Sprint 1 Summary: Cybersecurity Framework

Cyber Security & Networking, The Knowledge House Fellowship
Instructor: George Robbins

In today's digital age, cybersecurity threats are becoming more prevalent, and organizations need to take necessary measures to ensure the protection of sensitive information. One effective way of achieving this is through the implementation of a cybersecurity framework. A cybersecurity framework refers to a set of policies, procedures, and standards that organizations can use to manage cybersecurity risk (Cybersecurity Framework," n.d.). It outlines the best practices for securing sensitive data and minimizing cyber attacks. For non-profit organizations, cybersecurity is particularly important as they often handle sensitive data from donors and clients, including financial information and personal identifiable information (PII) as well as employee, program, service and organization data ("Why Cybersecurity Matters for Nonprofits," n.d.). Nonprofits are also vulnerable to cyber threats due to their limited resources and lack of awareness of cybersecurity risks.

A cybersecurity framework serves as a guide for business and organizational entities such as nonprofits to develop a robust cybersecurity program that addresses the specific risks they face. One such framework is the National Institute of Standards and Technology (NIST) 800-171, which provides guidelines for protecting controlled unclassified information (CUI) (National Institute of Standards and Technology, 2018). The framework outlines a set of security controls that organizations can use to secure CUI and mitigate cybersecurity risks (National Institute of Standards and Technology, 2018). Non-profit organizations can use the NIST 800-171 framework to implement effective cybersecurity controls that align with their mission, goals, and objectives (NIST, 2018).

The NIST Cybersecurity Framework provides a flexible and adaptable framework for managing cybersecurity risks. The framework is divided into five core functions: Identify, Protect, Detect, Respond, and Recover. The guidelines for NIST 800-171 are organized into 14 categories of security requirements (NIST, 2018). They each contain a set of specific controls which will be utilized in the development of a secure program for our Non-Profit Organization client. Below is the list of controls and their functions:

1. Access Control: This category includes controls that limit access to information systems, applications, and data to authorized personnel only (NIST, 2018). This includes requirements such as implementing multi-factor authentication, enforcing password policies, and maintaining an access control list (NIST, 2018).
2. Awareness and Training: This category includes controls that ensure personnel are trained and aware of their security responsibilities (NIST, 2018). This includes requirements such as providing security awareness training, reminding users to be vigilant when handling sensitive information, and conducting periodic security refresher training (NIST, 2018).
3. Audit and Accountability: This category includes controls that ensure that security-related events are logged, monitored, and analyzed (NIST, 2018). This includes requirements

such as maintaining an audit trail, performing regular audits of information systems and data, and analyzing security-related data to identify potential security incidents (NIST, 2018).

4. Configuration Management: This category includes controls that ensure that information systems are configured and managed to protect against security threats (NIST, 2018). This includes requirements such as implementing configuration baselines, managing system changes, and maintaining an up-to-date inventory of hardware and software (NIST, 2018).
5. Identification and Authentication: This category includes controls that ensure that individuals are properly identified and authenticated before accessing information systems, applications, or data (NIST, 2018). This includes requirements such as implementing multi-factor authentication, enforcing password policies, and monitoring and managing user accounts (NIST, 2018).
6. Incident Response: This category includes controls that ensure that security incidents are detected, reported, and responded to in a timely and effective manner (NIST, 2018). This includes requirements such as maintaining an incident response plan, conducting periodic exercises and drills, and implementing incident reporting procedures (NIST, 2018).
7. Maintenance: This category includes controls that ensure that information systems are maintained and updated to protect against security threats (NIST, 2018). This includes requirements such as maintaining up-to-date patches and security updates, monitoring system health, and ensuring the availability and integrity of system backups (NIST, 2018).
8. Media Protection: This category includes controls that ensure that information stored on physical media is protected against unauthorized access, theft, or damage (NIST, 2018). This includes requirements such as encrypting sensitive data, securely disposing of media when no longer needed, and ensuring the physical security of media storage facilities (NIST, 2018).
9. Personnel Security: This category includes controls that ensure that personnel are trustworthy and have appropriate security clearances and access levels (NIST, 2018). This includes requirements such as conducting background checks, implementing a security awareness program, and monitoring personnel for security violations (NIST, 2018).
10. Physical Protection: This category includes controls that ensure that physical assets such as equipment and facilities are protected against unauthorized access, theft, or damage (NIST, 2018). This includes requirements such as implementing access controls, maintaining secure facilities, and monitoring physical access to sensitive areas (NIST, 2018).
11. Risk Assessment: This category includes controls that ensure that security risks are identified and assessed, and that appropriate mitigation strategies are implemented (NIST, 2018). This includes requirements such as conducting regular risk assessments, developing a risk management plan, and implementing controls to mitigate identified risks (NIST, 2018).

