12-7-2022

Cybersecurity Maturity Model Capability in Aviation and Railway Industry

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

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

Cybersecurity Maturity Model Capability in Aviation and Railway Industry

Research-in-progress

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

Abstract

Cybersecurity is pivotal for the established aviation and railway industries. This study will examine the compliance of various levels of cybersecurity practices according to Cybersecurity Maturity Model Capability. This study will survey cybersecurity practices in aviation and railways. The data collected will be compared to identify which of the two industries is more compliant with the cybersecurity operational procedures. It will also enable the two industries to better evaluate and proactively address the threats by implementing cybersecurity best practices, governance and resilience processes.

Keywords Cybersecurity, CMMC, Aviation, Railways, Governance

1 Introduction

In various transportation systems, computers and communication networks play a crucial role. Intelligent transportation systems (ITS) are built on the foundation of these systems (Fok 2013; Kelarestaghi et al. 2018). The growth of ITS that integrate Information and Communication Technologies (ICT) leads to more services and features but, it contributes to various types of cyber-attacks (Tonn et al. 2019). In many of the world's most populated places, ITS has increased the effectiveness, uniformity, and efficiency of transportation networks (Iyer 2021). The technology revolution has benefited transportation systems significantly but it has also made data and goods more vulnerable to cyber-threats (Fok 2013). Moreover, when it comes to cybersecurity it has exalted risks that are amongst the most crucial issues affecting businesses worldwide. However, today's cyber challengers or nemesis work with more persistence and skill than before. With increased security, new goals emerge, such as asset, threat identification and identification of acceptable cybersecurity practices.

The aviation and railway transportation industries play a vital role in the enhancement of the global economy and are assets of the infrastructure. The two major transportation industries are used for transportation of passengers and cargo. The use of a variety of technologies and software solutions results in a wide range of data sets that are different from, yet inter-related with one another hence affecting the functioning of each other. For example, if a vulnerability is discovered in the European Rail Traffic Management System (ERTMS), it might affect all European railway systems (Masson and Gransart 2017). In the railway industry, cyber-attacks have become common. Hackers have previously attacked train firms in the United Kingdom, Germany, the United States, Poland, South Korea, Denmark, and Sweden (Kour et al. 2019). In 2003, a computer virus attacked the CSX Transportation system (a Florida railway corporation) and caused railway signals to be interrupted for times ranging from 15 minutes to 6 hours (Hancock 2003). In 2008, a 14-year-old Polish electronics prodigy hacked a tram system and derailed a tram, which crashed with another tram travelling in the opposite direction, injuring 12 passengers (Baker 2008). Aviation industry is no exception according to the PwC's 2015 Global Airline CEO Survey, 85% of airline CEOs perceive cybersecurity as significant and at alarming risk, especially due to the highly sensitive nature of flight systems and passenger data (Urban 2017).

For the protection of operators, economic considerations and citizen security, cybersecurity is considered significant in the transportation area (Masson and Gransart 2017). In both the aviation and railway industries, security is closely linked to system safety. In these industries cybersecurity refers to the protection of a secure system (Masson and Gransart 2017; Mohebbi et al. 2020). The protection of information systems against theft or destruction, as well as defense against cyber-fraud, external and internal risks, are essential for cybersecurity. The key concern for the railway and aviation industries is to minimize the risk of potential data loss while maintaining a consistent and reliable operation of their security systems. In the event of cyber-attack, serious repercussions might occur, including system failure, negative economic implications, and loss of sensitive data. To address these issues industries can follow the practices introduced within the Cybersecurity Maturity Model Certification (CMMC) to keep their systems protected and up to date (Brill 2020; Peters 2020). Therefore, this research will focus on whether the railway and the aviation industries are compliant with the CMMC.

