2021

Cyber Security Maturity Model Capability at The Airports

Ojaswini Malhotra
Griffith University, ojaswini.malhotra@griffithuni.edu.au

Sharmistha Dey
Griffith University, s.dey@griffith.edu.au

Ernest Foo
Griffith University, e.foo@griffith.edu.au

Mardé Helbig
Griffith University, m.helbig@griffith.edu.au

Cyber Security Maturity Model Capability at The Airports

Full research paper

Ojaswini Malhotra
School of Information and Communication Technology
Griffith University
Brisbane, Australia
Email: ojaswini.malhotra@griffithuni.edu.au

Sharmistha Dey
School of Information and Communication Technology
Griffith University
Brisbane, Australia
Email: s.dey@griffith.edu.au

Ernest Foo
School of Information and Communication Technology
Griffith University
Brisbane, Australia
Email: e.foo@griffith.edu.au

Mardé Helbig
School of Information and Communication Technology
Griffith University
Brisbane, Australia
Email: m.helbig@griffith.edu.au
nard.edu.au

Abstract

Cybersecurity is an important facilitator for essential aviation safety. The adoption rate for levels of cyber-security protocols at commercial airports is the focus of this research. Scope of this research is limited to cybersecurity maturity model capability norms covering fourteen domains. The paper presents primary data collected from several airport authorities. This survey-based study will be useful in identifying areas for improving operational procedures and developing strong cybersecurity governance at airports. This will allow airports to understand risks and respond proactively by adopting cybersecurity best practices and resilience measures. This study includes domestic, international, privately owned airports, airstrips, or aerodromes. This research found that level one of cyber-security maturity model is the most followed while proactive and advance levels i.e., level 4 and 5 are least adhered to. Most airports appear to have some resources allocated to cyber protection and resilience.
Keywords cyber-security, CMMC, airports, compliance, survey

1 Introduction

Cyber risks have been rising at an alarming rate in the past few years and with this comes two major aspects that should be addressed, namely cyber security and the management of data breaches(Bissell 2013; Feng et al. 2019; Hawamleh et al. 2020; Thakur et al. 2019). If we consider the USA alone then there have been 1,579 major data breaches resulting in over one thousand eight hundred million records that were exposed(Monteagudo 2021a). Moreover, when compared to 2016, cyber-crime had increased drastically by 44.7%(Monteagudo 2021b). Cyber fraud is the second most reported crime across the world and in the UK, it accounts for 50% of all crimes(Katz 2018).Perhaps the most comparable of industries that could be analysed for the determination of information security is the aviation industry. According to various research, the financial sector is considered the most when it comes to cyber risks or fraud(Lagazio et al. 2014; Leukfeldt et al. 2017). But the aviation industry is at a high risk and is being targeted by hackers, as it is perceived as an easy target(Meyer 2018). The aviation industry is the custodian of a vast amount of personal and sensitive data. According to relevant statistics with around 4,358 million passengers, the data gathered by the airlines is staggering, emphasizing that this industry is one of the prime targets of hackers(Meyer 2018).

Cybersecurity is a significant enabler for aviation safety(Lykou et al. 2018). Airports attempt to deliver optimal services in a dependable and long-term way by focusing on development, efficiency, safety, and security. The focus of this paper will be on the rate at which cybersecurity procedures are implemented at commercial airports. In addition, this study investigates whether airports are compliant with the Cybersecurity Capability Maturity Model Certification (CMMC)(Brill 2020; Peters 2020; Russell 2020).

A cyber-attack at an airport may result in loss of human life and data. Hence cyber security is directly related to the security and safety practices that must be followed and implemented at airports. Often the airport industry is neglected when compared to other industries, such as banking etc. Due to this very reason, it is often observed that the airport industry's cyber security cell in the IT department, is not up to date. Most airports do not have their own cyber security department and they outsource these services. It is necessary for the airports to have their own cyber department as airports contain the information of every traveller. Also, with the airport's check-in being more technologically advanced it makes it very easy for intruders to find a vulnerability within the system and steal sensitive data that might lead to a privacy breach. This could then lead to identity theft.

The lack of awareness amongst the airport officials also contributes to cyber-fraud, hence making it essential for the airport employees to be trained and educated about cyber-security, based on their specific role/duties and qualification. If sensitive or confidential information is leaked it not only leads to cyber-attacks which, can harm the organisation but also be the reason for cyber-terrorism(Janczewski and Colarik 2007; Lewis 2002). All these vital aspects play a pivotal role in the secure functioning of the airports. This then raises the question of how compliant the airports are with reference to CMMC levels and their practices.

This paper has been organised into the following sections. Section 2 presents a literature review of prior studies in this topic. Section 3 explains CMMC levels, domains, and associated practices. Section 4 discusses and explains the methodology adopted which is followed by section 5 and 6 that discuss and analyse the result of the survey. Section 7 presents the recommendations. This is followed by Section 8 which presents the conclusion and future work.

