1 Executive Summary

This report presents findings and recommendations from the comprehensive cybersecurity assessment conducted for NARO, Inc., a fictional nonprofit organization used to examine the state of cybersecurity measures that apply across industries. The focus of the assessment was to examine the cybersecurity posture currently in place within the organization, to identify potential weaknesses in that posture, and provide actionable recommendations on how it can improve its security structure. This applies to the modern-day digital world where it is envisaged that there is a range of cyber threats which could compromise sensitive information and hamper operations. Good cybersecurity practices are therefore called for in view of protection against any potential attacks.

The assessment utilized the NIST Cybersecurity Framework as an overarching guide and organized methodology for managing cybersecurity risk, organized around five core functions: Identification, Protection, Detection, Response, and Recovery. Using the framework was intended to provide the assessment team with additional insight into the cybersecurity landscape at NARO, Inc., coupled with recommendations tailored to the needs of that organization.

Key Findings:

The audit had exposed some of the critical vulnerabilities within the cybersecurity framework of NARO, Inc.-all carrying huge factors of risk to operational integrity and security of organizational data.

1. Lack of Inventory of All Critical Assets and IT Systems: The organization is not keeping an updated inventory of all critical assets and IT systems in the organization. This presents a gap that limits the full ability to manage the resources of NARO comprehensively and protect important information. Such an updated inventory will be important in recognizing potential risks and ensuring that protective measures are in place for all essential components.

2. Poor Control Access: The current practices of user account management cannot effectively provide restricted access to the particular position and role of each account user. When proper access control is not in place, even unauthorized users may gain access to critical systems, which again increases the chances of information leaks or any other kind of security incident.

3. Poor Employee Training in Cybersecurity: The review identified poor training on cybersecurity awareness. Employees are not well-trained to detect the potential for an attack and take action; thus, the organization may fall into the trap of security breaches caused by human error. Regular training is a critical factor that will help increase vigilance in cybersecurity.

4. Poor Oversight of Third Party Vendors: Inadequate monitoring by the company of third-party vendors that could pose significant cybersecurity risks to the organization. Because NARO relies on other external associates, significant security assessments need to be conducted on these associates to make certain they are consistent with NARO's standards.

5. Poor Incident Response Planning: Lack of a formal incident response plan where NARO should be readied on the proper management of cybersecurity incidents. Without proper documentation and testing of response procedures, it will lead to slower response times once an incident occurs, and that would have given greater damage to an organization.

Recommendations:

The assessment brings a number of active recommendations to address these vulnerabilities in order to improve the cybersecurity posture of NARO, Inc. by the following: Establishment and Maintenance of Asset Inventory: The organization needs to formulate an inventory of all critical assets and IT systems. It has to be updated continuously to reflect the changing technologies and operations. Clearly specifying what is to be protected will enable NARO to better prioritize cybersecurity efforts.

1. Apply Robust User Access Management Policies: The organization should establish and enforce a policy that restricts user access to systems based on the role of the individual and his responsibility. Each employee shall have only one account for logging into sensitive systems, and reviews of user access privileges shall be done periodically to prevent over-privileged accounts.

2. Improving cybersecurity training programs within the workplace: Program staff with comprehensive cybersecurity awareness. The training should cover basic concepts such as data handling best practices, how to avoid phishing, and password management. In this way, the employees will be more capable of recognizing the threats and taking proper action to prevent them. Therefore, NARO will result in much-reduced vulnerability to cyber events.

3. Perform Regular Third-Party Risk Assessments: It should be established with a due process in place, whereby NARO reviews the cybersecurity practices of third-party vendors to ensure the adherence of such third-party vendors to the NARO security standard, which includes security agreements. These regular assessments would lessen the associated risks of the partnerships from outside.

4. Formalize and test incident response procedures: That is, develop an incident response plan providing an outline of actions an organization should perform once a cybersecurity incident has taken place. It needs to spell out specific roles, responsibilities for team members, communication protocols, and any steps required to minimize damage. The incident response plan should be tested on a regular basis and updated so it really works and the employees are prepared for such cases.

The cybersecurity assessment for NARO, Inc. should act to bring a sense of urgency in operationalizing security improvements against an ever-evolving cyber threat landscape. From this report, NARO will implement the recommendations outlined herein to further develop its cybersecurity defenses, protect its critical operations, and, by all means, mitigate risks effectively. This proactive approach ensures that the stakeholders, clients, and partners will continue to have increased confidence in the organization's commitment to cybersecurity.

Contents

2 Introduction

In this fast-evolving digital world, organizations of every sector are using more and more technology in many ways to strengthen efficiency, unleash innovation, and deliver higher service levels. This, within the framework of digital transformation, can provide big opportunities but equally has a complex array of cybersecurity risks. Cyber threats loom large, growing in sophistication and pervasiveness, targeting organizations of all sizes and industries. Because the possibility of severe disruptions and major financial losses has never been greater-from data breaches and ransomware attacks to insider threats and phishing scams-the implementation of cybersecurity measures is very important to keep sensitive data safe and ensure operational integrity.

This report reviews the findings and recommendations from a comprehensive cybersecurity assessment conducted for NARO, Inc., a fictional nonprofit organization considered to review cybersecurity practices fitting many different sectors. The primary intent of the assessment has been to deeply analyze the current state of cybersecurity posture in the organization, recognize vulnerabilities that could pose a threat to it, and make suggestions with actionable steps on how to improve its security framework. Given that the stakes of cybersecurity failures can be very serious, including large reputational damages, legal liabilities, and stakeholder trust erosion, one can hardly overestimate the need for proactive cybersecurity behavior.

