ISEC 0635: Information Security Operations Management

Winter Term 2023

Eric Webb

Assignment 1: Executive Summary of Northrop Grumman's Security Operations.

Its no secret Northrop Grumman has a strong reputation for providing and innovating solutions within the aerospace and defense sectors. It is imperative for an organization like this to maintain a strong information security posture to protect sensitive data and systems from cyber threats and is needed to succeed in these highly competitive markets.

To maintain good security operations, Northrop 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 Northrop Grumman’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 Northrop Grumman 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: A responsible for following policies and 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.