2 Related Work

The transport industry, be it aviation, marine, or automotive, is prone to cyber security risks including cyber-attacks with several important factors like malware, denial-of-service assaults, and other types of manipulation of information(Azmi et al. 2020; Lehto 2013; Mezher et al. 2016). The importance of cyber security is underlined since the failure of even one important component can pose substantial obstacles to the entire system platform's operation. Artificial Intelligence provides new risks and attack vectors, but at the same time, it opens new possibilities for solving cyber security issues. Modern technology like the use of machine learning along with improved governance procedure at the airports with emphasis on the need for the Cyber Maturity Model, can be useful for strengthening the cyber security at the airports(Taleqani et al. 2018; Thomas et al. 2020). Keeping in mind the disparity between vulnerability of air travel and the aviation industry's initiatives towards prevention and protection, there is no doubt that cyberspace-related assaults have become one of the most significant dangers to aviation safety and security. While these attacks may be considered modest at present but, they are on the rise, and their ramifications will undoubtedly rise as well. However, tackling and resolving the problem is not simple(Fox 2016). All next generation functionalities will be subject to numerous threats if they are not

protected, and they will be unable to function properly without one of the key components of next generation, namely aviation security(Li and Kamal 2011; Manesh and Kaabouch 2017).

The Federal Aviation Administration (FAA) of the Unites States of America is responsible for managing the national airspace organization, which includes air traffic control(ATC) systems, events, amenities, and aircraft, as well as the personnel who run them(Dillingham et al. 2015). The FAA is adopting next generation Air Transportation System to replace the present radar-based air traffic control system with one that relies on satellite routing and robotics entailing cybersecurity concerns. Cybersecurity is quickly becoming a crucial enabler for aviation safety through the implementation of cybersecurity measures and best practices in airports to increase their cyber resilience (Lykou et al. 2018). In today's world, commercial airports must build their own cyber security posture. They are responsible for evaluating current norms and regulations and adapting them to the technology advancements of the airport. Airports develop, deploy, and secure network infrastructure, as well as cybersecurity solutions, in a variety of ways. To safeguard the safety of operations, passengers, and public, airport operators should put cyber security first. Due to technology advancements, cyber dangers and hazards will continue to expand, and the link between safety and security will become increasingly intertwined(Lykou et al. 2018).

Sudden increase of Cybercrime and Cyber terrorism is dangerous, with the latter being defined as a separate and unique threat that has become more dangerous with globalization and widespread use of the Internet that must be separately addressed(Abeyratne 2011). The most effective tactics used by cyber terrorists in the aviation sector is running Denial of Service (DoS), Distributed DoS, and hijacking attacks on airport information network services(Ugwoke et al. 2015). Prospective offenders of aviation terrorism must be thwarted from infringing security barriers and obtaining admittance to “secure” airport facilities and aircraft if planes and passengers, as well as property and persons on ground, are to be protected in the light of the fateful incident 9/11(Baker 2020). Cyber-terrorism links with tourism hence adopting best-practice cybersecurity incident response standards is a feasible strategy for dealing with cyber outbreaks in the aviation industry(Lekota and Coetzee 2019). There is need and necessity of the cyber-security practices to be in place, at every airport to mitigate the fear and losses caused to the tourists and tourism industry due to any cyber-threat or attack.

Cyber security challenges with respect to air traffic control based on automated dependent surveillance broadcast are also a cause of concern. Cyber threats and attacks are leading in compromise of future aircraft surveillance due to the advancements in aviation technologies(Jiang et al. 2018; Sampigethaya and Poovendran 2013). The aviation industry needs to tackle cybercrime by building a timely detection and response to looming threats(Schmidt 2016). The public has tremendous faith in the aviation business, and the sector has a chance to prepare for a danger that has not yet adversely disrupted its operations, which is why it is necessary to establish a thorough framework to respond to a cyber-attack event. Emphasis should be placed on conducting in-depth analysis by the authorized airport personnel, to mitigate and reduce spiteful attacks(Gopalakrishnan et al. 2013; Rajapaksha and Jayasuriya 2020; Suciu et al. 2019). As a result, the worldwide aviation community's future safety depends on how it implements preventative measures and, more significantly, how it recovers from destructive cyber-attacks. The cyber-security, is indispensable for airports so that all technologies can function and deliver an effective output. (Jiang et al. 2018; Sampigethaya and Poovendran 2013).

In the physical world, aircraft and air transport overcome several significant difficulties and hostilities. The advancements of the "cyber" layer, i.e., digital computers, data storage and networking, personnel, and processes, within the airframe, have been critical to the success of this difficult task. "Cyber" layer benefits the aviation industry and plays a crucial role in assisting future aircraft, airports, and air traffic control systems in overcoming 21st-century issues. The cyber layer has potential to significantly improve the quality and performance of each individual aircraft's gate-to-gate flight as well as the travel experience of each traveller and crew with a new paradigm for aviation security. There is a need to investigate the effects of the cyber layer and cyber–physical integration on aircraft and air transportation safety, functioning, and serviceability that indirectly links to the need of implementing the CMMC at airports, for a safe and secure air transportation system(Anaedevha and Ajibola 2020). There is necessity of using data from current literature and surveys to examine the NCAA's existing cyber/information security initiatives (if any) and to build an adaptive cybersecurity framework that is robust enough to ensure its safety(Anaedevha and Ajibola 2020).