Background of the Organization

NARO, Inc. represents this diverse array of organizations operating in the non-profit sector, characterized by mission-driven objectives and a commitment to serving the community. Many nonprofit organizations have sensitive information that might include donor lists, client information, and financial records. This makes them very attractive targets for cybercrime. As these organizations continue their growth in utilizing digital platforms and online interactions for furthering their respective missions, so, too, grow the risks associated with cyber threats.

The organization is further made technology-dependent by the fact that it interfaces with various stakeholders, namely donors, beneficiaries, volunteers, and regulatory agencies. Each one of these interfaces consists of sensitive information that, in case there is a breach in the security, it not only puts the data at risk but jeopardizes the very trust and confidence that the stakeholders have placed in the organization. Moreover, since nonprofits are usually funded through grants and donations, a cyber incident could affect the organization in carrying out its mission.

In this light, a robust cybersecurity framework becomes highly relevant to ensure operational integrity and protect the organization's mission. Cyber incidents disrupt operations, result in heavy financial losses, and cause reputational damage, which is often hard to repair. To this effect, NARO should give the highest priority to securing its assets and operations and, above all, sensitive information.

Objectives of the Assessment

A few key objectives underpinned the cybersecurity assessment. These guided the evaluation process and, importantly, structured the assessment in analyzing the organization's security measures on the basis of priority identification for critical assets. Basically, this involves determining what assets are fundamentally key to the operation of an organization in order to prioritize cybersecurity efforts, including data and information systems that support the organization's mission and processes, as well as people.

1. **User Access Control Assessment**: Access control is at the center of cybersecurity. The assessment examined how user access is granted, reviewed, and, where necessary, revoked to ensure that only persons with authorization come into contact with sensitive information.

2. **Testing Data Protection:** All organizations' cybersecurity strategies revolve around safeguarding sensitive data. This aspect entailed evaluating the current encryption of data, whether in transit or at rest, good data handling practices, and detection by an organization of any security incident and its response.

3. **Incident Response Readiness:** In this regard, responding appropriately to cybersecurity incidents, in order to minimize damage and ensure speedy recovery, becomes crucial. This review investigated the availability and efficiency of the incident response plan, including roles, responsibilities, communication protocols, and procedures for managing incidents developed by NARO.

4. **Third-Party Risk Management:** The organization increasingly depends on third-party vendors for different services. These can introduce new risks. The study researched how NARO managed the cybersecurity practices of its external partners to ensure alignment with organizational standards and did not compromise its security.

5. **Regulatory Compliance:** Undoubtedly, it is one of the important arms of cybersecurity, which will imply adherence to relevant regulations and industry standards. This assessment tested whether NARO followed the requisite laws and regulations, and whether its practices answered to set requirements.

By applying the structured methodology informed by the NIST Cybersecurity Framework, this assessment has aimed to provide an in-depth understanding of the cybersecurity landscape at NARO, Inc. The risk-based approach is central to the NIST framework because the priorities for cybersecurity are selected based on the set of threats that an organization confronts.

Importance of Cybersecurity Assessment

A cybersecurity assessment is not merely compliance but essential for the organization's resilience. Organizations today have to keep their finger continuously on the pulse of their cybersecurity posture against the emerging dimensions of threats. Cybersecurity assessments

provide insights into vulnerabilities, adequacy of controls in place, and improvements that need to be made to achieve substantial risk reduction.

Generally speaking, cybersecurity assessment means the thorough methodical investigation of organizational measures, policies, and procedures against security. This activity enables organizations to recognize organization weaknesses that can be utilized by cyber adversaries and let them understand the potential impact of the security breach on their operations. By taking proactive measures on these vulnerabilities, an organization can reduce general security risks and improve its posture before actual incidents occur.

Also, a proactive approach towards cybersecurity reinforces the organization's reputation, ensures the confidence of its stakeholders, and inculcates a security awareness culture among its employees. By paying extra attention to cybersecurity, NARO will be certain of maintaining itself as a trusted keeper of sensitive information for the protection of the interests of its stakeholders and in furtherance of its mission.

Structure of the Report

This report is organized around several key sections to provide clarity regarding the assessment process and the outcomes from the assessment. Immediately after this introduction is the Executive Summary, summarizing major findings and recommendations derived from the assessment. This will be followed by sections covering the assessment methodology utilized; activities conducted during the assessment; results of findings; and finally, conclusions and suggested follow up activities.

The sections are designed to build a comprehensive picture of NARO, Inc.'s cybersecurity posture and outline a clear path forward for enhancing its defenses. By this assessment, we seek not only to strengthen the security measures at NARO, Inc. but also to instill in its staff a culture of awareness about cybersecurity. This will help the organization be more proactive in the identification and resolution of threats that may arise, building resilience against an evolving cyber landscape by promoting engagement in cybersecurity practices.

It thus marks a necessary milestone for assurance that NARO, Inc. is appropriately poised to address the cybersecurity challenges of an increasingly digital world. If adopted, it fosters a proactive mindset toward security that helps protect the mission and retain stakeholder confidence as the organization navigates the depths of the modern threat landscape.

