Cybersecurity Risk Assessment Report:

<Project name>

<team name>

<Team members>

<Date>

Executive Summary

<Generate your own>

Introduction

<Modify to your specifications>

The purpose of this cyber risk assessment report is to meticulously evaluate and address the various cybersecurity risks associated with a groundbreaking student-led satellite project at <University>. This ambitious endeavor, driven by a dedicated team of cybersecurity majors, aims to construct, launch, and manage a satellite, marking a significant milestone in the university's foray into space exploration and technology. The focal point of our cybersecurity efforts centers on ensuring the robustness and integrity of the ground station computer system, which serves as the critical communication link between the team and the satellite.

The satellite project introduces a complex array of cyber risks that could potentially compromise the mission's success and safety. Recognizing the pivotal role of cybersecurity in this context, our team has embarked on a comprehensive risk assessment to identify, evaluate, and mitigate potential threats. This initiative is crucial for safeguarding the satellite and ground station against cyberattacks, operational failures, and compliance violations, thereby securing the mission's objectives and our stakeholders' investment in this venture.

Given the stakes of the project, our risk assessment extends beyond conventional cybersecurity challenges, encompassing unique threats associated with space operations, such as unauthorized command/control, jamming, battery draining attacks, and regulatory compliance failures. These challenges underscore the importance of a rigorous and adaptive cybersecurity strategy tailored to the specific needs and vulnerabilities of the satellite mission.

As we navigate through the complexities of cybersecurity in space technology, this report serves as a foundational document outlining our strategic approach to managing cyber risks.

By detailing our methodology, findings, and recommendations, this report aims to provide a clear and actionable roadmap for enhancing the cybersecurity posture of the satellite project. It is designed to inform and guide the project team and stakeholders ensuring that cybersecurity

considerations are integral to the project's planning, execution, and future management.

Methodology

The methodology employed in this cyber risk assessment is designed to systematically identify, evaluate, and propose measures to mitigate cybersecurity risks associated with the <> student-led satellite project. Given the project's focus on constructing and managing a satellite, including the crucial ground station computer, our approach integrates practical cybersecurity practices, compliance efforts, and collaborative insights from interdisciplinary teams. This section outlines the steps taken to ensure a thorough and effective cyber risk management process.

Risk Identification

Our first step in our methodology was to identify risks of the system, and in order to do that we needed to learn how the system functions and what regulations we would need to comply with. We identified regulatory requirements and some common satellite specific risks as well as other common risks to normal computers like the ground station computer. Meeting with the hardware team, we learned the components of the satellite and discovered potential avenues of attack through them. Conducting a vulnerability scan on the ground station computer was our final round of risk identification.

Risk Assessment

Following the identification of potential risks, the next step in our methodology was the thorough assessment of these risks. This phase involved evaluating the identified risks in terms of their likelihood of occurrence and potential impact on the project. Utilizing a combination of the information gleaned from our initial hardware team collaboration and the insights from our vulnerability assessment of the ground station computer, we were able to prioritize the risks based on a structured criteria. This evaluation took into account factors such as the severity of potential damage, the exploitability of identified vulnerabilities, and the criticality of affected system components. The risk assessment phase was instrumental in

quantifying and qualifying the nature of the cyber threats we faced, enabling us to develop a prioritized list of risks that warranted immediate attention and mitigation strategies.

Reporting + Recommendations

<Modify to your needs>

The final phase of our methodology culminated in the synthesis of our findings into this detailed report, which not only outlines the identified risks and their assessments but also proposes specific recommendations for mitigating these risks. This report serves as a strategic document, offering actionable insights and tailored recommendations aimed at enhancing the cybersecurity posture of the satellite project. Our recommendations are based on best practices in cyber security and are designed to address the unique vulnerabilities and threats identified through our comprehensive assessment process. Key recommendations include the implementation of secure configuration of hardware modules, regular software updates and vulnerability patches, and the development of contingency plans for critical systems. Through this reporting and recommendation phase, we aim to provide a clear and actionable path forward to mitigate the cyber risks associated with the satellite project, ensuring its security and compliance throughout its lifecycle.

Findings

Our team identified, assessed and prioritized various weaknesses in the system that may pose a threat to the project. Our findings are as follows.

<Modify to your needs>

Identified Risks

This section presents a comprehensive catalog of the cybersecurity risks identified during our assessment process. These risks, emerging from technical vulnerabilities, operational challenges, and external threats, highlight potential weaknesses within the satellite project's cyber infrastructure. Detailed herein are the various threat vectors that could

potentially compromise the integrity and functionality of both the satellite and the ground station.

Threat Vector #1 – Item

Threat/Risk Item

Explanation, analysis

Threat Vector #2 – Item

Threat/Risk Item

Explanation, analysis

Threat/Risk Item

Explanation, analysis

Threat/Risk Item

Explanation, analysis

Impact and Likelihood Assessment

Following the identification of potential risks, this section delves into a systematic evaluation of each risk in terms of its likelihood of occurrence and the extent of its potential impact on the project. We have given a score for each item’s impact level and its likelihood level, combining to indicate criticality. This assessment provides perspective on the severity of the identified risks, guiding the prioritization process by highlighting the threats that pose the greatest danger to the project's success and security.

<Modify to your needs>

1. Item

- Probability: (1-5) – Explain probability
- Impact: (1-5) – Explain impact

2. Item

- Probability: (1-5) – Explain probability

- Impact: (1-5) – Explain impact

Risk Prioritization

Building on the insights gained from the risk impact and likelihood assessment, this segment prioritizes the identified risks. By arranging the risks in order of their criticality, this prioritization aids in focusing mitigation efforts on the most significant threats first, ensuring efficient allocation of resources and strategic planning to address the vulnerabilities most likely to impact the project adversely.

Priority Rankings:

1. **Item**
2. **Item**
3. **Item**

Identified Risk	Component	Likelihood Score	Impact Score	Risk score	Mitigation
Item	Ground Station	2	4	8	Summary of mitigation strat
Item	Satellite Main Board	1	5	5	Summary of mitigation strat

Recommendations

Mitigation Recommendations

This section of the report delineates our targeted recommendations for mitigating the cyber risks identified during our comprehensive assessment. Drawing from the vulnerabilities and threats uncovered, we propose a series of strategic actions designed to enhance the cybersecurity posture of the satellite project, particularly focusing on the ground station computer, satellite command protocols, and overall system integrity.

Recommendation

Explanation

Recommendation

Explanation

Recommendation

Explanation

Conclusion + Additional Recommendations

Explain lessons learned, conclude, any additional non related recommendations