3 CMMC- Cyber Security Maturity Model Certification

The CMMC is a standard for integrating cybersecurity throughout the defence industrial base (DIB), which comprises over 300,000 enterprises. The CMMC is the Department of Defence reaction to large breaches of sensitive information on contractor information systems(Stokes and Childress 2020).

The National Institute of Standards and Technology (NIST)'s 800-171 guideline assists CMMC in addressing vulnerabilities in existing cybersecurity standards(Reciprocity 2020). An airport might self-assess and certify its cybersecurity posture using that standard. When the Department of Defence audited defence contractors, it discovered that too many of them were non-compliant with NIST SP 800-171, since the self-assessment allowed room for interpretation(Reciprocity 2020).The CMMC Accreditation Body overcomes this by requiring an independent contractor evaluation, which is conducted by a third-party assessment organisation (C3PAO) appointed by the CMMC Accreditation Body (CMMC-AB)(Reciprocity 2020). Airports are recommended to follow this standard as it is timely and covers all the security procedures making them resilient against cyber-attacks.

3.1 CMMC Levels and their Description

The CMMC framework consists of 171 cybersecurity best practices that are graded on a scale of one to five (Boatner et al. 2020). The CMMC maturity procedures formalize cybersecurity tasks to assure consistency, repeatability, and high quality. Starting with fundamental safeguarding at Level 1, the CMMC procedures progress to wide protection of Controlled Unclassified Information (CUI) at Level 3, and finally to lowering the risk of Advanced Persistent Threats (APTs) at Levels 4 and 5. The CMMC framework is accompanied by a certification scheme that verifies the process implementation.

Each CMMC level is made up of a series of processes and practices that are presented in Table 1 below. The procedures range from 'Basic Cyber Hygiene' at Level 1 to 'Advanced/Progressive' at Level 5, and the processes range from 'Performed' at Level 1 to 'Optimizing' at Level 5.

Levels	Processes	Practices
Level 5	Optimizing	Advanced/Progressive
Level 4	Reviewed	Proactive
Level 3	Managed	Good Cyber Hygiene
Level 2	Documented	Intermediate Cyber Hygiene
Level 1	Performed	Basic Cyber Hygiene

Table 1. CMMC Levels and their associated Processes and Practices

3.2 CMMC Domains

There are 17 domains in the CMMC model. Majority of these domains are derived from the security-relevant regions in Federal Information Processing Standard(FIPS) Publication 200 and the related security requirement families in NIST SP 800-171(Cyberassist 2020). The three domains of Asset Management (AM), Recovery (RE), and Situational Awareness (SA) are also included in the CMMC model (SA)(Cyberassist 2020).
The distribution of practices across domains per level is shown in Figure 1. The six domains of AC, AU, IR, RM, SC, and SI account for majority of practices (105 of 171).The distribution of practices across domains for Levels 4-5 is relatively more uniform than for Levels 1-3(Mellon and Hopkins 2020).The questionnaire was developed on the basis of distribution of practices as shown in Figure 1.