3 System Overview

NARO, Inc.'s infrastructure involves a blend of physical facilities, technological resources, and support services to enable research and development into electric vehicle charging systems. The organization is structured around two primary buildings: administrative and engineering. This division facilitates daily operations, different functions of the organization, and specialized work. Critical digital resources include laptops, centralized servers, a structured wireless network, and VPN-enabled remote access. Additionally, NARO contracts with a local IT service provider to resolve technical challenges and maintain system updates. This system overview outlines the interconnections amongst these systems and facilities, highlighting their roles in sustaining operational efficiency.

Physical Infrastructure

NARO, Inc. leases two office spaces designed to support both the administrative and engineering functionalities of the business. These buildings serve as the primary location for organizational activities, equipped with the necessary infrastructure to facilitate daily tasks. The administrative side occupies the first floor of a two-story building, which it shares with Geological Analysis and Surveying (GAS). The office space is enclosed and secured by a door, where NARO administrative staff can work on grant writing, financial management, and sales. The administrative building also contains custodial, storage, and kitchen facilities, as well as the server room—all of which are common areas shared between NARO and GAS.

The engineering group operates in a stand-alone building conveniently located across the parking lot from the administrative office. This facility is designed to support various engineering activities and research, featuring an office space for engineers, a specialized lab for equipment testing, a secure hazmat storage area for hazardous material, and vehicle bays that house designated workstations. The workstations are exclusively utilized in place of laptops due to the necessity for interfacing with electric vehicles to collect charging data.

To ensure the security of its facilities, NARO implements various access control systems to secure areas, monitor access, and enable entry. Both NARO office locations are secured with proximity cards and magnetic locks; however, the administrative office is typically left unlocked during business hours to accommodate visitors. It is noted that visitors are given a red visitor badge. The exterior doors of the administrative building also remain unlocked. In contrast, the engineering building keeps tight security by employing keypad locks on personnel doors, while the overhead doors in the vehicle bay are secured with padlocks. Visitors in the engineering space are escorted due to safety reasons.

IT Infrastructure

Laptops

NARO, Inc.'s IT system is designed to support flexible working arrangements and collaboration among employees. NARO equips every employee with a Windows laptop, preconfigured with essential software applications, including NordVPN, Office 365, and Zoom. For cybersecurity, the laptops feature Microsoft Defender for anti-virus and firewall protections, along with BitLocker encryption to safeguard data through password protections. Employees are permitted to install additional software on their laptops, including non-work related applications, such as TikTok. Laptops provide access to the NARO file server, enabling employees access to shared files and documents. Within the office, each cubicle is outfitted with a docking station that provides connectivity to power, monitors, Ethernet, and other peripherals, creating a desktop-like environment.

For remote work, laptops can be taken home by employees. All systems are configured with TeamViewer, enabling remote monitoring capabilities on laptops, including the option to remotely delete any sensitive information from the devices if necessary. All laptops and workstations are set to update automatically, ensuring that all software and security patches are current. Additionally, a consultant visits NARO every two months to perform updates on any systems and software that require attention and to address specific failures if they arise. NARO does note that they do not keep an inventory on software installed on devices.

All employees have unique accounts on the NARO Windows Domain, granting access to various services, including email. Passwords for these accounts are updated annually and comply with NIST guidelines, requiring a minimum of eight characters and a combination of different character types.

Two areas of NARO operate on different systems. The engineering lab is not integrated into the Windows Domain, instead using local accounts for access. The lab contains a combination of Windows and Linux systems and research data is securely transferred to NARO servers using protocols such as SSH, SCP, or rsync. Additionally, the hazmat engineer operates the only MAC system within NARO, which connects to the Windows Domain via the wireless network. All systems within the organization are integrated into the NARO wireless network, ensuring connectivity across facilities.

Servers

NARO, Inc. operates a central server infrastructure housed within the administrative building's server room. The server room is shared between NARO and GAS, with two desks equipped with workstations connected to a network KVM, enabling each direct access to their respective servers. NARO's infrastructure is connected to its own network, while GAS operates on a separate network. There are multiple server racks with sufficient power and cooling to support them. The server racks contain essential networking equipment, including an AT&T provided gateway, a Juniper SRX firewall, and a Netgear ProSafe JGS524 Gigabit switch, which facilitate both internet connectivity and secure access to the NARO network.

NARO's server infrastructure consists of 17 servers to meet its operational needs:

- Twelve (12) are Supermicro 2U Mainstream A+ SuperServer (AS-2024S-TR)
    - Utilized for research and development data
    - Running Ubuntu 18.04.6 LTS (Long-Term Support)
- Five (5) are Dell PowerEdge R940 Rack Servers
    - Utilized for the Windows Domain
    - Running Windows Server 2019

Backup hard drives are stored in the server room for on-site purposes. Prompt IT Assistance (PITA)—a local IT provider that NARO contracts with—also has developed a script that runs on NARO, Inc. systems to facilitate weekly backups to PITA servers. Backups are not encrypted.

Network Infrastructure

NARO's wireless network is divided into two parts, supporting both business operations and guest access. The primary NARO business network requires user authentication and implements MAC address filtering for enhanced security, while the guest network allows visitors to connect without needing a password. The network facilitates connectivity across the administrative and engineering buildings through the use of directional antennas installed on both roofs. Each building is equipped with three Ubiquiti U6+ Wi-Fi access points. Connectivity between the two buildings is maintained by a TP-Link 2.4 GHz N300 Long Range Outdoor CPE210. A Juniper SRX firewall is installed for network security. While network devices are patched as issues arise, they are not routinely updated.

