



INFORMATICS
INSTITUTE OF
TECHNOLOGY

INFORMATICS INSTITUTE OF TECHNOLOGY

In Collaboration with

UNIVERSITY OF WESTMINSTER

Framework for Cyber Security in Aviation

A dissertation by

Mr. Radeep Premkumar

Supervised by

Dr. Nimalaprakasan Skandhakumar

Submitted in partial fulfilment of the requirements for the MSc in Cyber security and Forensics degree at the University of Westminster.

September 2022

Abstract

In an increasingly complex transportation system, safety is of fundamental concern, as aircraft failure frequently results in fatalities and serious injuries. When it comes to aviation transportation safety, prevention is unquestionably the best method. A successful approach to preventing potential accidents from occurring has been demonstrated through the use of historical incident data. Aviation safety specialists analyse incident reports to determine the primary and contributing causes that contributed to the occurrence in order to identify possible safety concerns and develop effective prevention programs. However, the cost of hiring cyber security specialists and conducting their reviews has become excessively expensive in recent years. The number of incidences is expanding at a rapid pace, owing to the quickening of technological advancements and the expansion of the commercial as well as private aircraft transportation businesses, both public and private. Therefore, advanced text analysis algorithms should be used to assist aviation safety experts in the extraction of incident data, which will save time and effort. This study focuses on the issues of the aviation sector. The study was conducted by conducting a questionnaire survey of quantitative as well as qualitative study among passengers and cyber security experts and aviation experts respectively. IBM SPSS analytical software used for the statistical analysis of the data collected from the respondents. It is critical to recognize that APTs are never a novel method of executing an attack, nor are they something that could be blocked as well as disrupted before and the problem will be solved. An advanced persistent threat (APT) is better understood as a cyberattack campaign rather than as a particular sort of threat. There is no single defensive mechanism that can be used to stop these kinds of attacks from occurring. Because they rely upon signatures stored in their databases, the traditional techniques in use have been unable to prevent these new attacks. Instead, a defence-in-depth strategy, which employs many layers of protections to protect against such attacks, should be implemented. The global frameworks provided do not consider the local environment in terms of a country, and as a result, some organizations would find it really difficult to completely apply such frameworks because they are not adapted to meet their own business models and operations. The purpose of this study is to suggest a new framework that will take into consideration the airports' readiness and awareness levels, as well as a new and effective framework that is suited to the specific operations and process operations of the airport.

Keywords: *Aviation, IBM SPSS, APT attacks, PPT framework and Cyber security*