, M., Parangi, G. and Stiller, B., 2019. SEConomy: A Framework for the Economic Assessment of Cybersecurity. In *International Conference on the Economics of Grids, Clouds, Systems, and Services* (pp. 154-166). Springer, Cham.

Ryan, G., 2018. Introduction to positivism, interpretivism and critical theory. *Nurse researcher*, *25*(4), pp.41-49.

Sans, 2020. Available at: sans.org/reading-room/whitepapers/breaches/paper/36452#:~:text=In%20May%20or%20early%20June,(Security%20Experts%2C%202015). Accessed on [5th November 2020].

Shackelford, S.J. and Russell, S., 2014. Above the Cloud: Enhancing Cybersecurity in the Aerospace Sector. *FIU L. Rev.*, *10*, p.635.

Shukla, M., Johnson, S.D. and Jones, P., 2019. Does the NIS implementation strategy effectively address cyber security risks in the UK?. In *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (pp. 1-11). IEEE.

Simmons, H.O., 2017. Cybersecurity in Aviation: Constant Vigilance Required. *J. Air L. & Com.*, *82*, p.771.

SITA, 2020. Available at: http://www.centrodeestudiosaeronauticos.edu.co/cea/RelacionesInter/seminario-internacional-de-gestion-de-aeropuertos-en-contexto-global-de-crecimiento/Documents/4%20Juan%20Villanil%20CustomerPresentation_CyberSecurity.pdf . Accessed on 5th November 2020.

Skorupski, J. and Uchroński, P., 2017. A fuzzy model for evaluating metal detection equipment at airport security screening checkpoints. *International Journal of Critical Infrastructure Protection*, *16*, pp.39-48.

Strohmeier, M., Niedbala, A.K., Schäfer, M., Lenders, V. and Martinovic, I., 2018. Surveying aviation professionals on the security of the air traffic control system. In *Security and Security Interplay of Intelligent Software Systems* (pp. 135-152). Springer, Cham.

Suchodolski, J.C., 2018. Cybersecurity of Autonomous Systems in the Transportation Sector: An Examination of Regulatory and Private Law Approaches with Recommendations for Needed Reforms. *NCJL & Tech.*, *20*, p.121.

Suciu, G., Scheianu, A., Vulpe, A., Petre, I. and Suciu, V., 2018. Cyber-attacks–The impact over airports security and prevention modalities. In *World Conference on Information Systems and Technologies* (pp. 154-162). Springer, Cham.

Taherdoost, H., 2016. Sampling methods in research methodology; how to choose a sampling technique for research. *How to Choose a Sampling Technique for Research.*

Tam, K. and Jones, K.D., 2018. Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping. *Journal of Cyber Policy*, *3*(2), pp.147-164.

Tan, E.E.G., 2015. Cybersecurity in Civil Aviation: Need for Industry-wide Approach.

Tedeschi, P. and Sciancalepore, S., 2019. Edge and Fog Computing in Critical Infrastructures: Analysis, Security Threats, and Research Challenges. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 1-10). IEEE.

Tounsi, W. and Rais, H., 2018. A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & security*, *72*, pp.212-233.

Trimble, D., Monken, J. and Sand, A.F., 2017. A framework for cybersecurity assessments of critical port infrastructure. In *2017 International Conference on Cyber Conflict (CyCon US)* (pp. 1-7). IEEE.

Tumele, S., 2015. Case study research. *International Journal of Sales, Retailing & Marketing*, *4*(9), pp.68-78.

Urban, J.A., 2017. Not Your Granddaddy's Aviation Industry: The Need to Implement Cybersecurity Standards and Best Practices within the International Aviation Industry. *Alb. LJ Sci. & Tech.*, *27*, p.62.

Watkins, B., 2014. The impact of cyber attacks on the private sector. *Briefing Paper, Association for International Affair*, *12*.

Woiceshyn, J. and Daellenbach, U., 2018. Evaluating inductive vs deductive research in management studies. *Qualitative Research in Organizations and Management: An International Journal*.

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

Κοσσένα, Μ., 2019. Cyber security in air transportation.