Remote access to the network is provided through a VPN, which is pre-installed on employee-provided laptops. This allows users to log into their NARO Windows Domain, granting them access to online services and the network drive. Additionally, employees can connect to the NARO network using their personal devices, such as phones and laptops, through the VPN.

4 Assessment Methodology

For our assessment, Death Star Consulting utilized the ORION methodology—a structured, risk-based approach tailored specifically for evaluating the cybersecurity posture of small organizations. Informed by NISTIR 7621, this methodology aims to establish well-defined practices, procedures, and standards within small organizations, prioritizing cybersecurity efforts based on the criticality of key assets. ORION is organized into distinct phases that define the key areas to look at—orientation, risk assessment, infrastructure, operations, and norms and standards. Each phase is designed to systematically address vulnerabilities, ensure compliance, and enhance the overall security posture of small organizations.

ORION Methodology	
Phase	**Objective**
Orientation	To gain an understanding of the organization's structure, goals, security, and culture
Risk Assessment	To identify potential threats and vulnerabilities within the organization that could impact operations, data security, and overall resilience
Infrastructure	To assess the physical and network infrastructure to ensure it meets the operational and security needs of the organization
Operational Practices	To evaluate the established operational procedures in place that support security, efficiency, and compliance
Norms and Standards	To ensure adherence to relevant regulations and industry standards

Orientation

The first phase of the ORION methodology starts with Orientation—familiarizing one's self with the organization's structure, goals, security, and culture. It involves establishing a foundational understanding of the existing cybersecurity posture to identify where gaps exist and ensure subsequent steps align with the organization's goals. Orientation is essential for gathering key information, identifying critical assets, and analyzing relevant documentation and policies. The objective is to get to know your organization in order to provide the assessment team the necessary context to proceed effectively with later phases of the methodology.

The following activities are performed during the Orientation phase in order to supply the information and insights necessary to support the risk-based approach central to the ORION method. These activities help establish a baseline of existing practices and policies.

- *Review documentation*

  A comprehensive documentation review is an essential component of the Orientation phase, designed to assess the organization's existing security framework and establish a baseline for the evaluation. The review involved examining a wide range of policies and procedures, data handling procedures, training and awareness policies, regulatory compliance, incident response plans, backup and data recovery procedures, and all other vital and relevant documentation. Asset inventory lists are also analyzed to identify systems and data critical to operations, as well as potential risks with their storage and use. Organizational charts are looked at to understand the structure of processes and flow of information within the organization.

- *Engage with stakeholders*

  Interviews with stakeholders are held to gain insight into existing practices and perceived vulnerabilities. These discussions ensure the organization and assessment team align on risk management goals and help validate the context and information gathered from the documentation review.

Risk Assessment

Following Orientation, we move into Risk Assessment. During this phase, the focus is on identifying potential threats and vulnerabilities within the organization that could impact operations, data security, and overall resilience. It involves assessing the organization's likelihood of risk and potential impact of different threats so that our assessment team knows where to prioritize cybersecurity efforts.

The activities outlined in this section support the goal of assessing an organization's potential risks and vulnerabilities so that mitigation strategies can be implemented to minimize the likelihood of threats.

- *Identify all assets*

  A key activity in the Risk Assessment phase is to create a comprehensive list of all IT assets—hardware and software—and their configurations. This includes laptops, workstations, servers, firewalls, network devices, applications, and any other technology used to support the organization's operations. By completing this step, the assessment team gains a clearer understanding of the technological structure of the organization. Moreover, it provides crucial information required for an in-depth analysis of potential threats and vulnerabilities. Understanding the specific roles and configurations of each asset enables the team to assess the level of risk associated with them.

- *Assess for threats*

  Assessing for threats involves creating a list of all potential threats that can impact or impede operations. This step not only extends to cybersecurity threats, but also includes physical dangers to encompass all potential threats that may harm an organization's ability to operate. Cybersecurity threats may include malicious activities such as data breaches, malware, phishing scams, unauthorized access, or any other attack that may target sensitive data or systems. In addition to digital threats, threat assessment also factors in physical threats, such as natural disasters, fire, theft, or other hazards that may damage or disrupt operations. Evaluating physical threats ensures resilience is not just limited to digital defenses, but also includes the physical security of facilities and equipment. Moreover, it enables preparation and response for a multitude of incidents to ensure an operation can recover quickly and effectively.

- *Perform a risk analysis*

  Utilizing the information from the asset inventory and threat assessment, it is then vital to perform a risk analysis. This process involves analyzing the likelihood and potential impact of each identified threat. This can be done using a risk matrix, a tool designed to help assess and prioritize potential risks. It looks at both the probability of a threat occurring and the severity of its consequences to assign prioritization. For example, a threat with a high probability of occurring but an acceptable level of impact may not require as immediate attention as a threat with a low probability but severe consequences.

Infrastructure

In the Infrastructure phase of the ORION methodology, we are looking at the physical and network infrastructure to assess whether it meets the operational and security needs of the organization. It's vital to conduct a thorough analysis of the organization's system to ensure configurations are in place, updates and maintenance are performed regularly, and security measures are properly implemented.

The activities described in the Infrastructure phase all serve as preventative security measures to mitigate the potential for cybersecurity threats to occur in the first place. This stage can also allow the assessment team to identify gaps in security that expose the organization to exploits and effectively address them.

