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 Brief Overview:

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 for the organization to continue. 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 ledger of personnel responsible for executing the disaster recovery plan and their roles and responsibilities.
3. Risk Assessment: An assessment of potential risks and vulnerabilities to critical infrastructure such as natural disasters, cyberattacks, and other potential disruptions.
4. Backup and Recovery Strategy: Policies and procedures for backing up critical data and proprietary systems and recovering them in the event of a disaster or outage.
5. Emergency Response Plan: Polices and procedures for responding to an emergency, such as evacuating personnel, securing facilities, and mitigating damage.
6. Communication Plan: Policies and procedures to communicate effectively with all stakeholders, including employees, customers, vendors, and the public.
7. Testing and Maintenance: Policies and procedures to conduct regular testing and maintenance of the disaster recovery plan. This is to ensure its effectiveness and readiness.
8. Training and Awareness: Policies and procedures to train employees on the disaster recovery plan, emergency response procedures, and other critical components of continuity management.
9. Continuous Improvement: Policies and procedures to continuously review, critique, and improve the disaster recovery plan based on lessons learned from previous events, industry standards, and advancements in technologies.

Lockheed Martins Incident Response Plan:

1. Introduction: Overviews the plans purpose, scope, and objectives of the IRP.
2. Incident Response Team: A defined ledger 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: Defined polices and procedures for responding to an incident related to intellectual property, including containment, investigation, recovery, and reporting.
5. Evidence Collection: Polices and procedures for collecting and preserving evidence related to the incident, such as documentation, forensic analysis, and a chain of custody.
6. Legal and Regulatory Compliance: Polices and procedures for obeying legal and regulatory requirements such as data privacy laws and contract obligations.
7. Communication Plan: Polices and procedures to communicate effectively with all stakeholders, including employees, customers, vendors, and law enforcement.
8. Training and Awareness: Training for employees on the incident response plan, security policies and procedures, and other critical aspects of intellectual property protection.
9. Continuous Improvement: Polices and procedures for continuous review, critique, and improvement of the incident response plan. Based on lessons learned from previous incidents, industry standards, and advancements in technologies.

Lockheed Martins Version Control System Assured Operations Plan:

*Objective:*  The following 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 stored on GitHub and physical backups. This will lead to the assured operation of Lockheed's Version Control Systems and the proprietary intellectual property they contain.

*Protection of Organizational Intellectual Property:*

1. Access Control: Only authorized personnel should have access to the organization's codebase. This includes limiting access to the codebase by using access control on GitHub so that only designated individuals can read, write, or change access.
2. Encryption: Sensitive information should be encrypted to and from GitHub.
3. Two-Factor Authentication: Two-factor authentication should be implemented to prevent unauthorized access to the codebase such as a RSA-Token.
4. Strong Passwords: Strong passwords should be enforced to ensure that access to the codebase is only granted to authorized employees.
5. Limit Physical Access: Physical access to the organization's servers, workstations, and backups should be limited to authorized personnel.
6. Key Management: Private keys should be stored as environment variables and not directly in codebase.

*Implementation of Access Controls Including Cyber-Physical Security Controls:*

1. Firewall: A firewall should be installed and configured to protect the organization's network from unauthorized access to codebase and backups.
2. Intrusion Detection System: An intrusion detection system should be implemented to detect any irregular attempts to access the organization's codebase or network.
3. Cyber-Physical Security Controls: Physical access to the organization's codebase and physical backups should be limited and secured to prevent unauthorized access.
4. Regular Security Audits: Regular security audits should be conducted to ensure that the organization's codebase and network are secure.
5. GitHub Access Control: This includes limiting access to the codebase by using access control on GitHub so that only designated individuals can read, write, or change access.

*Patch and Change Management:*

1. Regular Updates: Regular updates are applied to Lockheed's software and systems to ensure that vulnerabilities are addressed in a timely manner.
2. Testing: Changes to Lockheed's Source Control Management procedures should be thoroughly tested before being deployed to ensure that they do not introduce vulnerabilities.
3. Version Control: Version control should be used to track changes made to the organization's codebase.
4. Backup and Recovery: Regular backups of the organization's codebase should be made and should be tested to ensure that it can be restored in the event of a disaster or system failure.

*Conclusion:* This Assured Operations Plan is designed to protect the Lockheed Martins intellectual property by implementing access controls, cuber-physical security controls, and maintaining patch and change management for the organization's codebase stored on GitHub and on physical backups. The plan ensures that Lockheed's proprietary codebase is protected from unauthorized access, vulnerabilities, and regular backups are made to ensure that the codebase can be restored in the event of a disaster.

Strategic Roles of the Organizational Stakeholders

*Board of Directors:* Ensures that adequate resources are provided to establish and maintain an effective security program and sets the policies that guide the organization's security while also overseeing the management team to ensure that security risks and assured operations are appropriately managed.

*Senior Management:* Responsible for following the board's security policies and ensuring the organization's security program aligns with business objectives. Ensures that resources are allocated to maintain an effective security program. Senior management makes crucial decisions about balancing risk vs cost to ensure the organization remains operationally secure.

*Chief Information Security Officer (CISO):* Responsible for developing and executing the organization's security and operational assurance strategy while ensuring that the security program aligns with objectives, complies with laws and regulations, and manages risk. The CISO oversees the organization's security operations and provide guidance to other stakeholders on security matters.

*IT Management (CIO, IT Director, etc.):* Responsible for managing security controls necessary for an effective security and assured operations program and ensures that security measures are consistent with the organization's security policies and standards. They oversee the day-to-day management of the organization's security and assured operations.

*Functional Area Management:* Responsible for managing the security risks within their respective areas and ensure that adequate controls are in place to protect sensitive data and systems within their jurisdiction. Functional Area Management works with IT management to implement security controls and ensure compliance with the organization's security policies and assured operation standards.

*Information Security personnel:* Responsible for the day-to-day implementation of the organization's security program and manage the technical aspects of the security program, including firewalls, intrusion detection systems, and security incident response. They work with other stakeholders to identify and mitigate security and assured operations risks.

*End users (employees, customers, sub-contractors/vendors, etc.):* Responsible for maintaining an effective security and assured operations program. They are responsible for abiding by the organization's security policies and standards, reporting security incidents, and participating in security awareness training.

Three Big Challenges When it Comes to Assured Operations and Contingency Plans:

Funding

Resource Allocation:

Communication:

*Funding: One of the biggest challenges in implementing contingency plans and System Specific assured operation plans is funding. Organizations may have limited resources to allocate towards security, and as such, it may be difficult to implement all necessary security measures.*

*Resource allocation: Even if an organization has the necessary funding to implement security measures, resource allocation can be a significant challenge. This is because there may be competing priorities for resources within the organization, and it may be challenging to allocate resources to security when other priorities seem more pressing.*

*Resistance to change: Another challenge in implementing contingency plans and System Specific assured operation plans is resistance to change. This can come from various stakeholders within the organization, including end-users, functional area management, and even senior management. Resistance to change can hinder the adoption of new security measures and can prevent organizations from achieving an assured operations environment.*

*Compliance requirements: Compliance requirements can also pose a significant challenge in implementing contingency plans and System Specific assured operation plans. Organizations must comply with various regulations, such as HIPAA, PCI, and GDPR, which can be complex and difficult to navigate. Compliance requirements may require organizations to implement specific security measures, and failure to comply can result in significant penalties.*

*Coordination and communication: Finally, coordination and communication can be a significant challenge in implementing contingency plans and System Specific assured operation plans. Effective communication between all stakeholders is critical to the success of the security program. Without effective communication, stakeholders may not be aware of the security risks and may not take the necessary steps to mitigate those risks.*

*In conclusion, organizations face significant challenges when implementing contingency plans, System Specific assured operation plans, and key strategic roles. These challenges include funding, resource allocation, resistance to change, compliance requirements, and coordination and communication. Overcoming these challenges requires a coordinated effort from all stakeholders within the organization.*

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>