1.1 Significance of study

The aviation and railway industries are two major pillars of the transportation system. Safety and security cannot be compromised as it can impact the passengers and cargo adversely. Travel is associated with leisure. Passengers using these transportation systems have increased crossing both national and international boundaries. Keeping this in mind it has become necessary for these travel sectors to incorporate intelligent infrastructure, implement smart facilities and update their cybersecurity practices. The implementation and adaptation of the advanced and latest cybersecurity practices will ensure safe travel for the passenger and cargo. This would provide safety against identity theft and cyber fraud which has become alarmingly common in recent times. The consequences of the cyber-threats or fraud require the aviation and the railway industries to implement risk assessment procedures and cybersecurity standards. This research would contribute to identify cybersecurity best practices and policies within the aviation and railway sector and compare their level of compliance with CMMC. The study would also play a vital role in improving the operational procedures and developing enhanced cybersecurity governance practices. This would allow the industries to better understand the risks and proactively respond by enforcing the best cybersecurity practices and resilience measures.

1.2 Research Problem

Unprecedented data loss might lead to a hostile cyber-attack, potentially resulting in loss of human life and property damage. As a result, cybersecurity is inextricably linked to the security and safety

procedures. In comparison to other businesses such as finance, aviation and railway industries are sometimes overlooked(Nobles et al. 2022; Thaduri et al. 2019). Ineffectiveness and a lack of awareness among authorities of aviation and railway industries greatly contribute to cyber-fraud. If any confidential information is exposed, it can lead to cyber-attacks which will then affect passengers, businesses and financial institutions. This can also be a very concerning rationale for cyber-terrorism. Despite many security procedures and practices that have been introduced to the industries, they still have been found to be vulnerable to cyber-theft as their databases have private and personal information of the travellers and cargo. Hence it becomes vital to research the compliance of cyber practices and procedures in these industries. This study will investigate the following research questions: Question 1: Are the aviation and railway industries compliant with the CMMC practices? Question 2: Which industry has a higher compliance with the CMMC norms and procedures?

1.3 Research Scope

The scope of this study will be limited to the CMMC practices and domains which are essential for both the aviation and railway industries. The domain for each level will be identified in accordance with the CMMC model (see Figure 1). The domains identified for cybersecurity practices are relevant to the aviation and railway industries. This research is an extension of the preliminary study on the implementation of CMMC model at the airports (Malhotra et al. 2021). The limitations of emphasizing the essential domains will keep the study more relevant. The focus of this study is on the evaluation of requirements at each level of CMMC model.

