CYBR 271 SECURE PROGRAMMING 2023
STUDENT NAME: Raashna Chand STUDENT ID: 300607575

PART ONE – Security Cards

1. Human Impacts.

Human Impact	***Impact on Stakeholder***
Emotional Wellbeing.	Constant unavailability and bugs of the service application may cause crew members to be irritated and upset that they are unable to perform their jobs properly.
Financial Wellbeing.	Confidential information such as manuals and airplane parts may be breached and accessed by competitors. This will allow them to use the knowledge to improve their own planes, financially profit from them, and cause financial loss to our company due to an inferior product.
Personal Data.	Crew certifications being accessed by unauthorized parties may allow these parties to impersonate crew members for other gain, and use these certifications for identity fraud.
Physical Wellbeing.	Inaccurate records of replacements of different parts of the airplane may mean that physical harm will take place, e.g. if a part needs to be repaired, but the instruction manual is for a different part and the crew member cannot tell that it is wrong, leading to an accident happening.
Relationships.	Crew members could distrust office members and be wary of what they are advising them to do, leading to crew ignoring instructions from the office and using the service application inaccurately.
Societal Wellbeing.	Customers no longer trust the company to provide quality airplanes for air travel due to inadequate repairs and faulty equipment.
The Biosphere.	Combined power usage of airplanes and data storage facilities requires lots of electricity, which may not be sourced from reliable energy sources.

2. Identify Threats to the System.

Human Impact	***Threat***	***Motivation***	***Resources***	***Method***
Emotional Wellbeing.	A denial of service attack by an attacker impacts availability of the service application.	Self-promotion: the person wants their name to be known for the fun of it and wants people to be scared of them.	Money: the person is able to pay a lot for bots to send requests to the service application and the web application.	Technological attack: The person launches a denial of service attack, overloading the data flows to and from the legacy web application and the service application. They announce it on their social media that the service application will be down for hours.
Financial	Someone from a	Money: The person wants to	Tools: the person has	Multi-phase attack: the person can

Human Impact	***Threat***	***Motivation***	***Resources***	***Method***
Wellbeing.	competing airplane manufacturing company gains access to instruction manuals and information on airplane parts that this company uses.	use this information to improve their company's airplanes to gain an edge over this company in the market and therefore take more profit.	cryptographic key crackers that are able to crack passwords and other credentials to use to access the databases.	slowly start to use their tools to gain credentials, peruse through the database like a normal employee would, so as to not raise any alarms. They can then download these instruction manuals and information to their own hard drive and transfer them to their own company's databases.
Personal Data.	The attacker would like to impersonate a crew member on a social media website and use it to catfish people into dating her.	Curiosity/boredom: the attacker just wants to see what she can get away with by poking around at the system and see what kinds of people she can fool.	Expertise: the attacker has had experience in social engineering to do just this, and has low-level experience in database injection.	Processes: the attacker would go through a process to change the crew member's login details to something the attacker can access. Upon success, the attacker can see all the personal information of the crew member and use it for her catfishing.
Physical Wellbeing.	An ex-crew member wants to exact revenge on their former manager through physical harm.	Malice or Revenge: the ex-crew member was reprimanded for a mistake by their former manager and hasn't let go of the grudge since.	Insider knowledge: the ex-crew member knows what parts are installed in each airplane, and what parts are suitable for each airplane. They are also aware of the times that the manager is on duty. This allows them to carry out what they want to do at the right time.	Physical attack: the ex-crew member secretly swaps out a part with an identical-looking object on their last day on duty. The object is something like an explosive. The manager will try to carry out repairs, but triggers something that makes the object explode.
Relationships.	An attacker impersonates an office member to give bad instructions on using the service application to the crew members.	Curiosity/boredom: the attacker is curious as to what will happen to the relationships when he sows distrust between everyone.	Time: the attacker has all the time in the world as he's unemployed, so he can do whatever he wants.	Processes: the attacker would exploit a flaw in the legacy web application that allows them to sign up as an office member without raising any suspicion. Then he would start sending out incorrect instructions to the crew members.