- *Evaluate network security*

  The assessment of the network architecture ensures it is designed to minimize vulnerabilities and protect assets. This process involves a comprehensive analysis of the configurations, security measures, and operational practices of firewalls and key network devices. Key considerations include:

  - Firewalls should be properly configured and up-to-date to monitor and filter traffic.

- Guest Wi-Fi should be segmented from business Wi-Fi to prevent unauthorized access to sensitive business resources.
- All network devices, including routers, switches, and access points, should have the latest firmware and security updates installed to mitigate vulnerabilities.
- Default credentials on all devices should be changed to strong, unique passwords.
- Access to network infrastructure should be logged and monitored to prevent unauthorized or suspicious activities.

Performing a thorough analysis of the network security architecture helps strengthen an organization's cybersecurity posture and ensures their infrastructure is resilient against threats.

- *Ensure data is backed up and recoverable*

Ensuring the safety and recoverability of data is a critical component of an organization's resilience. Backups protect against data loss caused by hardware failure, cyberattacks, accidental deletion, or natural disasters. Backups need to occur regularly and be stored off-site or in a secure cloud environment to ensure availability. All backups should be encrypted to protect sensitive data. Moreover, it's not enough to just backup data, but it's also vital to ensure the backup is recoverable by testing if the data can be restored quickly and effectively in the event of an incident.

- *Review the physical security*

Physical security is a vital aspect of safeguarding an organization's assets and data. Examining the physical security controls in place ensure that critical infrastructure and sensitive areas are protected against unauthorized access or harm. This review can include looking at visitor management—what procedures are in place to track and control visitor access (sign-ins, temp badges, etc.). It also involves verifying that locks, barriers, and surveillance systems are in place and functional to control and monitor access to restricted access. Ensure access controls are in place to limit authorized personnel only. By reviewing physical security measures, organizations can create a more secure environment for their operations.

- *Implement protective software on devices*

Effective implementation of protective measures can significantly reduce the risk of unauthorized access, malware infections, or data breaches. Make sure anti-malware and anti-virus software is installed and up-to-date on all systems, and that the software is configured to perform regular scans and protect against threats. Operating systems should be patched and running the latest software. Conduct vulnerability scans to identify potential security weaknesses on systems. Maintaining these protective measures help safeguard individual devices and sensitive information.

Operational Practices

After looking at infrastructure, we then look at operational practices. In the Operational Practices phase, the goal is to evaluate the established operational procedures in place that support security, efficiency, and compliance. This not only involves assessing what procedures are in place that promote cybersecurity efforts, but that they are enforced and adhered to. Strong operational practices help mitigate risks, safeguard sensitive data, and ensure business continuity.

In this stage of the methodology, the activities are focused on ensuring that established practices align with the cybersecurity goals, are effectively enforced, and are consistently adhered to by all personnel. These activities help promote strong operational practices.

- *Train employees on cybersecurity*

  Effective cybersecurity starts with the awareness and actions of the employees. This step ensures that comprehensive cybersecurity training is in place for all employees, and that the content and efficacy of any programs in place are appropriate and effective. Cybersecurity training should enable and equip employees with the knowledge and skills to recognize and respond to potential threats. Ensure employees understand the basics of cybersecurity, including identifying phishing emails and avoiding suspicious links. Employees should also be made aware of and adhere to password policies. Train employees on the organization's cybersecurity policies, especially when it comes to utilizing VPNs, organization devices, or accessing organizational resources through personal devices. Cybersecurity training should not be a one-time event, but rather on-going and regularly tested. Training content should be updated to reflect evolving threats and organizational changes. Cybersecurity education helps significantly reduce the risk of human-related vulnerabilities.

- *Implement access control*

  Access control ensures only authorized individuals have access to systems, data, and resources. Properly implementation of access control mechanisms and policies help mitigate the risk of unauthorized access. Ensure your organization regularly logs, monitors, and reviews permissions for current roles and responsibilities. Employees should only have access to the resources required to perform their job, and no more. As previously mentioned in the Infrastructure phase, also ensure physical access controls are in place, such as keycards or badges, to control access to restricted areas. Access should be based on the principle of least privilege, where employees only have the minimum permissions or access necessary to fulfill their role.

- *Ensure data is handled, encrypted, and disposed of properly.*

  Proper handling of data can help protect against data breaches, leakage, or loss. Data handling procedures and policies should be in place and practiced at all times so that sensitive data is not at risk of becoming available to unauthorized individuals. Data handling procedures can include implementing data classification policies, limiting who

has access to sensitive data, and minimzing the amount of data kept. Sensitive data that is kept should be encrypted. Encryption ensures that even if data is intercepted or stolen, it remains unreadable without the correct decryption key. Data should be encrypted in transit and at rest, and even backup data should be encrypted. Lastly, once data is no longer needed, it still needs to be disposed of securely. Data should not be recoverable when it is disposed of. For example, dumpster diving is a potential threat to cybersecurity, so it is important to shred sensitive data rather than just throwing it away. Electronically, this can include wiping data or destroying physical media (hard drives, USB) to ensure the data cannot be restored.

Norms and Standards

Lastly, the ORION methodology looks at cybersecurity norms, and compares existing regulations and standards against organizational practices to ensure adherence. This phase is essential for confirming that the organization's cybersecurity practices are aligned with recognized frameworks, regulatory requirements, and accepted standards.