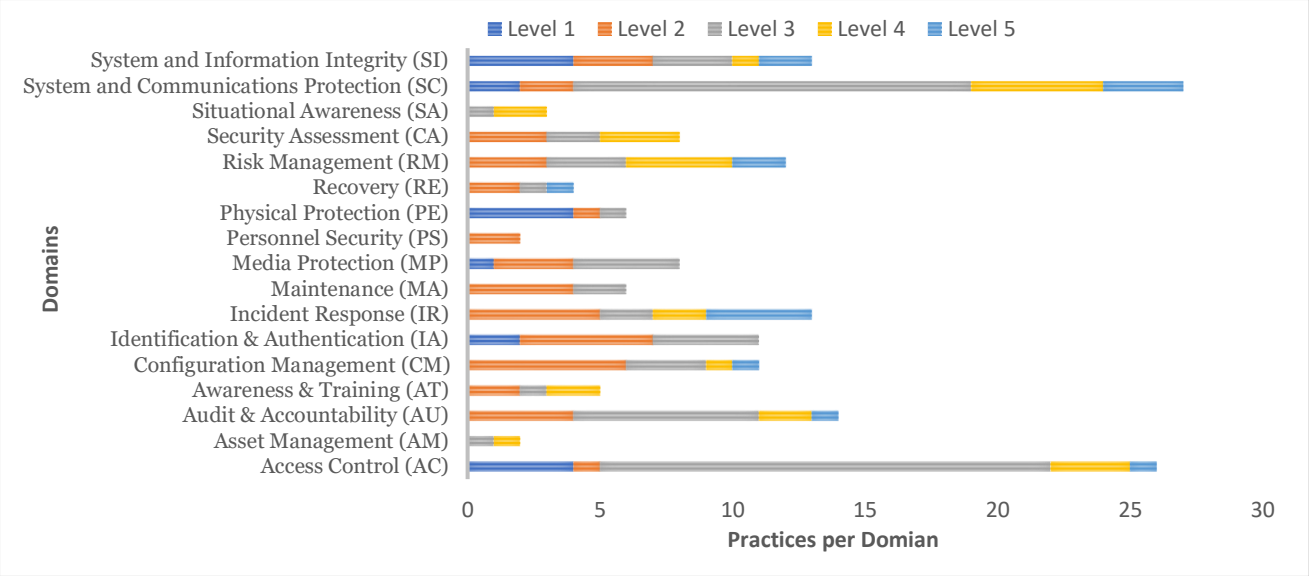


Figure 1: CMMC Practices for Domains at each Level

4 Methodology

The nature of the study is exploratory and analytical. The survey emphasizes on the field of cyber-security at airports and their provisions to set up cybersecurity controls. Survey methodology was adopted to ensure that the views of the airport officials could be obtained through the questionnaire and their awareness regarding the compliance of CMMC could be recorded. This research utilises both data obtained from the literature review and data collected from a survey. The survey focused on some of the busiest airports to analyse the understanding of airport IT and cyber-security personnel about cyber security practices followed at the airport with reference to the CMMC model framework. The survey respondents included airport officials and employees of the cyber department and/or the IT department. The survey was designed by including all CMMC levels, and the questions were grouped according to each level. This design would enable the researchers to investigate how aware and compliant the airports were with the CMMC model.

This research discusses all 5 levels of CMMC, but the study does not include all 171 practices due to the time and space constraints. The results of the survey focused on the governance of cyber-security, such as, the CCMC certification requirements and capabilities. Hence this study provides an overview of the airport's compliance with CMMC practices.

4.1 Survey

450 airports were contacted of which 150 airports declined to participate in the survey. Formal emails were sent to 300 airports, of which 24 responded, because either most of the airports were small airports or aerodrome so they did not respond to survey. Many did not wish to participate as they did not have a specified cyber or IT, department. In some cases, their designated employees had gone oversees due to their personal commitments and no one designated to this role was present at the airport. In some cases, the designated employees had gone oversees due to their personal commitments and no one designated to this role was present at the airport. For of the smaller airports, they were not operating due to Corona Virus. Some chose not to disclose their information due to privacy reasons. The survey responses were monitored for the kind of responses received for every level.

4.2 Developing the Survey

The questions were designed to make it simple for all airport employees to understand and respond to. The questions were created keeping in with practices covered under a specific domain for every level (figure 1). The category of questions included yes/no, agree/disagree, multiple choice questions (MCQs), linear scale etc. with 40 questions in total. The survey was developed using google forms which gave enough options to maintain user integrity and privacy by including consent from the participants. The questionnaire was prepared covering all five levels in 14 domains. Every level had a certain number of questions depending on the number of domains that were covered in that specific level - Level 1: Q1-Q5, Level2: Q6-Q19, Level 3: Q20-Q24, Level 4: Q25-Q33, Level 5: Q34-Q40.

5 Survey Results

Figure 2 below, presents compliance with CMMC practices for each level. The results were compiled by the combined analysis of the responses received for each individual question. After segregating the responses of each question into three categories of efficient, moderate, and below average, a response table was constructed for each question at each compliance level. These tables were then used to calculate the percentage for the three categories distinctly, for each compliance level. Subsequently this information was used to draw out a comparison for each category and level. Figure 2 represents total responses per level, with reference to *efficient, moderate,* and *below average* responses. The questions for every level varied depending upon the domains covered in that level.

The criterion for choosing scale of efficient, moderate and below average depended upon the choices given to the respondent for every question. For questions that were measured on a scale of 1-5, a response of 4 or 5 was considered as *efficient* while 3 was considered as *moderate* and the rest were considered as *below average*. For yes or no and unsure questions, yes was considered *efficient* the rest were considered as *below average*. For questions involving options like strongly agree, agree, and disagree strongly agree was considered as *efficient* while agree was considered as *moderate* and disagree as *below average*. Some questions involved frequency of compliance with options such as within last month, within last 3 months and, 12 months or more than 12 months. For such questions the option within last one month was considered as *efficient*, within last 3 months was considered as *moderate* and 12 months or more than 12 months were considered as *below average*.

