Sprint 2 Summary:
Threat & Vulnerability Assessment

Authors: Elizabeth Bond and Jane Pierre

Contributors: Frederick Asante, Shemar Brown, Tianna Green, Jonathan Henao, Lucas Higgs, Aaron Kaah and Mishelly Sandoval

Cyber Security & Networking

The Knowledge House

Instructor: George Robbins

April 30, 2023

Cybersecurity and networking are critical areas of concern for non-profit organizations due to the various security risks they face. These risks can negatively impact their operations, reputation, and ability to fulfill their missions. A comprehensive security program for non-profit organizations should include threat, vulnerability, and risk assessments. There are several reasons why non-profit organizations need these assessments. First, threat assessments can help identify potential security threats, such as cyberattacks, theft, or vandalism, and develop strategies to mitigate those risks (Meloy & Yakeley, 2019). Second, vulnerability assessments can identify weaknesses in physical security, network security, and operational security, and develop strategies to address those vulnerabilities (Meadows, 2020). Additionally, risk assessments can help prioritize security resources by identifying the most significant risks and developing strategies to mitigate those risks (ISO, 2018). Lastly, non-profit organizations may be subject to various regulations, such as data privacy or safety standards, that require them to conduct regular risk assessments and implement appropriate security measures (American Bar Association, 2018).

The scope of this paper is to discuss the threat and vulnerability assessments as a critical part of a cybersecurity program for the client, The Knowledge House (herein known as TKH), a non-profit educational organization. Before building a cybersecurity program for TKH, it is crucial to assess the company's current cybersecurity posture, business needs, and potential risks. This summary defines threat, vulnerability and risk and explains their associated assessments and their components. This summary also discusses our group’s approach to conducting a threat and vulnerability assessment with TKH, what steps were carried out as well as a discussion of the tools used. At the time of publishing and submission of Sprint 2 for this Capstone project, a statement of scope had been given to TKH’s leadership for review and the group is still finalizing with TKH leadership, information and permission for an in-person visit to the organization’s headquarters in Bronx, New York. As a result, this summary will only focus on the aforementioned as well as, discuss the seven steps to completing a threat, vulnerability and risk assessment, explain the tools that were used in an independent preliminary

investigation of TKH, and explain the assessment tools that would be used during the in-person visit.

In cybersecurity, a threat refers to a potential danger or harm that could compromise the security of an organization's assets. A threat can be intentional or unintentional, and it can come from a variety of sources, including hackers, insiders, and natural disasters. Threats can take many forms, such as malware, phishing attacks, denial-of-service attacks, and physical theft or destruction of equipment. Therefore, organizations need to be able to identify potential threats to their systems and take measures to protect themselves against them (Meadows, 2020).

Vulnerability refers to a weakness or flaw in a system, process, or technology that could be exploited by a threat actor to gain unauthorized access or cause harm. In the context of cybersecurity, vulnerabilities can be found in various areas, such as software, hardware, network configuration, and user behavior. For example, outdated software with unpatched security vulnerabilities is a common target for attackers. Similarly, weak passwords or unsecured network connections can make an organization more vulnerable to cyberattacks. Therefore, organizations need to conduct regular vulnerability assessments to identify and address security weaknesses before they can be exploited (Meadows, 2020).

Risk refers to the likelihood and potential impact of harm resulting from a threat exploiting a vulnerability. In cybersecurity, risk assessment is the process of evaluating potential risks to determine their likelihood and potential impact. Risk assessments can help organizations identify and prioritize security risks based on the likelihood and potential impact of harm. For example, a high-risk vulnerability, such as an unpatched system with known exploits, would require immediate attention and remediation. Risk assessments are essential in developing effective security measures to protect against potential threats and vulnerabilities, as well as in the allocation of resources to mitigate identified risks (ISO, 2018).

