**Project Plan:**

**Aviation Cybersecurity Awareness Platform**

**Ritesh Mahendrakumar Vaidya | L39150615**

**Project | Computer Science**

**Introduction**

Data protection, passenger safety and aviation operations are of prime importance in terms of cybersecurity. Financial and operational risks are faced with an increasing threat: ransomware, phishing, as well as Insider attacks in the industry. But, although there are ICAO, EASA and FAA regulations, employees don’t have a sufficient level of real-life cybersecurity training. As a gamification, real-time threat simulators, practical exercises based on an interactive cybersecurity awareness platform, this project seeks to touch upon these aspects.

**Why is This Important?**

Even though aviation may be a technical realm, it is still quite susceptible to hackers. It is used by hackers to spy on others, to conduct operational sabotage and also for financial gain. Breach can lead to flight delays, data theft, or reputational harm. Traditional training methods do not create the necessary cybersecurity skills given to the employees. This initiative bridges the compliance to actual threat mitigation gap and ensures that aviation personnel are prepared to protect vital systems.

**Literature Review**

Weak passwords, phishing and mishandling private data are a major cause of cybersecurity breaches in aviation, and human error makes up the vast majority of them. The traditional training doesn’t involve real-world threat preparation. Through a focused project, this paper introduces interactive, scenario-based, gamified training with real time simulation to build more engagement, improve retention, and increase security skill levels of aviation professionals.

**Problem Statement and Motivation**

Evaluation of real-world aviation cybersecurity training on critical infrastructure skills, and their impact on pilot and air traffic controller vulnerability was conducted. Passenger data and flight systems are exploited by cyber threats that are often too late detected. This project is aimed at developing an interactive platform that will improve awareness, response and overall aviation security with my passion for technology, cybersecurity and aviation.

**Aim and Objectives**

This project aims to develop an interactive cybersecurity awareness platform to increase the aviation workers’ ability to determine what cyberthreats are occurring, stem the threat, and deal with it. It will then analyse existing training programs, detect risks, determine cybersecurity awareness and install a gamified, real-time threat simulation platform. The platform’s efficacy will be evaluated through case studies and expert comments, and incorporated cybersecurity training suggestions will be made to aviation safety procedures.

