CYBR 271 SECURE PROGRAMMING 2023
STUDENT NAME: Thomas Green STUDENT ID: 300536064

PART ONE – Security Cards

1. Human Impacts.

Human Impact	***Impact on Stakeholder***
Emotional Wellbeing.	Stakeholders might experience heightened stress and frustration if Service Application experiences system unavailability or data breaches. These issues could lead to disruptions in their workflow and uncertainty about the accuracy of their tasks, causing emotional distress.
Financial Wellbeing.	Unauthorised alterations and inaccuracies in maintenance records could lead to disputes, legal issues, and financial losses. System unavailability might cause delays, penalties and reputation impact, while confidentiality breaches could compromise competitive edge and financial stability.
Personal Data.	Insufficient data protection measures may expose Aircraft maintenance personnels' sensitive information, risking identity theft or unauthorised access.
Physical Wellbeing.	Innaccurate maintenance instructions or system unavailability within the Service Application may result in proper aircraft servicing, potentially endangering the physical wellbeing of crew members and passengers. This underscores the critical need for precise information delivery to ensure safe maintenance procedures for personnel.
Relationships.	Failure to deliver precise maintenance instructions through the service application could result in accidents, tarnishing the organizations reputation and jeopardizing stakeholder relationships. Moreover, unauthorized alterations or data breaches might strain regulatory and partner relationships raising compliance concerns and potential disputes.
Societal Wellbeing.	Widespread system vulnerabilities could erode public trust in the aviation industry, impacting the societal wellbeing of those who rely on air travel. Accidents stemming from unauthorized alterations might raise concerns about aviation safety potentially leading to mass hysteria and affecting access to transportation resources.
The Biosphere.	If the Service Application's unavailability or unauthorized alterations lead to aircraft accidents, it could harm environment and wildlife. Engine run time extensions due to delays might cause excessive resource consumption, while inproper maintenance procedures could result in increased emissions, contributing to environmental degradation.

2. Identify Threats to the System.

Human Impact	***Threat***	***Motivation***	***Resources***	***Method***
Emotional Wellbeing.	Unauthorised Access to Aircraft Records	Desire or Obsession: Threat actor might seek unauthorised entry into aircraft maintenance records in order to reveal sensntive data about organisation's maintenance policies, procedures or aircraft specifics	Tools: Threat actor could wield sophisticated hacking abilities, enabling them to leverage potential vulnerabilities in the Service Application or the organisation's data center security protocols	Technological Attack: Threat actor might employ their advanced methods to breach aircraft maintenance database. Sucessful breach could expose confidential maintence records, leading to emotional distress among personnel who feel violated and concerned about potential breach consequences
Financial Wellbeing.	Insider Fraud	Money: An insider threat, like an employee or contractor, could participate in fraudulent actions to siphon funds or valuable assets from the orgnisation for personal benefit	Money: Insider threat possess necessary access to financial systems, accounts and sensitive financial data, which they could exploit for carrying out fraudulent transactions	Technological Attack: Threat actor might trigger unauthorised financial transactions, falsify signatures, tamper with accounting records, or redirect funs to personal accounts, resulting in substantial fincancial losses for the organisation
Personal Data.	Social Engineering and Phishing Attacks	Desire or Obsession: Adversary might employ techniques (social engineering) and phishing attacks to mislead maintence crew members into revealing passwords and credentials, enabling unauthorised access to personal data stored within service application	Inside Capabilities: Adversary could use persuasive tactics either by email or message techniques to deceive misleading crew members	Technological Attack: Adversary sent emails and messages deemed fraudlent that appear legitimate to prompt maintence crew members to enter credentials on fake website pages to gain information for benefit
Pysical Wellbeing.	Human mistakes recording information	Unusual Motivations: Aircraft information documentation can	Inside Capabilities: Maintence crew holds responsibility of	Indirect Attack: Unintentional errors in aircraft information

Human Impact	***Threat***	***Motivation***	***Resources***	***Method***
		be flawed due to human errors due to maintence crew neglecting duties	aircraft upkeep. Inattentive crews can introduce errors during aircraft information documentation	documentation can arise from crew. Crew is anticipated to accurately record information
Relationships.	Damage to Interorganizational Relations	Politics: An adversary with political motives might attempt to damage the relationships between organizations within the aviation industry by targeting the Aircraft Service Application	Inside Capabilities: The adversary, possibly an insider with access to interorganizational communication and data, could exploit their inside capabilities to sabotage communication channels and create misunderstandings	Manipulation or Coercion: The adversary may manipulate or disrupt interorganizational communications through unauthorized alterations or data breaches. By sowing discord and mistrust, they can harm relationships between airlines, maintenance providers, and other stakeholders, negatively impacting collaborative efforts and business parternships
Societal Wellbeing.	Disruption of Public Infrastructure	Malice or Revenge: An adversary driven by malice or a desire for revenge might attempt to disrupt public infrastructure, such as airports or air traffic control systems, by targeting the Aircraft Service Application	Inside Capabilities: The adversary, potentially an insider with knowledge of public infrastructure and cyber-physical systems, could exploit their inside capabilities to identify vulnerabilities and disrupt critical systems	Physical Attack: The adversary may engage in physical attacks on public infrastructure or cyber-physical systems connected to the application. Such attacks can lead to disruptions in air travel, causing physical harm, affecting access to resources, and negatively impacting the emotional wellbeing of society
The Biosphere.	System malfunctions	Unusual Motivations: Service Application not being used properly by crew or sevice applications not properly being implemented. As a result	Inside Capabilities: Access to service applications and functionalities by developers and crew	Indirect Attack: indirect damage to service application by improper use carried out by developers or crew