Threat, vulnerability, and risk assessments are essential components of a comprehensive cybersecurity program. While they share some similarities, they differ in their focus and scope. Threat assessment focuses on identifying potential attackers or malicious actors, evaluating the likelihood and potential impact of harm from specific threats, and developing strategies to mitigate those risks. Vulnerability assessment focuses on identifying weaknesses in an organization's infrastructure, systems, and operations, evaluating the likelihood and potential impact of harm resulting from those vulnerabilities, and developing strategies to address those vulnerabilities. Risk assessment focuses on identifying potential risks to people, property, or the environment, evaluating the likelihood and potential impact of harm resulting from those risks, and analyzing hazards, vulnerabilities, and existing risk mitigation measures.

A comprehensive threat and vulnerability/risk assessment typically involves seven key parts or steps that are essential for identifying, evaluating, and mitigating potential security risks. The following are the seven parts/steps of a threat and vulnerability/risk assessment:

1. Define the scope: Establish the scope of the assessment by defining the assets to be protected, the threats to those assets, and the potential impact of those threats (ISO, 2018).
2. Identify potential threats: Identify potential threats to the organization, such as natural disasters, cyberattacks, theft, or vandalism (Meloy & Yakeley, 2019).
3. Assess vulnerabilities: Evaluate the organization's vulnerabilities, including physical security, network security, and operational security, to determine the likelihood and potential impact of harm resulting from those vulnerabilities (Meadows, 2020).
4. Analyze risks: Analyze the risks posed by identified threats and vulnerabilities, considering the likelihood and potential impact of harm (ISO, 2018).
5. Prioritize risks: Prioritize the identified risks based on their potential impact and likelihood of occurrence, and develop strategies to mitigate the most significant risks (Meloy & Yakeley, 2019).

6. Develop a risk management plan: Develop a risk management plan that includes strategies to address identified risks, such as implementing security measures or transferring risk through insurance (ISO, 2018).
7. Monitor and update: Regularly monitor the effectiveness of the risk management plan and update it as necessary based on changes in the organization's operations, infrastructure, or risk landscape (Meadows, 2020).

The use of threat, vulnerability, and risk assessments aligns with the guidelines set forth in NIST 800-171. Specifically, Section 3.12.4 of the standard requires that contractors "periodically assesses risk to the confidentiality, integrity, and availability of CUI [Controlled Unclassified Information] on the contractor's unclassified information system and implementing security controls to mitigate such risks." This requires contractors to conduct regular risk assessments, which include identifying potential threats, assessing vulnerabilities, and developing strategies to mitigate those risks. By aligning with NIST 800-171, organizations can ensure that they are following industry best practices and complying with relevant regulations and standards. Threat, vulnerability, and risk assessments play a critical role in the development and implementation of effective cybersecurity programs, align with relevant regulations and standards, and help organizations meet their overall cybersecurity goals.

To assess the current cybersecurity program in place, several tools can be used, such as vulnerability scanners, network mapping tools, and traffic analyzers. Nmap, OpenVAS, Metasploit, Burp Suite and Wireshark are examples of such tools (Lyon, 2019).

Nmap is a network exploration and mapping tool that can discover hosts and services on a network. It helps identify open ports, running services, and operating systems. Nmap also detects vulnerabilities in the network and checks for potential attack vectors (Nmap, n.d.).

OpenVAS is a vulnerability scanner that scans a network for known vulnerabilities in the system, services, and applications. OpenVAS provides an extensive database of known vulnerabilities and helps prioritize which vulnerabilities need to be addressed first (Greenbone Networks GmbH, 2021).

Metasploit is a penetration testing tool that helps identify vulnerabilities in a network and exploit them to gain access. It is an open-source framework that provides a comprehensive suite of tools to test the security posture of an organization (Rapid7, 2021).

Burp Suite is a popular web application security testing tool that is widely used in the cybersecurity industry. It is a software suite that consists of several tools, including a proxy server, scanner, and various tools for intercepting and modifying HTTP/S traffic. Burp Suite can be used to identify vulnerabilities in web applications, such as SQL injection, cross-site scripting (XSS), and other common attack vectors (PortSwigger, n.d.). In a threat, vulnerability, and risk assessment, Burp Suite can be used to simulate attacks on web applications to identify potential vulnerabilities and weaknesses in their security posture.

