**Key Asset and Threat Identification**

David Boardman

CJ 682

8/30/2021

Key Asset and Threat Identification

Founded by Collis Potter Huntington, the Newport News Shipbuilding Company has built ships for 135 years that have served the nation in peace and war. The company, located in Newport News City, Virginia, has a legacy for creating excellent ships for U.S. and commercial clients in design, construction, overhaul, and repair. Currently, a division of Huntington Ingalls Industries, Newport News Shipbuilding Company builds designs, builds, and refuels the nation’s nuclear-powered aircraft carriers (Military Installations, n.d.). Besides, the company is one of the country’s two shipyards with the capability to design and build nuclear-powered submarines and provide fleet services for naval ships.

**Vulnerability Identification**

**Comprehensive Profile of the Key Asset**

Newport News Shipbuilding company is a critical infrastructure for the U.S. under the Department of Defense. The company also partners with the Department of Energy and other government customers, providing them with engineering and project management services. The Newport News Shipbuilding Company's yard contains nuclear-powered aircraft carriers, Virginia-class nuclear-powered submarines, Liberty ships used during the Second World War, and Los Angeles-class nuclear-powered submarines. Moreover, the shipyard has the most dominant position in the warship construction business for America, holding more than 550 acres of land in Newport News City, Virginia (Military Installations, n.d.).

**Why the Key Asset Deserves Protection Based on the Profile of the Location**

While there have not been any terrorist attacks on Newport News Shipbuilding, the company is at risk of other forms of attack. According to Dujardin (2015), the company's design drawings and the sailors are more vulnerable to attack if enemies get wind of the schematics. Information that could be stolen includes technology infrastructure, propulsion systems for the carriers, defensive mechanisms, and storage areas for the weapons. If enemies get knowledge of any of these areas, they would be able to attack the company in terms of its operational capabilities and functions (Dujardin, 2015). As a result, unauthorized disclosure of such knowledge would give the foreign adversaries an economic and military advantage. Besides, foreign understanding of the company's ship and aircraft designs would increase their knowledge of where to strike because they would know the location of the propulsion systems and the reactors.

The company owns a lot of proprietary information and sensitive documents that are not classified but are protected by the Naval Nuclear Propulsion Information (NNPI) (Dujardin, 2015). No foreign nationals are allowed to see these documents, and only the Navy or the Newport News Shipbuilding are authorized to release the information. However, the company embraces cybersecurity and various security strategies to combat the increasing challenge of external threats and vulnerabilities. Besides, the company ensures that all personnel and organizations with access to crucial information networks and assets understand that cybersecurity is a collaborative effort (Newport News Shipbuilding, n.d.).

**Common Vulnerabilities of the Critical Infrastructure Sector**

Newport News Shipbuilding Company faces various vulnerabilities, including personnel, physical, and cyber, that could compromise its security. The company faces physical vulnerabilities such as physical equipment theft, considering that Newport News city is not very safe. However, the crime rates are unlikely to be linked with terrorist activities. The company is also prone to cyberattacks. Pomerleau (2019) explains that the company suffered a large-scale hacking campaign initiated by various organs orchestrated by the Chinese government. Besides, the company’s cyber vulnerability in its defense industrial base makes it a key target for foreign espionage. Newport News Shipbuilding Company is a target for hackers because it keeps a lot of classified and sensitive information for its products and its connection with the federal government (Pomerleau, 2019).

**Known and/or Probable Vulnerabilities of the Key Asset**

The crucial vulnerabilities of the company include cyberattacks. Large-scale hackers target the key asset aiming to access its proprietary information. Feared hacking groups from China, such as APT10, have previously connected and penetrated the key asset's servers (Pomerleau, 2019). However, the company has denied having lost any information to the hacker group. Despite the situation, the company must stay keen to ensure the safety of its sensitive documents.

**Vulnerability Assessment**

**The Impact of Terrorist Group’s Motivations, Capabilities, and Tactics**

The APT10 hacker group is engaged in global computer intrusions, stealing data from various global companies (Fire Eye, n.d.)y. The hacker group is motivated by its conspiracy to commit wire fraud, commit computer intrusions, and commit identity theft. They often target a diverse array of companies in commercial activities and the technology industry, including satellite and maritime technology, aviation, automotive supplies, healthcare, pharmaceutical manufacturing, industrial factory automation, and information technology services, among others (U.S. Department of Justice, 2018). The hacker group has extensive capabilities of hacking into private networks as they have been consistent in obtaining unauthorized access to computers belonging to multiple technology-related companies. The group uses technology and its experts to steal sensitive data belonging to the Navy and other groups.

**Key asset’s Vulnerabilities Most Likely to be Exploited by Terrorists**

Newport News Shipbuilding Company owns proprietary information on how it designs, builds, and refuels its ships and aircraft. Therefore, this area has the highest threat from terrorists or any other group that might want to attack the group. This is because access to the company's proprietary information would give the attackers the power to mount attacks on the U.S. entities using equipment manufactured by the company.

**Current Vulnerability Level of the Key Asset**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **THREAT FACTORS** | | | | | | **Threat Level**  **(1–10)** | **Motivation**  P = Political  R = Religious  E = Environmental  Ra = Racial  S = Special Interest  **(Choose one or more)** | **WMD Categories**  C = Chemical  B = Biological  R = Radiological  N = Nuclear  E = Explosive  **(Choose one or more)** |
| **PTE** | **Existence**  **(1)** | **Violent History**  **(1)** | **Intentions**  **(2)** | **WMD Capability**  **(2)** | **Targeting**  **(3)** |
| 1 | 1 | 0 | 1 | 0 | 4 | 2 | P and S | None |

Newport News Shipbuilding's threat level is low because there have not been previous terrorist attacks on the company. However, the company may face cyber attacks because it is a target for its proprietary information. Hackers would want to get hold of its technological information to plan attacks. Therefore, the organization needs to mount proper cybersecurity plans to prevent such occurrences in the future.

References

Dujardin, P. (2015, 06 21). *Espionage case: Spy's schemes could have made the Navy's newest aircraft carrier more vulnerable*. Retrieved 08 30, 2021, from Daily Press: https://www.dailypress.com/news/newport-news/dp-nws-ford-carrier-espionage-20150620-story.html

Fire Eye. (n.d.). *Advanced Persistent Threat Groups*. Retrieved 08 30, 2021, from Fire Eye: https://www.fireeye.com/current-threats/apt-groups.html

Military Installations. (n.d.). *Newport News Shipyard In-depth Overview*. Retrieved 08 30, 2021, from Military Installations: https://installations.militaryonesource.mil/in-depth-overview/newport-news-shipyard

Newport News Shipbuilding. (n.d.). *Cybersecurity*. Retrieved 08 30, 2021, from Newport News Shipbuilding: https://supplier.huntingtoningalls.com/sourcing/cybersecurity/

Pomerleau, M. (2019, 06 27). *Hackers are repeatedly targeting Navy contractors*. Retrieved 08 30, 2021, from Fifth Domain: https://www.fifthdomain.com/industry/2019/06/27/hackers-are-repeatedly-targeting-navy-contractors/

U.S. Department of Justice. (2018, 12 20). *Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information*. Retrieved 08 30, 2021, from U.S. Department of Justice: https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion