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.

Lockheed Martin is one of the largest defense contractors in the world and has a global reach on the defense and aerospace industries. Lockheed has a strong reputation for innovation and excellence in its products and services which can include fighter jets, helicopters, missiles, radar systems, spacecraft, energy, and advanced technologies for cybersecurity. Lockheed Martin came to be as a result of a merge between the Lockheed Corporation and Martin Marietta. Today they are committed to the advancement of Science, Technology, Engineering, and Math. (STEM)

*Lockheed Martins Business Continuity Plan:*

1. Introduction: Overviews the plans purpose, scope, and objectives of the BCP.
2. Business Impact Analysis: Performs an assessment of Lockheed's’ processes, systems, functions, and intellectual property that are critical. The assessment is done to identify potential threats, vulnerabilities, and impacts.
3. Risk Management: Defined policies and procedures for identifying, assessing, and mitigating risks to critical business operations, assets, and data.
4. Crisis Management: Defined policies and procedures to manage crises, emergencies, and disasters effectively.
5. Business Continuity Strategy: Defined policies and procedures to ensure continuity of essential business operations during and after a disruptive event.
6. IT Disaster Recovery Plan: Defined policies and procedures to restore critical IT systems, networks, and data in the event of a disaster or outage.
7. Communication Plan: Defined policies and procedures to communicate effectively with all stakeholders, including employees, customers, vendors, and the public.
8. Training and Awareness: Training set in place so that employees can be educated on the business continuity plan and emergency response procedures.
9. Testing and Maintenance: Defined policies and procedures to conduct regular testing and maintenance of the business continuity plan to ensure its readiness and effectiveness.

*Lockheed Martins Disaster Recover Plan:*

1. Introduction: Overviews the plans purpose, scope, and objectives of the DRP.
2. Disaster Recovery Team: a list of the key personnel responsible for executing the disaster recovery plan and their roles and responsibilities.
3. Risk Assessment: a thorough assessment of potential risks and vulnerabilities to critical systems and infrastructure, including natural disasters, cyberattacks, and other potential disruptions.
4. Backup and Recovery Strategy: a plan for backing up critical data and systems and recovering them in the event of a disaster or outage.
5. Emergency Response Plan: a set of procedures and protocols for responding to an emergency, such as evacuating personnel, securing facilities, and mitigating damage.
6. Communication Plan: a comprehensive strategy to communicate effectively with all stakeholders, including employees, customers, vendors, and the public.
7. Testing and Maintenance: a plan to conduct regular testing and maintenance of the disaster recovery plan to ensure its effectiveness and readiness.
8. Training and Awareness: a plan to train employees on the disaster recovery plan, emergency response procedures, and other critical aspects of continuity management.
9. Continuous Improvement: a process for continuously reviewing and improving the disaster recovery plan based on lessons learned from actual events, changes in technology, and other factors.

*Lockheed Martins Incident Response Plan:*

1. Introduction: Overviews the plans purpose, scope, and objectives of the IRP.
2. Incident Response Team: Definitions of the employees responsible for executing the incident response plan along with their roles and responsibilities.
3. Threat Assessment:An assessment of potential threats and vulnerabilities to organizational intellectual property, including internal and external threats. Along with methods for detecting and monitoring them.
4. Incident Response Procedures: Procedural definitions for responding to an incident related to intellectual property, including containment, investigation, recovery, and reporting.
5. Evidence Collection: Definitions for collecting and preserving evidence related to the incident, including documentation, forensic analysis, and a chain of custody.
6. Legal and Regulatory Compliance: Definitions and procedures for complying with legal and regulatory requirements related to the protection of intellectual property such as data privacy laws and contractual obligations.
7. Communication Plan: Defined procedures to communicate effectively with all stakeholders, including employees, customers, vendors, and law enforcement authorities.
8. Training and Awareness: Training of employees on the incident response plan, security policies and procedures, and other critical aspects of intellectual property protection.
9. Continuous Improvement: Procedures to continuously review, critique, and improve the incident response plan. Based on lessons learned from actual incidents, changes in technology, and other experiences.

https://sustainability.lockheedmartin.com/sustainability/content/Lockheed\_Martin\_2020\_Sustainability\_Report.pdf

It is no secret that Lockheed Martin has a strong reputation for providing and innovating solutions within the aerospace and defense industries. It is imperative for an organization like Lockheed to maintain a strong information security posture to protect systems from cyber threats. Cyber protection is needed to succeed in these highly competitive markets.

To maintain good security operations, Lockheed employs a combination of software, hardware, practices, and people. This is done by implementing good security functions such as firewalls , intrusion detection, intrusion prevention, access controls, policies, procedures, training, and having a dedicated team of security professionals.

To help assess Lockheed Martin’s security posture, a Strengths-Weaknesses-Opportunities-Threats (SWOT) matrix was conducted. A SWOT matrix is a tool that can be used to help define the SWOT properties in an organization.

SWOT Matrix of Lockheed Martin’s Security Operations

Strengths: Extensive security hardware and software from having a history of government / military contracts and an experienced security team.

Weaknesses: Employee awareness, training, and slow turn around implementing updates after identification of evolving threats.

Opportunities: Potential to grow in the areas of Artificial Intelligence, Machine Learning, and Blockchain.

Threats: Staying up to date with regulatory requirements and defending against a growing sophistication of cyberattacks.

To address organizational challenges, it is essential that roles are clearly defined to all stakeholders. There should be a coordinated effort from all parties to ensure the organizations security posture.

Board of Directors: Provide the funding for security initiatives, monitor organizations compliance, and set security policies and guidelines.

Senior Management: Implements security policies and guidelines set by the Board of Directors. They ensure security initiatives align with the overall strategy, while simultaneously managing risk.

Chief Information Security Officer: Responsible for the security posture of the organization. They create policies and procedures, handle incidents, oversee the security program, and provide guidance to the senior management.

IT Management: Oversees implementation of security controls. They also monitor events, mitigates threats, and patch vulnerabilities.

Functional Area Management: A more specialized management that focuses on their respective areas. They ensure personnel are trained and can perform their duties within their responsibilities.

Information Security Personnel: Implement and maintain security controls by monitoring, managing, and reacting to security events.

End users: Responsible for following policies, procedures, and reporting incidents. They should be properly trained to better understand maintaining security.

Addressing the threats mentioned above of employee awareness, training, and timely implementation of updates are crucial when maintaining a strong security posture. Failing to address these weaknesses can result in avoidable security incidents.

Increased Risk of Security Breaches: Not providing proper training, having poor employee comprehension, and not implementing patches and updates in a timely manner can lead to increased risk of breaches.

Reduced Effectiveness of Security Controls: If employees are not knowledgeable about the security controls they are more like to use them in a reduced manner. Similarly if updates and patches are not performed the controls are likely to be used in a reduced state.

Agitated Compliance and Regulation: Failing to address employee awareness and applying updates and patches can lead to compliance and regulation issues down the road. Negligent employees can cause all types of havoc within compliance while failing to update systems can also be against regulations.

**References**

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>