- *Ensure compliance with legal and industry requirements*

  This step involves reviewing policies and procedures to ensure compliance with applicable laws and regulations. These may include global frameworks such as HIPAA, industry-specific regulations such as PCI DSS, or other laws such as data privacy laws. Our assessment team will assess the scope of applicable laws based on the type of data the organization handles and the sector in which it operates. We will then review the internal policies related to data handling, access control, incident response, and privacy to ensure that the procedures are in place to meet the obligations outlined in relevant laws.

5 Assessment Activities

Asset Identification

The assessment team precisely evaluated NARO’s existing asset inventory procedures and sought to determine whether the organization maintained a thorough and updated record of all important IT assets. This evaluation set the stage for a strong cybersecurity posture and helped to strengthen our defenses. The review was included and was important.

The effectiveness of current practices was assessed through the analysis of inventory management tools and manual processes.

IT staff shared understandings through interviews to understand challenges in asset tracking and to identify the extent of manual work versus automation and the frequency of updates.

The findings showed that NARO's asset inventory lacked consistency and comprehensiveness and this deficiency weakens its ability to identify and protect important assets effectively. The team suggested that the company should implement automated inventory management tools and also conduct periodic manual verifications so that they can guarantee accuracy in their stock records. Real-time understandings into its technical ecosystem would be provided to NARO by this dual approach so that vulnerabilities can be promptly identified and protective measures can be zeroed in on.

Cybersecurity Training Evaluation

Employees must be aware and prepared, and they play important roles in an organization's cybersecurity strategy. A thorough evaluation of NARO’s cybersecurity training programs was included in the assessment to measure their relevance and frequency and overall efficacy. The team engaged in key activities such as planning and organizing events.

Training material review involved assessing existing training content for coverage of important topics such as phishing awareness and secure data handling while also evaluating incident response protocols: the results drew attention to important gaps that need to be addressed.

Employee surveys were conducted to gauge staff understanding of cybersecurity protocols and to identify knowledge gaps.

The team analyzed existing performance metrics related to training outcomes and evaluated the effect of current programs.

The evaluation showed that the training program has important gaps. Sessions occurred sporadically but lacked depth and consistency and did not focus on high-risk areas such as sophisticated phishing attacks and secure practices for data handling.

The assessment recommended that we hold regular training sessions, and these sessions should be tailored to fit our organization's needs. These sessions must include activities and discussions.

Employees participate in phishing simulations so they can recognize and respond to real-world threats.

Scenario-based exercises improve incident response readiness through interactive simulations.

Active competency and alignment with evolving threat landscapes are guaranteed by refresher courses.

Integration of Assessment Activities

Both asset identification and cybersecurity training evaluation serve integral components of a wider strategic approach to enhance the cybersecurity resilience of NARO. An up-to-date asset inventory lays the groundwork for risk reduction and strong employee training programs help reduce human error. These activities form a proactive defense mechanism and equip NARO with the tools and knowledge to reduce risks and respond effectively to emerging threats.

6 Assessment Results and Recommendations

This section provides a summary of the findings from the assessment activities described in Section 5, grouped into Strengths, Weaknesses, and Observations to give a fair and actionable overview of NARO's cybersecurity posture.

Strengths

The assessment identified several practices and policies related to which NARO has been effective. These form a good basis for its work in the field of cybersecurity. These are those strengths which, if preserved and expanded when possible, will contribute positively toward organizational resilience:

Basic Asset Inventory Framework:

- Although not fully implemented, there is a groundwork asset inventory process in place, which NARO has initiated to form a foundation for new enhancements.
- The organization is appreciative of the inventory process, as shown by partial documentation and occasional updates.

Employee Engagement in Cybersecurity Training:

- Surveys indicated a general willingness of employees to engage in cybersecurity training programs, reflecting a positive organizational culture.
- Although training does need to improve, at least some formal cybersecurity training is conducted, and a conscious effort toward reducing human-error vulnerabilities is being made.

Collaborative IT Team Culture:

- The IT personnel were cooperative in the interviews and candid regarding today's struggles, which allowed deep insight into current operations, processes, and constraints.
- This sets up the organization nicely for the effective implementation of new cybersecurity practices.

Weaknesses

The testbed assessment identified a number of findings that represent risks to NARO's overall cybersecurity posture. Each finding is rated by its Severity Rating to support prioritization.

Incomplete Asset Inventory-HIGH:

- Asset inventory incomplete, incoherent, and does not account for new, acquired, and legacy assets. Incomprehensive inventory provides blind spots for risk management.
- Impact: Inability to identify all key assets means inability to monitor threats and/or inability to patch systems.
- Recommendation: Automate the asset management system and perform quarterly reviews for completeness and accuracy.

Lack of Regular Cybersecurity Training (MEDIUM Severity):

- Inadequate frequency of training in view of rapidly changing cyber threats; key topics such as phishing awareness and safe data handling are not well represented.
- Impact: Employees remain unprepared to handle sophisticated cyberattacks, increasing the likelihood of human-error-based breaches.
- Recommendation: The training shall be conducted quarterly, scenario-based, and focused on emerging threats along with practical exercises.

Manual-Intensive Asset Management (LOW Severity):

- Excessive use of manual updating of inventories leads to a greater chance of mistakes and delay in finding security gaps.
- Business Impact: Operational efficiency is limited, as well as the response towards any vulnerability.