12. Security Assessment: This category includes controls that ensure that information systems and applications are periodically assessed to identify potential vulnerabilities and weaknesses (NIST, 2018). This includes requirements such as conducting periodic security assessments, testing information systems for vulnerabilities, and implementing remediation plans to address identified weaknesses (NIST, 2018).
13. System and Communications Protection: This category includes controls that ensure that information systems and communications networks are protected against unauthorized access, theft, or damage (NIST, 2018). This includes requirements such as implementing firewalls and intrusion detection systems, encrypting data in transit, and securing wireless networks (NIST, 2018).
14. System and Information Integrity: This category includes controls that ensure that information systems and applications are protected against unauthorized access, modification, or destruction (NIST, 2018). This includes requirements such as implementing anti-virus software, monitoring system activity, and implementing system backups and recovery procedures (NIST, 2018).

NIST 800-171 will be the main cybersecurity framework utilized to design and implement the secure program for our client for several reasons. First, NIST 800-171 is a widely recognized and respected cybersecurity framework that provides a comprehensive approach to managing cybersecurity risk. According to Cybersecurity Ventures, a leading cybersecurity research firm, NIST 800-171 is one of the top cybersecurity frameworks used by organizations worldwide (Morgan, 2018). Second, it's a flexible framework that can be tailored to the unique needs and risk profile of each organization. This makes it a good fit for growing non-profit organizations that may have limited resources and varying levels of cybersecurity expertise. As explained by its developers, NIST 800-171 is "scalable, repeatable, and manageable" (NIST, 2015, p. 3).

Additionally, it also has a built-in component to protect our client's is designed to protect Controlled Unclassified Information (CUI), which is the type of information that non-profit organizations (such as our client) are likely to handle. This includes sensitive data from donors and clients, including financial information and personal identifiable information (PII) as well as employee, program, service, and organizational data (NIST, 2015). Moreover, remaining in compliance with NIST 800-171 can help non-profit organizations meet legal and regulatory requirements related to cybersecurity. Additionally, implementing NIST 800-171 can help non-profit organizations build trust with donors, clients, and stakeholders by demonstrating their commitment to protecting sensitive information. According to a survey by the Better Business Bureau, 84% of donors say that they are more likely to support a non-profit organization that has strong cybersecurity practices in place (Better Business Bureau, 2019).

In conclusion, non-profit organizations face unique cybersecurity challenges due to their limited resources and handling of sensitive information. Implementing a cybersecurity framework such as the NIST 800-171 provides a structured approach to identifying and managing cybersecurity risks, and helps to build trust with stakeholders. By prioritizing cybersecurity, non-profit organizations can protect sensitive data, maintain their reputation, and continue to make a positive impact in their communities.

References:

Better Business Bureau. (2019). Donors value cybersecurity practices. Retrieved from https://www.bbb.org/globalassets/local-bbbs/bbb-nw-fl/bbb-cybersecurity-report-final.pdf

Cybersecurity Framework. (n.d.). National Cybersecurity Center of Excellence. Retrieved from https://www.nccoe.nist.gov/projects/building-blocks/cybersecurity-framework

National Institute of Standards and Technology. (2018). NIST special publication 800-171: Protecting controlled unclassified information in nonfederal systems and organizations. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

National Institute of Standards and Technology. (2015). Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity, version 1.1. Retrieved from https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11-final

Morgan, S. (2018). Top 5 cybersecurity frameworks and why they matter. Forbes. Retrieved from https://www.forbes.com/sites/forbestechcouncil/2018/06/25/top-5-cybersecurity-frameworks-and-why-they-matter/?sh=6c5eeba766fb

Rouse, M. (2021). Cybersecurity framework. TechTarget. https://searchsecurity.techtarget.com/definition/cybersecurity-framework

Why cybersecurity matters for nonprofits. (n.d.). TechSoup. Retrieved from https://www.techsoup.org/support/articles-and-how-tos/why-cybersecurity-matters-for-nonprofits