2 Related Works

A cybersecurity strategy incorporates methods to prevent, detect and react to the attacks for further management of data breaches (Lawrence 2009). The transportation industries are vulnerable to cybersecurity threats, which include malware, denial-of-service attacks, and other kinds of data manipulation (Azmi et al. 2020; Mezher et al. 2016). According to PwC's survey 85% of airline CEOs expressed their concerns about cyber risk versus 61% of CEOs in other industries (Urban 2017). Like any other industry, airlines are concerned about protecting sensitive customer or company data. Another threat for the aviation industry is the technological advancements used for the improvisation in the connectivity of the flight operation systems with ground crew and the air traffic systems. In 2013, the Air Transportation Network (ATN) carried over 48 million tons of freight and over 2.6 billion passengers. The global economic value for the same period was estimated to be 2.2 trillion dollars (Abeyratne 2016). Any cyber fraud in the aviation industry would lead to disastrous social and economic consequences. While the enhanced technological advancements are essential for improving the financial and operational performances, it is laying down the path for the opportunists who seek ways to exploit these advancements. Therefore, it is recommended for the aviation industry to upgrade their security procedures along with the adoption of advanced technologies to allow for a safe innovation (Starkie 2012). Air traffic control based on automated dependent surveillance broadcast is also a factor to consider for cybersecurity. Due to developments in aviation technology, cyber threats and attacks are posing a threat to future aircraft surveillance (Jiang et al. 2018; Sampigethaya and Poovendran 2013).Cyber-attacks are also becoming a cause of concern for the railway industry (Braband 2017; Kour et al. 2019). In 2011 in the north-western region of United States, hackers attacked remote computers, stopping the train signals (Masson and Gransart 2017). This incident demonstrates the dangers that railways encounter when they rely on current commercial-off-the-shelf (COTS) communication and computer equipment. The WannaCry virus has damaged train passenger information systems (Braband 2017).UK rail was struck by at least 4 significant data breaches in 2015. Cyber espionage like hacking into computer systems containing government data and key infrastructure in order to gain information (Cheshire 2016). In 2015, North Korea was suspected of pirating subway system in Seoul for several months. Dozens of terminals were infested with malware. Finally, in November 2016, the ticketing system of the BART at San Francisco was attacked by a ransomware that cyphers the hard disk of the ticket vending machines (Mohebbi et al. 2020). During a weekend, the public transport infrastructure was available for free until a solution was found (Masson and Gransart 2017). A cyber-attack on a South Korean subway system in 2015 resulted in data and information leaks (Hayden 2015), as well as a significant data breach at the Swedish Transport Agency that resulted in the release of personal transport data (Borg et al.). Rail Europe stated in May 2018 that a malware assault had resulted in a three-month data breach of credit and debit cards (Whittaker 2018). A huge Distributed Denial of Service (DDoS) attack on the Danish national rail operator (DSB) in May 2018 also rendered some activities, including ticketing systems and communication infrastructure, inoperable (Paganini 2018).Modern technologies, such as the use of machine learning, combined with enhanced governance procedures within the aviation and railway industries, with a focus on the

requirement for the Cyber Maturity Model, can help improve cybersecurity (Taleqani et al. 2018; Thomas et al. 2020). The rise in cybercrime and cyber terrorism is concerning, with the latter being regarded as a distinct and discrete threat that has grown more serious as a result of globalisation and broad internet usage and must be dealt with individually (Abeyratne 2011). Cyber-terrorism is linked to tourism, implementing best practice cybersecurity incident response standards in the aviation industry is a viable technique for dealing with cyber threats (Lekota and Coetzee 2019). To limit the anxiety and damages caused to travellers and the tourism sector, cybersecurity policies are required.

3 Cybersecurity Maturity Model Certification

On January 31, 2020, the US Department of Defense (DoD) published the Cybersecurity Maturity Model Certification (CMMC) version 1.0, which is the latest cyber-security compliance model. It was designed in collaboration with University Affiliated Research Centers, Federally Funded Research and Development Centers, and the private sector(Stokes and Childress 2020). Each CMMC level comprises a set of procedures and practices, as shown in Table 1. Level 1 practices vary from 'Basic Cyber Hygiene' to 'Advanced/Progressive' at Level 5, while Level 5 procedures range from 'Performed' to 'Optimizing.'

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

Prior to CMMC, the National Institute of Standards and Technology (NIST) 800-171 model was introduced. But DoD determined that too many contractors were non-compliant with NIST SP 800-171, since self-assessment had a lot of room for interpretation for identifying the security flaws (Reciprocity 2020). The CMMC Accreditation Body (CMMC-AB) addressed this by demanding an independent contractor evaluation, which has to be carried out by CMMC Third Party Assessment Organisation (C3PAO) selected by CMMC-AB(Reciprocity 2020). This standard hence can be used by aviation or railway industries to examine and certify their cybersecurity posture. In the CMMC model, there are 17 domains. The majority of these domains are drawn from Federal Information Processing System (FIPS) Publication 200's security-relevant regions and NIST SP 800-171's corresponding security requirement families (Cyberassist 2020). Figure 1 depicts the distribution of practices across domains and levels. The AC, AU, IR, RM, SC, and SI domains comprise the majority of practices (105 of 171)(Mellon and Hopkins 2020).