Wireshark is a traffic analyzer that captures and analyzes network traffic in real-time. It helps identify any malicious activity or traffic anomalies and can be used to identify the root cause of any security incidents (Wireshark Foundation, 2021).

To prevent and mitigate potential security threats, strong authentication and access control mechanisms should be implemented to limit unauthorized access to sensitive systems and data. Firewalls and intrusion detection systems should also be in place to monitor and block suspicious network traffic. Regular system updates and patching can help protect against known vulnerabilities, and robust backup and disaster recovery plans can help mitigate the impact of successful attacks. Finally, ongoing employee training and awareness initiatives can help promote a culture of cybersecurity, reducing the risk of insider threats and human error (Mehmood et al., 2021).

Our group conducted a preliminary assessment of TKH by utilizing websites such as Virustotal.com, Shodan.io and other cybersecurity websites in order to find additional information such as IP addresses the organization is using as well as whether they have shown up in any nefarious reports of suspicious activity online Virustotal. (n.d.). At the time of publishing this summary, our results showed that no security vendors had listed TKH's multiple IP addresses as malicious (Shodan, n.d.) However, we could not affirm that their SSL certificates were valid (Shodan, n.d.). As mentioned earlier, a statement of scope was written and submitted to TKH that explained the boundaries and limitations of our assessment. Also, an email asking the IT Technician questions regarding TKH's data security has also been sent and awaits a response.
Once we are given access to complete a full threat, vulnerability and risk assessment, we would provide a report of our findings and explain how we will incorporate the information and data collected into the development and implementation of a secure program for The Knowledge House.

In conclusion, cybersecurity and networking are critical aspects of any organization's operations, especially for non-profit organizations. The implementation of a comprehensive security program that includes threat, vulnerability, and risk assessments is necessary to identify potential threats, assess vulnerabilities, and develop effective mitigation strategies. The seven steps of a comprehensive assessment, which includes defining the scope, identifying potential threats, assessing vulnerabilities, analyzing risks, prioritizing risks, developing a risk management plan, and regularly monitoring and updating it, can be used to conduct thorough assessments. Aligning with regulations and standards, such as NIST 800-171, can ensure that organizations meet industry best practices and comply with relevant regulations. Additionally, the use of tools such as Nmap, OpenVAS, Metasploit, and Wireshark can aid in assessing and mitigating potential threats. The implementation of strong authentication and access control mechanisms, firewalls and intrusion detection systems, regular system updates and patching, and ongoing employee training and awareness initiatives are also critical in preventing and mitigating potential security

threats. Through an in-depth assessment and implementation of effective security measures, as well as regular monitoring and updating of their secure programs, non-profit organizations like The Knowledge House can protect their operations, reputation, and ability to fulfill their missions while demonstrating their commitment to protecting private data and assets against evolving threats.

References:

American Bar Association. (2018). Nonprofit organizations and data protection: Why risk assessments are critical. https://www.americanbar.org/groups/business_law/publications/blt/2018/07/nonprofit-organizations-and-data-protection-why-risk-assessments-are-critical/

PortSwigger Ltd. (n.d.). Burp Suite. Retrieved April 30, 2023, from https://portswigger.net/burp

ISO. (2018). ISO 31000:2018 Risk management - Guidelines. International Organization for Standardization. https://www.iso.org/standard/65694.html

Meloy, J. R., & Yakeley, J. (2019). Threat Assessment: Contemporary Practice and Emerging Issues. Journal of Threat Assessment and Management, 6(1), 1-12. https://doi.org/10.1037/tam0000119

Meadows, R. (2020). Vulnerability Assessment. In A. Staniforth (Ed.), Cyber Security (pp. 431-435). Springer. https://doi.org/10.1007/978-3-030-19957-0_85

National Institute of Standards and Technology. (2015). Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. Special Publication 800-171. https://doi.org/10.6028/NIST.SP.800-171

Shodan. (n.d.). Shodan. Retrieved April 30, 2023, from https://www.shodan.io/

Virustotal. (n.d.). VirusTotal - Free Online Virus, Malware and URL Scanner. Retrieved April 30, 2023, from https://www.virustotal.com/