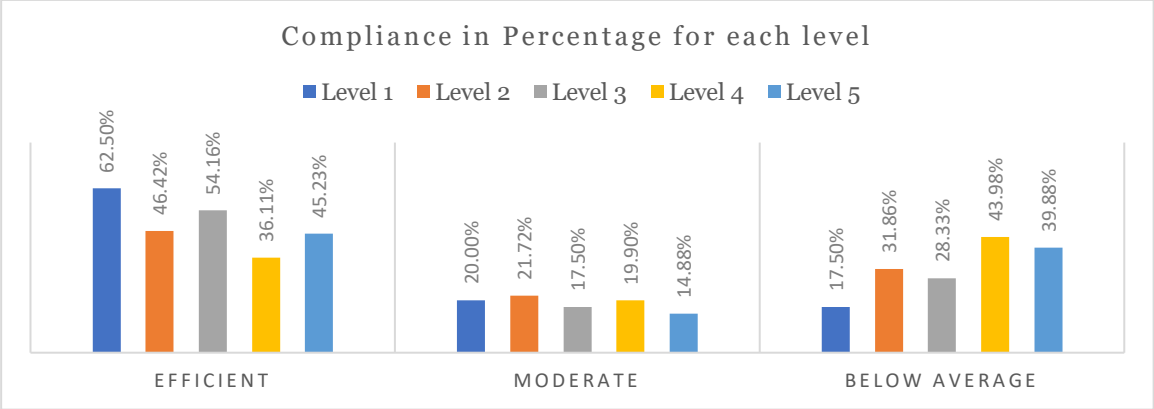


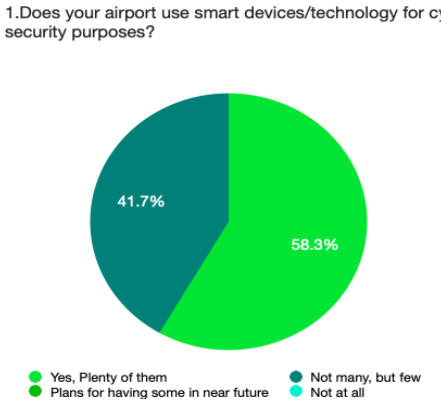
Figure 2: Compliance in Percentage for each level

6 Analysis and Discussion

The survey questions were classified into Level 1, Level 2, Level 3, Level 4, Level 5 according to the CMMC Model. As presented in figure 2, the combined responses by the airports were classified as *efficient, moderate,* and *below average*. It was observed that 62.5% of the airports were compliant with level 1, as it includes the basic cyber-hygiene practices. The results showed that the airports follow level 3 more than level 2, that is 54.16% as compared to 46.42%. From level 2 and 3 it can be inferred that airports had also implemented the processes of management much better than documentation. The airports are least compliant with level 4 with only 36.11% efficiency, followed by level 5 with 45.23%. From level 4 and 5 results, it can be concluded that airports do follow the processes that involve optimization of their practices which is covered in level 5, but they do not have enough processes for reviewing their adherence to implemented practices, which is part of level 4.
It was noted that most surveyed airports are either fully compliant to some extent with level 1 and level 3 practices. But the most *below average* compliance was obtained in level 4, level 5 and level 2. These findings highlight that airports need to be more proactive with their cyber-security practices, to mitigate unforeseen cyber-threat situations. It is evident that airports across all levels have maximum percentage of *efficient* responses for all levels except level 4. The *below average* percentage is higher than that of the *moderate* average compliance of results consisting of all the levels except for level 1.

The results presented in figure 3 below for question 1 show that, 58.3% of the airports have access to smart devices or technology for cyber security purposes. The remaining 41.7 % reported the use of few cyber security devices and technology. From the survey results it can be concluded that all the airports were aware of the importance of these devices and technology required to maintain

cyber security. The responses indicated that all the airports had anti-virus software installed for more than 3 years. This ensures basic protection against malicious software and programs.



Responses by Airports

Choices for Participant	Number of Responses
Yes, Plenty of them	14
Not many, but few	10
Plans for having some in near future	0
Not at all	0

Figure 3: Use of smart devices for cyber security at airports

The results of question 5 "*Is the FCI (Federal Contract Information) being protected?"* present that more than 50% of airports have the Federal Contract Information (FCI) protected. The rest of the airports are unsure, denoting a lack of proper cyber security awareness as well as equipment to make sure that sensitive information such as the FCI is protected. The results for Question 9 "*Are the airport authorities managing and auditing access to CUI?*" show that 50% of airports agree that their authorities were able to manage and audit access to Controlled Unclassified Information (CUI). Moreover, 29.2% were unsure about the management and accessibility of CUI. 20.8 % of airport personnel reported that there was no such practice was considered. Figure 4 question 14 below, shows that 41.7% of the airports had conducted risk assessment within the last 6-12 months, followed by 33.3% of the airports who had conducted their risk assessments in the last 3 months.25% of them within the last 12 months or more. Although the time span of conducting the risk assessments varied for every airport depending on their organizational structure, it was clear that they had all conducted a risk assessment which is important for maintaining basic cyber hygiene. The survey results showed that penetration tests are not widespread among the airports, which indicates a lack of intermediate cyber hygiene. This can be improved by implementing penetration testing exercises at the airports.

Responses by Airports

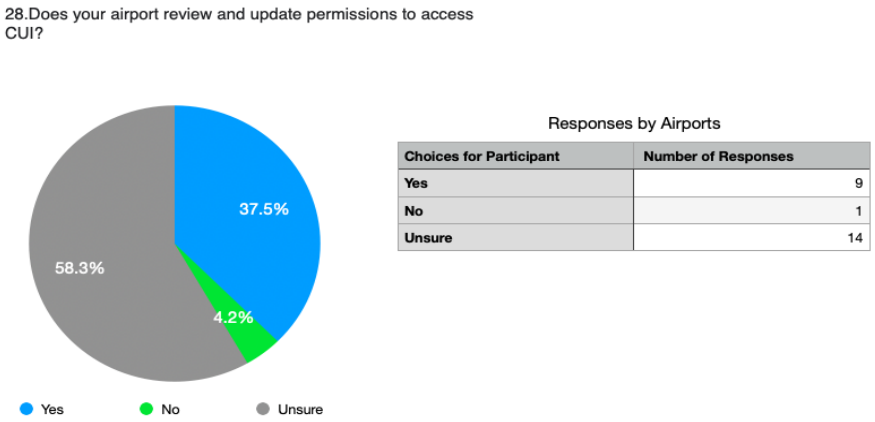
Choices for Participant	Number of Responses
Within last 1 month	0
Within last 3 months	8
6-12 months	10
12 months or more	6