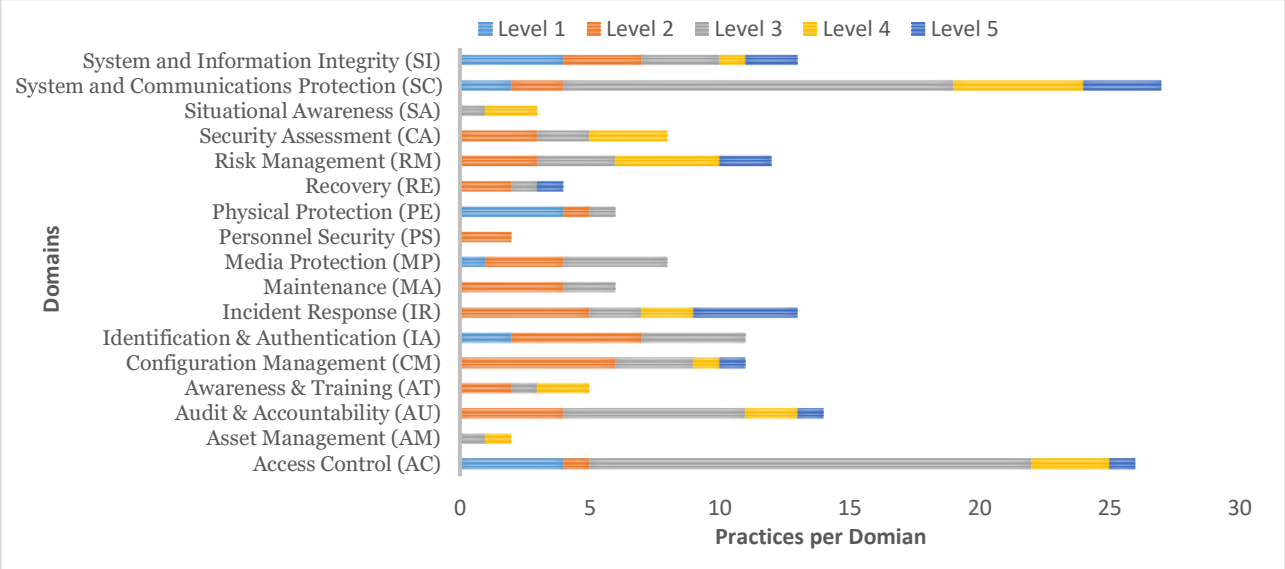

Figure 1. CMMC Practices for Domains at Each Level

CMMC is a single standard for integrating cybersecurity throughout the defense industrial base (DIB), which comprises over 300,000 enterprises(Stokes and Childress 2020).

CMMC accreditation will ultimately be mandatory for DoD contractors. All suppliers at all levels of the supply chain, as well as small companies, commercial item contractors, and international suppliers, are included. The CMMC Accreditation Body (CMMC-AB) will work closely with the Department of Defense to create processes for certifying third-party assessment organisations (CP3AOs) and assessors who will assess firms' CMMC levels (Stokes and Childress 2020).

4 Methodology

A survey will be used to collect data through a set of well-structured questionnaires. There will be questionnaires developed for aviation and railway industries. This research is a comparative study focusing on the aviation and railway industries. The reports of some major airports, airlines and railways globally will be reviewed to gain an understanding of the research problem. This study aims to identify the industry's compliance to with domains associated with levels in the CMMC framework. The most relevant practices per domain which are efficient to be addressed and implemented by the aviation and railway industries will be selected as depicted in figure 1 and the survey questions will be developed for every level. Thereafter, the data collected from survey responses will be both qualitatively and quantitatively analyzed. A comparison of best practices of the two industries will be determined. A preliminary study had focused only on airports. This study will extend the preliminary study to investigate cybersecurity procedures in the railway industry.