- Recommendation: Minimize manual work by migrating to automated tools for tracking with higher accuracy.

Observations

The following were some findings that were remarkable but did not have adequate data to be definitive strengths and weaknesses:

Shadow IT Practices

- The interviewing of the staff revealed instances of unauthorized use of software and cloud services.
- Implication: Tools used without monitoring may introduce vulnerabilities or bypass organizational controls. Further inquiry should be made to ascertain the scope of this issue.

Limited Training Feedback Mechanisms

- There is no formal mechanism for soliciting feedback relevant to training sessions to understand how well they went.
- It means that without data-driven insights, it would be very challenging to fully accommodate training programs that cater to the needs of employees.

Scalability Issues:

- Current systems cannot cater to organizational increase in the future, especially around inventory and training.
- This might be enough today, but scaling up in the near future would require further investments in systems and workforce.

Recommendations

Based on the findings above, the recommendations that clearly can be given are on addressing weaknesses, capitalizing on strengths, and to further explore observations.

Strengthen Asset Management:

- Automated inventory management solutions should be installed to provide more accuracy and better coverage.
- Develop standard asset documentations, tracking, and decommissioning processes.

Enhancing Cybersecurity Training:

- Design an in-depth course curriculum that covers advanced topics on cybersecurity.
- Increase the frequency; include interactive training components such as phishing simulations.

Shadow IT and Investigation of Feedback Mechanisms:

- Conduct organization-wide audits to uncover unauthorized tools in use.
- It will be a training session feedback loop that measures employee engagement in terms of learning outcomes.

Leveraging the identified strengths, embracing critical weaknesses, and exploring key observations will afford NARO the opportunity for a far more robust cybersecurity framework-one that is resilient, adaptive, and in line with best practices.

7 Conclusions and Follow-On Activities

Conclusions

This cybersecurity assessment of NARO, Inc., has furnished critical insight into the security posture of the organization, pointing out weaknesses that may well have a materially significant impact on operational integrity and stakeholder trust. As an organization navigates this ever-evolving cyber threat landscape, proactive identification and remediation of potential weaknesses within security frameworks is highly relevant. Key conclusions emphasized in findings from this assessment include:

1. **Cyber Threat Vulnerability:** Poor asset management, insider threats due to access control and lack of employee training, weak risk management practices for third-party vendors, and poor incident response plans are some critical vulnerabilities identified in the assessment. Any one of these can provide an opening for cybercriminals to attack an organization and cause data breaches with losses of money, besides bringing a bad name to the organization.

2. **Structuring a Proactive Cybersecurity Strategy:** Cybersecurity is no longer solely an IT issue, but it also relates to organizational risk management. The study appears to support the fact that there is a dire need for having a proactive strategy in cybersecurity in order to anticipate risk before it materializes, and to take mitigating action. Periodic assessment and continuous monitoring, devoted to the improvement of the security based on emerging threats, are needed for this proactive approach.

3. **Holistic Security Measures Are Called For:** Cybersecurity cannot be done piecemeal. Reviewers informed the audit of the need to adopt a whole-of-government security system that affords a comprehensive approach toward cybersecurity through risk management, user training, incident response, and third-party vendor assessments. This way, all elements in the organization are connected with their cybersecurity initiatives to create a robust operation.

4. **Whole Organization Engagement**: The engagement and commitment of all stakeholders are the backbone for successful implementation in cybersecurity. Everyone-from senior management to the very important role of the line employee-adds to a culture of security. The promotion of cybersecurity awareness and responsibility at all levels in support of a common commitment to protect organizational assets.

5. **Continuous Improvement is Paramount:** The field of cybersecurity is so dynamic that no organization can afford to be complacent but must strive by constant evaluation for improvement. The assessment outlined that NARO needed to commit to regular evaluation and refinement of its cybersecurity policy and practice. These are the regular audits, training of employees, and updating of security protocols that will make the organization resilient against emerging threats.

6. **Alignment with the NIST Cybersecurity Framework:** Conclusions from this assessment emphasize the need for the NARO cybersecurity efforts to be benchmarked against the NIST Cybersecurity Framework. The core of the framework is built around five vital functions that an organization can use appropriately to manage and reduce cybersecurity risk in working baselines: Identify, Protect, Detect, Respond, and Recover.

In all, this cybersecurity assessment provides a very critical backbone for the improvement of NARO, Inc.'s security posture. Being cognizant of the identified vulnerabilities and taking proactive and holistic cybersecurity steps, NARO will be in a better position to strengthen its defenses against such attacks, protect continuity, and foster stakeholder trust in their operations. Following-on activities below are proposed in support of the organization for realization of these objectives.

Follow-On Activities

What follows are some proposed follow-on activities that effectively implement recommendations from this assessment to nurture a robust cybersecurity culture within NARO, Inc. This is in order to ensure the organization addresses the identified vulnerabilities while making provisions toward cultivating a proactive approach toward cybersecurity that would adapt to an ever-changing threat landscape.

1. Create a Cybersecurity Task Force:

Objective: Set up a selective task force that assures the proper implementation of cybersecurity initiatives.

Actions:
- Identify team members from departments like IT, compliance, human resources, and operations.
- Designate specific responsibilities to each member so that accountability and definite outcomes may be assured through teamwork.
- Schedule periodic meetings to review progress made, discuss challenges, and adapt strategies as needed.
- The task force will also engage in advocating at all levels within the organization for communication on cyber security issues.