Figure 4: Frequency of risk assessment at airports

The results for question 16 "*What is the frequency of penetration testing exercise at the airport?*" shows that majority of airports (41.7%) conduct a penetration testing exercise every six months. Some (12.5%) of them do it in a time span of every two years. There are a few (16.7%) which conduct such exercises once in a year, while very few (4.2%) of them conduct these exercises every four to five years. It was observed that 50% of airports agreed to follow the deny-all, permit-by-exception(whitelisting) and deny-by-exception(blacklisting) policy. Some of them (20.8%) strongly agree to have followed these policies at their airports. The rest of them were neutral in their responses. The results for question 23"*Do you agree that Whitelisting and Blacklisting policy is followed at your airport?"* overall have

been incredibly positive and only a few airports that are neutral should consider implementing this policy, as it is crucial in maintaining good cyber-hygiene at any organization, especially referring to level 3 implementation of the domain of Configuration Management in the CMMC model.

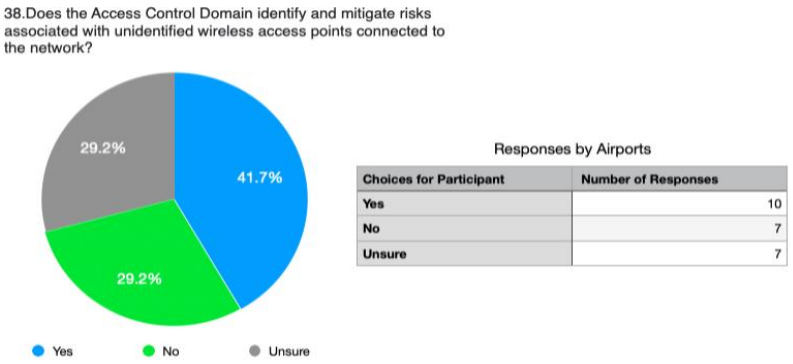
The survey question 28 as presented in figure 5 shows that 41.7% of the airports do not have a particular procedure to resolve the advanced persistent threats (APT). 16.7% have expressed that they have never observed any APT to date. Some of the airports chose that the time required for resolving an APT ranged from 6-12 months while others chose time ranging from 0-6 months. Very few were unsure regarding reviewing and updating permissions to access CUI. In the case of review and update permissions to access CUI, 58.3% of the airports reported of being unsure. The rest 37.5%, agreed upon reviewing and updating permissions to access the CUI. 4.2% denied having any such permissions.



Choices for Participant	Number of Responses
Yes	9
No	1
Unsure	14

Figure 5: Update, review permissions for accessing CUI at airports

The survey results for question 30"*Are practical exercises, which deal with current threat scenarios, part of cyber awareness training? Is proper feedback provided to the participating staff?"* show that 37.5% of the airports have a practical exercise-based training setup with a proper feedback mechanism, while 29.2% state that they do have practical training but lack a feedback process. The rest of the airports have no practical training, which might make them vulnerable to sudden attacks. 41.7% of the airports confirmed use of scanning tools and ad-hoc tests. Some of them are not sure regarding the usage, and 25% are unaware about such tools or tests being conducted. The survey responses for question 38 (figure 6) have been mixed as 41.7% of the airports agreed having response teams, with 12.5% strongly agreeing. Some responded neutral, which may indicate that they could have a response team but might not be always functioning. In addition, 20.8% of the airports disagree on having any such 24/7 response facility. In addition, 20.8% of the airports disagreed having a 24/7 response facility. 41.7% agreed on identification and mitigation of such risks as shown in figure 6. Airports that disagreed and responded as neutral are equal in percentage (29.2%).



Choices for Participant	Number of Responses
Yes	10
No	7
Unsure	7

Figure 6: Mitigating risk with respect to access control at airports

7 Recommendations

From the analysis of the survey results it can be recommended that the airports should consider compiling a yearly a cyber-security and maturity report. This report should include cyber-security practices that are followed or will be followed in the future. Airport systems contain vulnerable and sensitive information, in the event of a cyber threat or cyber-incident, every airport must preserve and uphold a backup of all its data. Therefore, it is necessary to understand their data and what parts of it are compliant with CMMC. This would be a crucial step in achieving CMMC compliance. Tax-related data, sensitive intelligence data, patents, and intellectual property are all examples of Controlled Unclassified Information (CUI). It is critical for airports to understand what CUI they collect, how it is processed, and where it is stored to appropriately decide the level of CMMC compliance they need to achieve. To find, monitor, and classify CUI, airports might employ solutions such as Data Loss Prevention technologies. It is impossible for the departments at an airport to keep track of and mitigate every security risk due to the complexity of airport functionality; as a result, all airport departments need to be informed about the implications and recommended practices to avoid penalties. It is also recommended that all airport employees should be given cyber training so that all credentials remain protected.

