1. After the recent downtime of the NOTAM system by the FAA, which turned out to be caused by a contractor mistakenly deleting files, you are tasked with preventing this system's downtime in the future.

Asset: The NOTAM System. Since the damage done with this system shutting down was catastrophic, the goal is to devise a plan to prevent downtime in the future for any reason.

Threat 1: Downtime due to employee errors either deliberate or mistaken. In the example above, the downtime was due to a mistake by an employee, however, the actions in a similar scenario could be deliberate.

Threat 2: Cyber Attacks. The system could also face downtime due to cyber attacks and these could again lead to significant damage and cost the government millions of dollars.

Countermeasure 1 (non-technical): To combat deliberate employee error, I would instate more thorough background checks when hiring. As for mistaken errors, I would educate employees in more depth about the system and limit their access to parts of the system that could cause significant damage. Thus, the more sensitive parts of the system would be limited to trusted experts who know what they are doing.

Countermeasure 2 (technical): I would upgrade the cybersecurity of the NOTAM system to prevent cyberattacks and bring the security up to date with prevalent cyber attacks today. This would help prevent downtime due to cyber attacks.

2. A professor at State University wants to perform classified research for the US government. In addition to having to handle international students performing the research, one has to ensure the security of the information as well. Describe how you would ensure such confidentiality.

Asset: The classified research for the US government would be the asset in this case. This would be sensitive information which must be kept confidential.

Threat 1: The classified information being leaked by students. With the international students, they are being exposed to sensitive information valuable to another country.

Threat 2: The information being compromised due to low security in general.

Countermeasure 1: Keeping the information given to the students to an absolute minimum. This would only include giving information absolutely necessary for the students to perform research. Also making the students (international or not) go through thorough background checks and making them sign confidentiality agreements.

Countermeasure 2: Keeping access to the research data to a minimum. Ideally, only the professor and government agents should be given complete access to the information. This countermeasure also includes reinforcing the security of the computer systems the information is stored on. Additionally, physical access to this computer is limited as well. This will help minimize leaks and prevent the data from being compromised.

3. These days Catalytic Converters are being stolen from cars. How would one combat this problem?

Asset: The catalytic converter is an essential component of the vehicle's emission control system, which helps to decrease the amount of pollutants emitted from the exhaust pipe. It is expensive to replace and thieves damage cars when stealing them.

Threat: The theft of Catalytic Converters in Charlottesville.

Countermeasure 1: Increase police patrolling in parking garages at night, preventing the theft of these converters when they are most likely to be stolen by thieves.

Countermeasure 2: Educate car owners about tactics to prevent Catalytic Converter theft such as installing anti-theft devices, painting the number, scratching in your VIN, etc.