Human Impact	***Threat***	***Motivation***	***Resources***	***Method***
Societal Wellbeing.	An Israeli state-sponsored organization modifies the databases to provide inaccurate information on airplane parts.	Diplomacy/warfare: the Israeli government wants to sabotage the company's country's resources in hopes of starting a full-scale war.	Impunity: since the organization has the support of the Israeli government, anything they do will almost certainly have no negative consequences.	Technological attack: the organization uses an SQL injection (presuming that SQL is indeed the language) to give them full access to the database, and gain privileged access to modify data in the tables. This will hinder maintenance tasks and cause airplane faults that may be harmful for passengers.
The Biosphere.	An environmental activist sabotages the database's power supply.	World View: the activist is concerned with the company's carbon footprint and wants them to address this issue.	Inside capabilities: the activist has a collaborating office member that has physical access to the facility housing the power supply of the database.	Attack cover up and Physical attack: The insider that the activist has will provide the office with a distraction (such as a fire alarm or an important meeting) that will allow them to tamper with the power supply. This will take systems offline for a long time, delaying maintenance tasks.

4. Identify the Most Relevant Threats to the System

Identify the THREE most relevant threats to the system.

Ranking (most to least)	**Threat**
1.	Someone from a competing airplane manufacturing company gains access to instruction manuals and information on airplane parts that this company uses.
2.	A person/organization modifies the databases to provide inaccurate information on airplane parts.
3.	A denial of service attack by an attacker impacts availability of the service application.

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

Write your answer here.

I defined threats as relevant based on how likely the threat will occur, or in other words, how realistic the threat is.

I think that an organization or person trying to access databases for their own personal or financial gain is the most realistic threat. Even if the airplane manufacturing company isn’t the best in the world, competing companies will want to find out what they can do better. People are always hungry for more information. They can do this through semi-legitimate means, such as through an ex-employer of the company, or they can do so illegally. This threat can also be carried out in a vast array of ways – social engineering, technological attack, manipulation and coercion, to name a few. For this reason, I think this threat is the most relevant.

The second most relevant is a person or organization modifying the database to provide inaccurate information about parts. It doesn’t necessarily have to be a state-sponsored organization – though say, if the airplane manufacturing company made military aircraft, then this specific threat would be higher up on the list. Again, competing companies may want to sabotage their competitors to gain an edge over them in the market. Ruining their reputation would be the best way to do so. Moreover, SQL and other database injections are very common attacks. Attackers could use the Service Application and the Legacy Web Application to take advantage of inputs not being sanitized and manipulate information on the database.

The third most relevant in my opinion is a denial of service attack on the service application. The service application may not be configured to process a lot of requests at the same time. Anyone can flood the service application with a bunch of fake requests and impact its loading time. While the scenario of a hacker wanting to do this for self-promotion is unlikely, a DoS attack can be used as a cover-up for a vast array of other attacks, such as database modification and database access mentioned before, or even for in-person attacks such as theft or physical harm.

5. Propose How to Mitigate the Threats

Threat	***Mitigation (what and why will work)***	***Negative Effects***
Someone from a competing airplane manufacturing company gains access to instruction manuals and information on airplane parts that this company uses.	Encrypt the instruction manuals and other information using an encryption algorithm such as RSA. That way, if any one downloads anything from the databases, they will need the private key to decrypt everything.	- Who will have access to the private key? The more people with the key, the more chances this key will fall into the wrong hands, and the less effective this mitigation will be. - The system may malfunction in a way that files in the service application will be unreadable to crew members - It may be inconvenient for crew members and office staff to always need to access the private key just to read a few pages of a manual
A person/organization modifies the databases to provide inaccurate information on airplane parts.	Sanitize inputs; make sure that only certain people can access and modify the database, malicious code cannot be inserted, and that certain tricks such as 1=1 doesn't give one full access to the database. In this way, unauthorized parties won't be able to modify the database using attacks such as SQL injection.	This will not address attacks where the attacker can simply impersonate an office/crew member that *is* allowed to access and modify the database, and therefore carry out the attack without a problem. Sanitizing inputs is long and arduous, and therefore some inputs may get missed, which an attacker can then take advantage of.
A denial of service attack by an attacker impacts availability of the service application.	Implement a DDoS protection software such as "Cloudflare" or "haproxy". This will detect if incoming traffic is legitimate and not botted, reducing the chance of a DDoS attack being successful.	This will increase the loading time of the service application, as the software needs several seconds to up to a minute to check incoming traffic, and this will be a source of inconvenience for the staff. The software may even detect legitimate traffic as botted, leading to more inconvenience.