5 Preliminary Study Results

450 airports were contacted and 300 responded. Due to the pandemic and absence of concerned staff only 24 airports could participate out of the 300 respondents in the survey. Figure 2 shows compliance with CMMC procedures for each level. The findings were obtained using a combined analysis of all the responses received for each question. After categorizing each question's responses into three categories: *efficient, moderate, and below average*, a response table for each question at each compliance level was created. These tables were used to compute the percentages for each compliance level for the three categories separately. This data was used to create a comparison for each category and 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 *efficient* while 3 was considered as *moderate* and the rest were considered *below average*. For yes, no and unsure questions, yes was considered *efficient* the rest were considered *below average*. For questions involving options like strongly agree, agree, and disagree. Strongly agree was considered *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 *moderate* and 12 months or more than 12 months were considered *below average*.

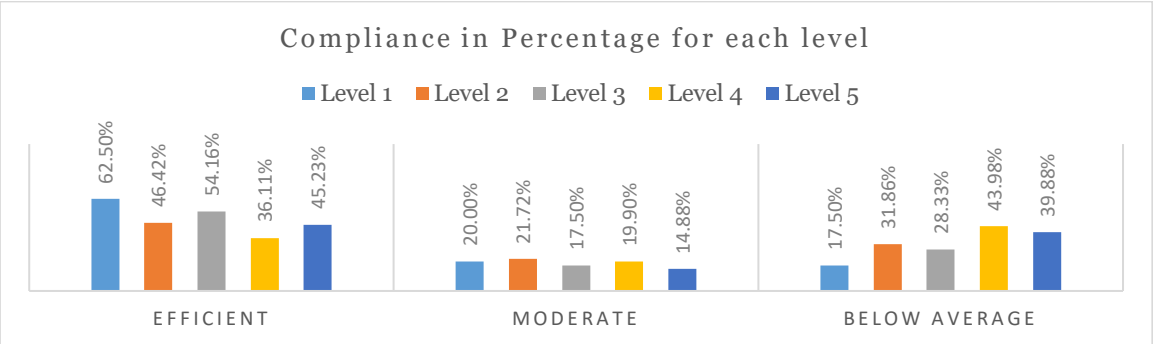

Figure 2. Compliance in Percentage for Each Level

The survey questions were grouped into Level 1,2,3,4 and 5 of the CMMC model. Level 1 compliance was 62.5%, which covers most basic cyber-hygiene standards. The results showed that airports are more likely to follow level 3 than level 2, with 54.16% following level 3. Level 2 was followed by 46.42%. Management practices were implemented better than documentation, as evidenced by levels 2 and 3. 36.11% were compliant to level 4 efficiency, followed by 45.23% for level 5. Based on

the results of levels 4 and 5, it can be determined that airports follow the procedures that include optimizing their practices (level 5), but they do not have adequate processes for assessing their adherence to established practices (level 4). The majority of airports were either compliant or somewhat compliant with level 1 and 3 procedures. However, level 4, 5, and 2 had the lowest levels compliance levels. These findings depict, the need to be more proactive with cybersecurity policies. Except for level 4, airports at all levels have the highest percentage of efficient answers. The proportion of outcomes that are below average is larger than the moderate average compliance of results, which includes all levels except level 1.

6 Conclusion and Future Research

The results of the preliminary study found that most airports have limited resources for cybersecurity and resilience. Only a few airports appear to have a more sophisticated cybersecurity mechanism in place. Technical-based cybersecurity procedures have a high adoption rate across all airport types. However, organisational laws and standards have a lower implementation rate, implying a low level of cybersecurity awareness and training priority. According to the findings, level one is the most adhered to, whereas proactive and advanced levels, i.e., level 4 and 5, are the least adhered levels. The result from the preliminary study lays the foundation for this research. Future research will investigate the compliance with the CMMC model within the two major transportation industry that is aviation and railways. Also, it will determine what the policy makers in the aviation and railway industries include in their security programs to mitigate cyber-fraud risks.

7 References

Abeyratne, R. 2016. *Regulation of Air Transport*. Springer.