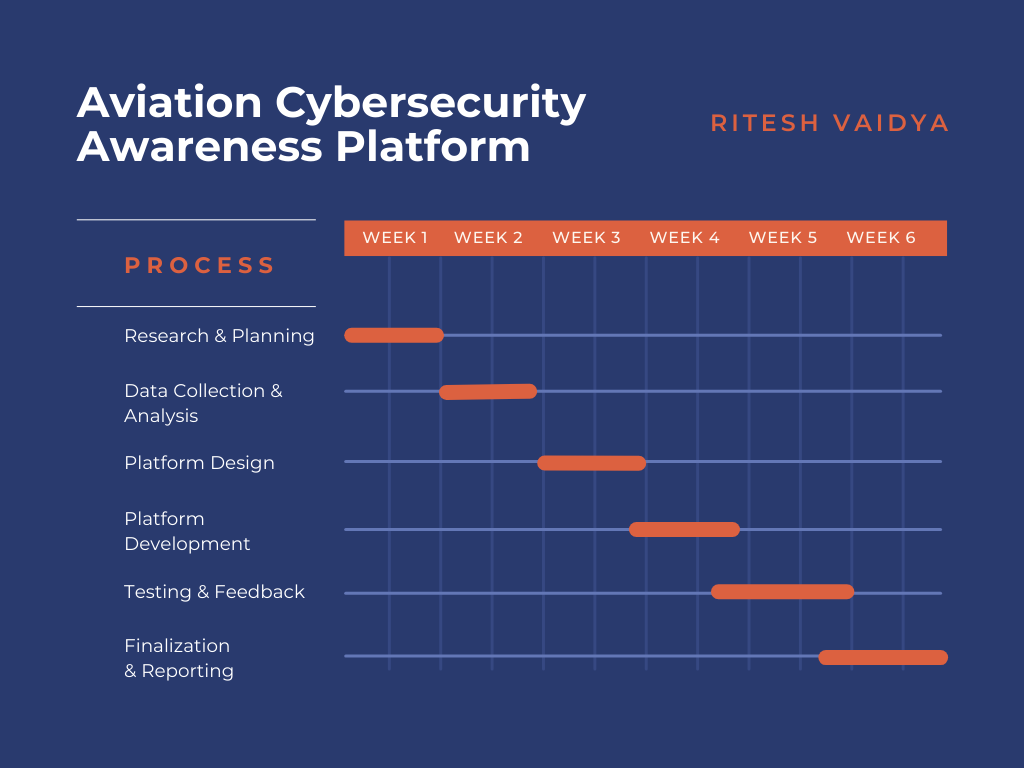
**Expected Outcomes**

In order to address the cybersecurity training shortages in aviation, an interactive cybersecurity awareness platform will be developed as a working prototype. In the study, cyberthreats will be addressed, any training deficiencies assessed, and recommendations provided across the board. Security awareness of personnel will rise, errors that cause cyber mishaps will decrease and aviation’s defences against changing threats will be strengthened.

**Research Strategy**

To determine how the aviation industry determines cybersecurity awareness, this study employs a secondary qualitative research technique, reading industry/publications, academic literature, and regulatory standards. The study will then review cyberthreat and training techniques. The next thing is the designing and creating of the interactive cybersecurity platform. Its efficacy will be evaluated through case studies and expert input, and will finally suggest final improvements for the aviation cybersecurity training program.

**Time Line**



**Ethical Considerations**

The fact that this study uses secondary data means that ethical issues that arise during personal data collecting are not relevant. In order to uphold academic integrity, all sources will be properly attributed, and none of the private aviation security information shall be used. Ethical standards will be followed in the creation of cybersecurity training as the study will always be open and reliable.

**Conclusion**

However, the cybersecurity attacks threaten aviation operations and safety, but knowledge about these issues is low. The goal of this project is to plug that gap by building an interactive training platform that makes cybersecurity readiness more gamified, simulation, and adaptive learning.

By increasing aviation resilience through raising awareness and reducing exposures associated with human error, this effort will lead to this result. It is motivated by my love of technology and aviation and, as far as I see it, this study can give out a significant and lasting impact in industrial security.

**Appendices**

**Appendix A: Survey Questions**

Included in this section are sample survey questions asked in the research, which assess the current cybersecurity awareness levels of aviation professionals.

Sample Questions:

1. To what extent are you aware of the threats that are present in aviation organizations?

2. Have formal training on cybersecurity that can be related to the aviation systems of the company?

3. Considering the type of cyber threats, you perceive as most critical in the aviation field?

4. On what frequency do you conduct cybersecurity exercises, like using simulations?

5. What would you recommend be done to improve the aviation cybersecurity training?

**Appendix B: Case Studies**

The following availing real-life cybersecurity scenarios are demonstrated in this section, with information on the consequences of the breach on operations and safety and possible measures of prevention.

Example Case Study:

According to August, the incident involved a major airline being attacked by ransomware, resulting in disrupted flight operations and a data breach.

•Consequence: flight delays, heavy losses and compromise of the important passengers’ data.

•Resolution: More secure infrastructure, better education of personnel and the presence of new control mechanisms.

**Appendix C: Platform Design Overview**

The interactive platform’s interface and features are described in this appendix along with screenshots and design specifications.

Key Features:

Gamification: The ideas that have been proposed include presenting challenges and simulated cyber threats.

•Real-time Alerts: Instant notifications about simulated security breaches.

•Adaptive Training Module: Using AI-based learning, the training module adapts to the user’s performance.

•Interactive Exercises: Hands-on cybersecurity drills and quizzes.