Human Impact	***Threat***	***Motivation***	***Resources***	***Method***
		neglectful behaviour or usage by service applicatione		

4. Identify the Most Relevant Threats to the System

Identify the THREE most relevant threats to the system.

Ranking (most to least)	**Threat**
1.	Data Breach by Attacker
2.	Unauthorised Access of Records
3.	Manipulation of Maintence Checklists

Define what you mean by “relevant” and discuss why you chose these threats to the system as most relevant.

“Relevant” in this context refers to the severity of potential consequences and the likelihood of the threats being exploited. These three threats are relevant because they have the potential for significant impact on the safety, security, and wellbeing of individuals, society, and the overall aviation industry. The scenarios selected are based on the realistic possibly of exploitation, considering the sensitivity of the data involved and the potential for harm if a successful attack occurs.

Data breach most relevant due to potential for negative impacts. Successful breach compromises privacy and personal security, eroding stakeholder trust and organisation’s reputation. Data loss can be exploited against the organisation, leading to financial and legal liabilities. The risk of data breaches is heightened with the implementation of the Service Application, broadening the attack surface. As technology plays a critical role in modern business, the likelihood of a data breach is relevant.

Unauthorised access to records, driven by financial motivations and theft of valuable intellectual property. Threat is pertinent due to the potential financial gains for attackers. Valuable assets such as maintenance methods, aircraft information, and sentitive data can be exploited and sold to competitors.

Manipulation of maintenance checklists as third most relevant because it poses a direct risk to safety of crew and passengers. Threat endangers physical and societal wellbeing in aviation operations. Unchecked maintenance issues could lead to critical incidents, causing panic, distrust, and reputational damage.

5. Propose How to Mitigate the Threats

Threat	***Mitigation (what and why will work)***	***Negative Effects***
Data Breach by Attacker	Adopting multi-factor authentication (MFA) requires users to authenticate their identity using multiple verification methods, such as passwords, biometrics or security tokens. This approach adds an extra layer of security, making it more challenging for attackers to gain unauthorised access. By demanding multiple forms of verification, MFA effectively mitigates the risk of data breaches by fortifying the authentication process and thwarting attempts by malicious actors	Users need to provide additional forms of verification beyond their usual credentials. While this extra layer of security enhances protection, it also requires users to adapt to a slightly modified login process. This change may necessitate a short period of adjustment, potentially causing a temporary sense of inconvenience or frustration among users who are accustomed to a more streamlined authentication process. This should be addressed when implemented offering clear user education and support during the transition phase to minimise negativity while users adapt to it
Unauthorised Access of Records	Intrusion detection system (IDS) actively surveils the system, analysing patterns of access and behavior for anomalies or signs of suspicious activity. By employing this technology, administrators receive real-time alers when potential threats are detected, enabiling swift response and intervention. This mitigation measure acts as a defense mechanism, swiftly identifying and thwarting unauthorised access attepts.	IDS can occasionally produce false positives, misidentifying harmless actions as threats, or false negatives, missing actual threats. This introduces the challenge of increased alert management for administrators. They must carefully review and validate each alert to ensure accurate threat detection. This process, while viatal for security, can potentially lead to alert

Threat	***Mitigation (what and why will work)***	***Negative Effects***
		fatigue where administrators spend significant time distinguishing between genuine threats and benign activities, aiming to prevent unnessary disruption to normal operations
Manipulation of Maintence Checklists	Implementing real-time data auditing involves continuously monitoring checklist changes in real time, allowing for immediate detection of any unauthorised modifications. Administrators are promptly alerted to these alterations, empowering them to take corrective actions. By adopting real-time data auditing, the system gains ability to maintain integrity of maintenance checklists, preventing unauthorised alterations and maintaining trust of critical maintence procedures	Continuous monitoring and analysis of data in real time could lead to marginal increase in system resource utilisation. During periods of heightened auditing activity, such as simulataneous updates and checks, there might be a temporary reduction in system performance. This dip in responsiveness could occur due to additional processing load placed on the system as it actively tracks and verifies changes, potentially affecting the overall user experience during these moments.