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

Baker, G. 2008. "Schoolboy Hacks into City's Tram System," *The Telegraph* (11), p. 2008.

Borg, M., Olsson, T., Franke, U., and Assar, S. "Digitalization of Swedish Government Agencies," *40th International Conference on Software Engineering: Software Engineering in Society*, pp. 37-46.

Braband, J. 2017. "Cyber Security in Railways: Quo Vadis?," *International conference on reliability, safety and security of railway systems*: Springer, pp. 3-14.

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.

Cheshire, T. 2016. "Four Cyber Attacks on Uk Railways in a Year."

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

Fok, E. 2013. "An Introduction to Cybersecurity Issues in Modern Transportation Systems," *ITE Journal* (3), p. 19.

Hancock, D. 2003. "Virus Disrupts Train Signals," *CBS News*).

Hayden, S. 2015. "Cyber Attack on South Korean Subway System Could Be a Sign of Nastier Things to Come." Vice News.

Iyer, L. S. 2021. "Ai Enabled Applications Towards Intelligent Transportation," *Transportation Engineering* (5), p. 100083.

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.

Kelarestaghi, K. B., Heaslip, K., Khalilikhah, M., Fuentes, A., and Fessmann, V. 2018. "Intelligent Transportation System Security: Hacked Message Signs," *SAE International Journal of Transportation Cybersecurity and Privacy* (1:11-01-02-0004), pp. 75-90.

Kour, R., Aljumaili, M., Karim, R., and Tretten, P. 2019. "Emaintenance in Railways: Issues and Challenges in Cybersecurity," *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit* (233:10), pp. 1012-1022.

Lawrence, P. 2009. "Meeting the Challenge of Aviation Emissions: An Aircraft Industry Perspective," *Technology Analysis & Strategic Management* (21:1), pp. 79-92.

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.

Malhotra, O., Dey, S., Foo, E., and Helbig, M. 2021. "Cyber Security Maturity Model Capability at the Airports,").

Masson, É., and Gransart, C. 2017. "Cyber Security for Railways–a Huge Challenge–Shift2rail Perspective," *International workshop on communication technologies for vehicles*: Springer, pp. 97-104.

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

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.

Mohebbi, S., Zhang, Q., Wells, E. C., Zhao, T., Nguyen, H., Li, M., Abdel-Mottaleb, N., Uddin, S., Lu, Q., and Wakhungu, M. J. 2020. "Cyber-Physical-Social Interdependencies and Organizational Resilience: A Review of Water, Transportation, and Cyber Infrastructure Systems and Processes," *Sustainable Cities and Society* (62), p. 102327.

Nobles, C., Burrell, D., and Waller, T. 2022. "The Need for a Global Aviation Cybersecurity Defense Policy," *Land Forces Academy Review* (27:1), pp. 19-26.

Paganini, P. 2018. "Massive Ddos Attack Hit the Danish State Rail Operator Dsb."

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

Reciprocity. 2020. "What Is the Cmmc Framework?" Retrieved July 10 2022, from reciprocity.com/resources/what-is-the-cmmc-framework/

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

Starkie, D. 2012. "European Airports and Airlines: Evolving Relationships and the Regulatory Implications," *Journal of Air Transport Management* (21), pp. 40-49.

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

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.

Thaduri, A., Aljumaili, M., Kour, R., and Karim, R. 2019. "Cybersecurity for Emaintenance in Railway Infrastructure: Risks and Consequences," *International Journal of System Assurance Engineering and Management* (10:2), pp. 149-159.

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

Tonn, G., Kesan, J. P., Zhang, L., and Czajkowski, J. 2019. "Cyber Risk and Insurance for Transportation Infrastructure," *Transport policy* (79), pp. 103-114.

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.

Whittaker, Z. 2018. "Rail Europe Had a Three-Month Long Credit Card Breach." ZD Net.

Copyright