8 Conclusion

Most airports have few resources allocated to cyber protection and resilience. A few airports appear to have a more developed cyber security procedure. For all airport types, technical-based cybersecurity processes have a significant implementation rate, while organisational regulations, and standards have lower implementation rates, involving low levels of cyber security awareness and training priority. This study concludes that level one is most followed, while proactive and advance levels i.e., level 4 and 5, are least adhered to.

Commercial airports, airlines, business associates, and policymakers all have a shared responsibility for safeguarding airports against rising cyber threats. As a result, a collaborative cyber-resilience model defining the appropriate cyber security practices for airports is becoming increasingly important. Airport operators should prioritise cyber security initiatives to ensure the safety of operations for airlines and passengers. Cyber risks and associated threats will grow in parallel with technological developments, while the connection between safety and security in aviation will become interdependent.

For future research, all the CMMC practices including all 17 domains and all levels, could be considered. The surveys may be targeted to a specific country to achieve an in-depth analysis. Since airports are the face of the travel industry further research is needed in this area. There could also be research conducted by combining cyber-security governance and cyber-terrorism, as both are interlinked, and it would benefit the airports to improve their cyber-security practices and protocols.

9 References

Abeyratne, R. 2011. "Cyber Terrorism and Aviation—National and International Responses," Journal of Transportation Security volume (4:4), pp. 337-349.

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

Advances in Scientific Research and Engineering (ijasre) (6:1), pp. 188-195.

Azmi, R., Kautsarina, K., Apriany, I., and Tibben, W. J. 2020. Revisiting “Cyber” Definition: Context, History, and Domain. IGI Global.

Baker, D. M. 2020. "Tourism and Terrorism: Terrorists' Threats to Commercial Aviation Safety and Security," Tourism, Terrorism and Security. Emerald Publishing Limited 2020), pp. 163-181.

Bissell, K. 2013. "A Strategic Approach to Cybersecurity: As Cybercrime Grows Faster Than Companies Can Defend against, It's Time for a Serious Discussion on Cybersecurity. Though Many Are Calling for Federal Standards and Regulations--Which May Be a Matter of Time--in Their Absence, Organizations Should Transform How They Think About Cybersecurity.," Financial Executive (29:2), pp. 36-42.

Boatner, I., Chestler, A., and Mullen, J. 2020. "Insight: New Dod Cybersecurity Certification Holds Key to Contracts." Retrieved July 12 2021, from https://news.bloomberglaw.com/tech-and-telecom-law/insight-new-dod-cybersecurity-certification-holds-key-to-contracts

Brill, A. 2020. "Us and Eu Governmental Efforts to Protect Controlled Unclassified Information from Cyber Threats," Toward Effective Cyber Defense in Accordance with the Rules of Law (149), p. 81.

Cyberassist. 2020. "Cybersecurity Maturity Model Certification (Cmmc)." Retrieved July 12 2021, from https://ndisac.org/dibscc/cyberassist/cybersecurity-maturity-model-certification/

Dillingham, G., Wilshusen, G., and Barkakati, N. 2015. "Air Traffic Control: Faa Needs a More Comprehensive Approach to Address Cybersecurity as Agency Transitions to Nextgen," Congressional Requesters, p. 56.

Feng, B., Li, Q., Ji, Y., Guo, D., and Meng, X. 2019. "Stopping the Cyberattack in the Early Stage: Assessing the Security Risks of Social Network Users," Security and Communication Networks).

Fox, S. J. 2016. "Flying Challenges for the Future: Aviation Preparedness–in the Face of Cyber-Terrorism.," Journal of transportation security (9:3), pp. 191-218.

Gopalakrishnan, K., Govindarasu, M., Jacobson, D. W., and Phares, B. M. 2013. "Cyber Security for Airports," International Journal for Traffic and Transport Engineering (3:4), pp. 365 - 376.

Hawamleh, A. M. A., Alorfi, A. S. M., Al-Gasawneh, J. A., and Al-Rawashdeh, G. 2020. "Cyber Security and Ethical Hacking: The Importance of Protecting User Data," Solid State Technology (63:5), pp. 7894-7899.

Janczewski, L., and Colarik, A. 2007. Cyber Warfare and Cyber Terrorism. IGI Global.

Jiang, Y., Yin, S., and Kaynak, O. 2018. "Data-Driven Monitoring and Safety Control of Industrial Cyber-Physical Systems: Basics and Beyond." IEEE, pp. 47374 - 47384.

Katz, G. 2018. "British Airways Hack: Credit Card Details of 380,000 Stolen." Retrieved July 15 2021, from https://www.usatoday.com/story/travel/flights/todayinthesky/2018/09/07/british-airways-hack-credit-card-details-stolen/1223887002/

Lagazio, M., Sherif, N., and Cushman, M. 2014. "A Multi-Level Approach to Understanding the Impact of Cyber Crime on the Financial Sector," Computers & Security (45), pp. 58-74.