2. Formulate an In-depth Cyber Security Action Plan:

Objective: The formulation of an action plan which has summarized particular actions on how to mitigate the identified vulnerabilities.

Actions:
- Prioritization of the action according to the finding of the risk assessment; that is, first starting with the high risk vulnerabilities.
- Clearly, outline timelines for every action point and assign responsibility to ensure timely execution.

- Include relevant performance metrics to measure the effectiveness of the actions implemented over time, which can thus help modify the plan based on the data collected.

3. Conduct a Thorough Risk Assessment:

Objective: Look for New Threats and Vulnerabilities in the Organization's Risk Landscape

Actions:

- Apply both qualitative and quantitative techniques to perform risk assessments with new technologies and new processes.
- Perform periodic updates of the risk assessment to account for changes in the operations, technologies, and threats of the organization.
- Document observations and update the cyber security action plan in order to address newly identified vulnerabilities.

4. Implement Effective User Access Management Policies:

Objective: Strengthen user access control with a view to offer increased security to sensitive information and systems.

Actions:

- Formulate a policy stating that every employee accessing sensitive information must access it using a unique account.
- Develop and implement role-based access policies. Allow access only on a need-to-know principle based on job responsibilities.
- Regular audits of rights assigned to individual users and revoking those users whose job no longer warrants access

5. Enhancement of Cybersecurity Training Programs:

Objective: Foster a culture of cybersecurity awareness

Actions:

- Elaborate a proper training module with full coverage of topics that need to be discussed, including phishing awareness, sensitive data handling, and password management.
- Schedule regular trainings for all employees, including training for new employees and refresher courses.
- Training Effectiveness: Assessment and feedback are highly important for the continuous enhancement of training content and methods of delivery.
- Contemplate scenario-based training exercises that would serve to equip employees with better response capabilities in the face of an actual cyber incident.

6. Incident Response Plan:

Objective: The incident response plan should be straightforward and feasible to enable the organization to respond to a cybersecurity incident.

Actions:

- Document all the processes involved in responding to an incident: detect the incident, analyze it, contain it, eradicate it, recover from it, and conduct post incident activities.
- Clearly outline the roles and responsibilities of team members in case a cybersecurity incident is encountered to ensure an effective response.
- Conduct tabletop exercises and simulations to evaluate the incident response plan to make necessary changes learned from such exercises.
- Put in place incident reporting and escalation mechanisms to ensure timely communication concerning security incidents.

7. Vendor Security Assessment Protocol:

Objective: To ensure that third-party vendors meet NARO standards on cybersecurity.

Actions:

- Design a third-party vendor assessment process: security requirements, compliance checking, and auditing on a periodic basis. Each third-party vendor will be prepared with documentation related to the details of their cybersecurity and their certifications. Establish proper communication with your vendors for continuous assessments and updates on their security practices.

8. Plan for Cybersecurity Audits:

Objective: Periodic assessment of the adequacy in cybersecurity.

Actions:

- Run comprehensive audits at least annually and cover all aspects of the cybersecurity framework, including policies, procedures, and technical controls.
- Use audit findings to help update cybersecurity action plans and ensure the remediation of any identified vulnerabilities.
- Document the outcome of audits and share findings with stakeholders to ensure accountability.

9. Continuous Monitoring and Threat Intelligence:

Objective: To understand emerging threats and vulnerabilities within the cybersecurity landscape.

Actions:

- Invest in threat intelligence toolkits that would provide updates in real-time concerning the current cybersecurity threats facing NARO.

- Establish a Security Operations Centre, outsource the function, or ensure network activities are monitored for events that portray abnormal activities
- Review the measures regularly for adjustments, drawing on knowledge from experiences related to monitoring activities and from threat intelligence reports.

10. Cybersecurity Awareness:

Objective: Making cybersecurity part of the culture in the organization

Actions:
- Create an open environment where employees could freely mention possible cybersecurity concerns with no threat of reprisal against them.
- Reward employees to show good security practice, which would provide them a sense of ownership and accountability.
- Run frequent security awareness campaigns, making sure cybersecurity is at the top of the minds of employees, via posters, newsletters, and resources on the intranet.

11. Engagement with External Cybersecurity Experts:

Objective: Leverage expertise in further strengthening security.

Actions:
- Collaborate with cybersecurity consultants or firms that perform reviews and make recommendations from time to time.
- Attend industry conferences and training classes to remain current about recent trends in cybersecurity, technologies, and best practices.
- Employ third-party services for the purpose of penetration testing and vulnerability assessment to gain unbiased knowledge of the organization's security posture.

12. Resourcing for Cybersecurity Initiatives:

Objective: The cybersecurity initiatives are provided with the necessary resources and supported accordingly.

Actions:
- Develop a budget that would allow for technology investments, training programs, and staffing for cybersecurity.
- Demonstrate to stakeholders the various risks and consequences of poor cybersecurity to justify requests for funding.
- Research grants and other funding opportunities available to nonprofits for improving cybersecurity capability.

The follow-on activities will further improve cybersecurity for Naro, Inc.: protect the necessary assets and make the organization resilient to survive in the new digital space. Continuous

improvement, proactive risk management, and embedding a culture of security awareness will place NARO in the leading position in cybersecurity across its industry, thereby enabling the mission and protection of stakeholders.