ISEC 0635: Information Security Operations Management

Winter Term 2023

Eric Webb

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

The company of 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. This is needed to succeed in these highly competitive markets.

To maintain a good security operations, Northrop employs a combination of software, hardware, practices, and people. This id 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.

Performing a SWOT matrix on Northrop Grumman from a security operations perspective revealed the following:

Strengths: Has extensive security hardware and software from having a history of government contracts. Has an experienced security team from doing government contracts.

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

Opportunities:

Threats;

*strengths include its robust hardware and software security systems, and its experienced team of security professionals.*

*weaknesses were identified in the areas of employee training and awareness, potential insider threats, and the need to continually update and improve security measures to stay ahead of evolving threats.*

*Opportunities were found in the potential to expand the use of advanced technologies such as artificial intelligence and machine learning in security operations,*

*threats included the growing sophistication of cyber attacks and the need to comply with evolving regulatory requirements.*