Lehto, M. 2013. "The Cyberspace Threats and Cyber Security Objectives in the Cyber Security Strategies.," International Journal of Cyber Warfare and Terrorism (3:3), pp. 1-18.

Lekota, F., and Coetzee, M. 2019. "Cybersecurity Incident Response for the Sub-Saharan African Aviation Industry," in: International Conference on Cyber Warfare and Security. ProQuest, pp. 536-XII.

Leukfeldt, E. R., Lavorgna, A., and Kleemans, E. R. 2017. "Organised Cybercrime or Cybercrime That Is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime," European Journal on Criminal Policy and Research (23:3), pp. 287-300.

Lewis, J. A. 2002. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic & International Studies Washington, DC.

Li, W., and Kamal, P. 2011. "Integrated Aviation Security for Defense-in-Depth of Next Generation Air Transportation System," in: 2011 IEEE International Conference on Technologies for Homeland Security (HST). Waltham, MA, USA: IEEE, pp. 136-142.

Lykou, G., Anagnostopoulou, A., and Gritzalis, D. 2018. "Smart Airport Cybersecurity: Threat Mitigation and Cyber Resilience Controls," IEEE Global IoT Summit (GIoTS), Bilbao, Spain: IEEE.

Manesh, M. R., and Kaabouch, N. 2017. "Analysis of Vulnerabilities, Attacks, Countermeasures and Overall Risk of the Automatic Dependent Surveillance-Broadcast (Ads-B) System," International Journal of Critical Infrastructure Protection (19), pp. 16-31.

Mellon, C., and Hopkins, J. 2020. "Cmmc Version 1.02," p. 28.

Meyer, S. 2018. "Airline Data Breaches Worrying." Retrieved 15 JULY 2021, 2021, from https://www.cpomagazine.com/cyber-security/airline-data-breaches-worrying/

Mezher, T., Khatib, S. E., and Sooriyaarachchi, T. M. 2016. "Cyberattacks on Critical Infrastructure and Potential Sustainable Development Impacts," in Sustainable Development Impacts. In Civil and

Environmental Engineering: Concepts, Methodologies, Tools, and Applications. IGI Global, pp. 545-562.

Monteagudo, J. 2021a. "Aviation Cybersecurity – High Level Analysis, Major Challenges and Where the Industry Is Heading." Retrieved July 7 2021, from https://cyberstartupobservatory.com/aviation-cybersecurity-major-challenges/

Monteagudo, J. 2021b. "Aviation Cybersecurity – High Level Analysis, Major Challenges and Where the Industry Is Heading. ." Retrieved 17th July, 2021

Peters, H. M. 2020. "Defense Acquisitions: Dods Cybersecurity Maturity Model Certification Framework," LIBRARY OF CONGRESS WASHINGTON DC.

Rajapaksha, A., and Jayasuriya, N. 2020. "Smart Airport: A Review on Future of the Airport Operation," Global Journal of Management and Business (20).

Reciprocity. 2020. "What Is the Cmmc Framework?" Retrieved July 10 2021, from https://reciprocity.com/resources/what-is-the-cmmc-framework/

Russell, S. 2020. "Trusted Ci Webinar: Cybersecurity Maturity Model Certification (Cmmc),").

Sampigethaya, K., and Poovendran, R. 2013. "Aviation Cyber–Physical Systems: Foundations for Future Aircraft and Air Transport," IEEE, pp. 1834 - 1855.

Schmidt, A. V. 2016. "Cyberterrorism: Combating the Aviation Industry's Vulnerability to Cyberattack," Suffolk Transnat'l L.), p. 169.

Stokes, A., and Childress, M. 2020. "The Cybersecurity Maturity Model Certification Explained: What Defense Contractors Need to Know." Retrieved July 10 2021, from https://www.csoonline.com/article/3535797/the-cybersecurity-maturity-model-certification-explained-what-defense-contractors-need-to-know.html

Suciu, G., Scheianu, A., Petre, I., Chiva, L., and Bosoc, C. S. 2019. "Cybersecurity Threats Analysis for Airports," in: World Conference on Information Systems and Technologies,WorldCIST 2019. Springer Verlag, pp. 252-262.

Taleqani, A. R., Nygard, K. E., Bridgelall, R., and Hough, J. 2018. "Machine Learning Approach to Cyber Security in Aviation," in: 2018 IEEE International Conference on Electro/Information Technology (EIT). Rochester, MI, USA: IEEE, pp. 0147-0152.

Thakur, K., Hayajneh, T., and Tseng, J. 2019. "Cyber Security in Social Media: Challenges and the Way Forward," IT Professional (21:2), pp. 41 - 49.

Thomas, T., Vijayaraghavan, A. P., and Emmanuel, S. 2020. Machine Learning Approaches in Cyber Security Analytics. Springer.

Ugwoke, F. N., Okafor, K. C., and Chijindu, V. C. 2015. "Security Qos Profiling against Cyber Terrorism in Airport Network Systems," in: 2015 International Conference on Cyberspace Abuja, Nigeria: IEEE, pp. 241-251.

Copyright