ISEC 0635: Information Security Operations Management

Winter Term 2023

Eric Webb

Professor Ling Wang

Assignment 2: An Overview of Lockheed Martin's Business Continuity, Disaster Recovery, and Incident Response.

Dear Executives,

This executive report details an overview of Lockheed Martin's business continuity, disaster recovery, and incident response plans. The report describes the plans, policies, and procedures developed to ensure business continuity, disaster recovery, and incident response within the Lockheed Martin organization with a focus on source code management. It is imperative that Lockheed maintains strong postures in these domains to stay competitive in the aerospace and defense industries.

The business continuity plan outlines nine policies and procedures for ensuring continuity of essential business operations during and after a disruptive event. These include an introduction, business impact analysis, risk management, crisis management, business continuity strategy, IT disaster recovery plan, communication plan, training and awareness, and testing and maintenance.

The disaster recovery plan entails eight policies and procedures for backing up critical data and proprietary systems, recovering them in the event of an outage, and continuously improving the plan. The policies and procedures include an introduction, disaster recovery team, risk assessment, backup and recovery strategy, emergency response plan, communication plan, testing and maintenance, training and awareness, and continuous improvement.

The incident response plan details nine policies and procedures for responding to an incident related to intellectual property, including containment, investigation, recovery, and reporting. It includes an introduction, incident response team, threat assessment, incident response procedures, evidence collection, legal and regulatory compliance, communication plan, training and awareness, and continuous improvement.

Lockheed Martins version control system assured operations plan documents policies and procedures to protect intellectual property, implement access controls, and maintain patch and change management for Lockheed Martin's codebase which is primarily stored on GitHub and physical backups. This documents and helps assure the operation of Lockheed's Version Control Systems and protects the proprietary intellectual property they contain.

In conclusion, Lockheed Martin's business continuity, disaster recovery, and incident response plans provide a comprehensive framework for ensuring the continuity of essential business operations during and after a disruptive event, backing up proprietary systems, recovering them in the event of a disaster or outage, and responding to incidents related to intellectual property. The plans are a testament of Lockheed Martin's commitment to innovation, excellence, and the advancement of Science, Technology, Engineering, and Math in a safe and secure manner.

Thank you again!

-ERIC WEBB

CISSP

**References**

[**https://sustainability.lockheedmartin.com/sustainability/Content/Lockheed\_Martin\_2020\_Sustainability\_Report.pdf**](https://sustainability.lockheedmartin.com/sustainability/Content/Lockheed_Martin_2020_Sustainability_Report.pdf)

Naik, N., Jenkins, P., Grace, P., & Song, J. (2022). Comparing Attack Models for IT Systems: Lockheed Martin’s Cyber Kill Chain, MITRE ATT&CK Framework and Diamond Model. 2022 IEEE International Symposium on Systems Engineering (ISSE), Systems Engineering (ISSE), 2022 IEEE International Symposium On, 1–7. <https://doi-org.ezproxylocal.library.nova.edu/10.1109/ISSE54508.2022.10005490>

Lockheed Martin Corp SWOT Analysis. (2022). Lockheed Martin Corporation SWOT Analysis, 1–7. <https://search-ebscohost-com.ezproxylocal.library.nova.edu/login.aspx?direct=true&db=buh&AN=160991532&site=eds-live>