NARO, INC ASSESSMENT REPORT

Prepared by: Isaac Caldera, Khoa Nguyen, Ronald Dewees

ByteMunchers

Executive Summary

NARO, Inc. (NARO) is a non-profit organization specializing in research and development for renewable energy solutions and electric vehicle (EV) charging infrastructure. Due to the critical nature of their research and the sensitivity of their data, NARO engaged ByteMunchers Consulting (BM) to conduct a comprehensive cybersecurity assessment. This assessment's primary goal was to evaluate NARO's current cybersecurity measures, identify vulnerabilities, and provide actionable recommendations to improve their overall security posture.

This report provides detailed observations, analysis of identified weaknesses, and recommended mitigation strategies. The assessment team focused on key areas, including network and communication security, physical and technical security, data storage policies, and continuity planning. The findings revealed several strengths in NARO's approach, particularly in their use of secured physical spaces and automated backup procedures. However, multiple vulnerabilities were identified, such as gaps in remote access security, inconsistent physical security practices, location hazards and shared server facilities with another organization. While this review outlines all the findings and weaknesses that need to be addressed, ByteMunchers also calls on NARO to prioritize the development of an access control system first due to it crucial nature. We extend our gratitude to the NARO staff, particularly Mr. William Donaldson III and his team, for their cooperation and valuable insights for this assessment. Their contributions significantly play a vital role in the comprehensiveness of this report.

1 Introduction

1.1 Background

With the increasing rise in recent cyber incidents with data breaches which potentially affect billions within tech giants like Meta. NARO's focus is on EV charging solutions and wishes to assess their vulnerabilities to potential cyber incidents. The assessment will be aimed at identifying weaknesses in NARO's cybersecurity framework as we compare it to NIST to recommend improvements.

1.2 Scope

The scope of this assessment will be our audit checklist of NARO's security and related policies. A focus will be placed on management access, physical security, wireless security, software control, and best practices for handling data. In management access, we will assess the management system based on the principle of least privilege in the access to information of both departments of NARO (management and engineering). We will also evaluate NARO policies with the aim of reducing the risk of phishing and internal threats. In security, we will examine NARO's current physical and system security to find potential vulnerabilities from external breaches such as poor lock mechanisms, or proper trackers.

However, we will not be conducting penetration testing as it is invasive to NARO's operations as a smaller business and can potentially disrupt business temporarily.

1.3 Report Organization

The report will be organized with Section 2, providing a clear overview of NARO's facilities and systems. Sections 3 and 4 will focus on the details of the assessment methodology and the activities that will be conducted. In Section 5, there will be the results of the activities in Section 4 which indicate the strengths, weaknesses, and results from our observation of NARO's framework along with mitigation strategies. Section 6 concludes the report by outlining the findings and any follow-up activities.

2 System Overview

Given that NARO operates on two completely different buildings with clearly defined job specialties, our security research team will conduct an overall assessment of the physical facilities and the systems of each facility along with its specific function. The

purpose of this comprehensive evaluation of the system and facilities is to identify potential vulnerabilities and risks in terms of security and safety in the working facility. We will later provide a detailed analysis that will focus on the strengths and weaknesses discovered based on the information found in this section.

2.1 Facility of Engineering Building

The NARO Engineering Building will serve as the central building designated for conducting production, research, design, and testing of technology. This research facility will play the most vital role because it will be the main core functionality of the NARO company. The Engineering Building will include several components, which include Office space (cubicles) for engineers to handle the paperwork, a lab space for testing, a hazardous material storage area, and a vehicle bay.

Overall access control of the Engineering Building: secured using a keypad lock and exterior padlock for the overhead doors. All these access points required badges or PIN codes to enter and operate 24/7 on a daily basis.

Overall Components breakdown:

1. Office space
    a. Purpose: Designate a work area for engineers to work at desks, including documentation, reporting, analysis, design, and product research.
    b. Equipment: A work laptop is provided at each desk, with access to proper VPN services and Office 365 installed for multi-work purposes.
    c. Access: This area is secured using a proximity card. These doors are unlocked and allow public access to the lobby area during business hours (9:00 a.m. to 5:00 p.m.). Everyone can go out without the need to check for credentials/pin.
2. Lab space
    a. Purpose: Designate testing and conducting analysis area for Battery Technology, Solar panel Technology and EV compatibility.
    b. Equipment: The lab provides engineers with work devices that are mixes of both Windows and Linux operating systems. These devices are used to securely transfer critical information to the server in the Administrative Building using SSH, secure copy (SCP), and rsync. All of these devices are connected and limited to the NARO wireless network to gain access to the server.

   c. Access: This area is secured with a keypad lock that requires either badges or employees' pins, which only allow access to the proper role (Admin, Engineers).
3. Hazmat storage area
   a. Purpose: This area is used for the storage of hazardous materials, including lead, arsenic, cadmium, selenium, and lithium, which are used as core components for the assembly and manufacture of electric battery systems as well as solar energy panels.
   b. Structure: During the interview with the chief engineer, he provided information that the hazmat would consist of three central departments that were classified based on the danger of the materials, toxic things like technological waste collected from failed experiments would be stored at the highest level, and products along with other materials would be stored at the lower two levels.
   c. Equipment: Devices and computers in this area will use a Mac operating system with built-in material management software.
   d. Access: This area is highly restricted even with engineers, only approved personnel with proper access code are allowed to enter.
4. Vehicle bays
   a. Purpose: This area is designed to conduct EV testing on vehicles. These vehicles can be brought inside the building and connected to a prototype charger.
   b. Equipment: NARO provides special workstations which include computers for these stations since the provided work laptop isn't compatible with an expansion card to interface with the EVS for testing and collecting data purposes.
   c. Access: This area is secured and required access card or pin to entered

2.2 Facility of Administrative Building

The administrative building handles paperwork, interacts with customers, and manages the overall information flow. Unlike the Engineering Buildings, the administrative building is not standalone but only occupies a half of the entire building shared with GAS company. This work area is also connected to another company and has common areas such as custodial, storage, server room, and kitchen.

Overall critical components of Administrative Building breakdown:

1. Office space

a. Purpose: Designate as a work area for the staff who handle Grant writing, Financial and accounting, and sales responsibility.
b. Equipment: A work laptop is provided at each desk, with access to proper VPN services and Office 365 installed for multi-work purposes.
c. Access: The exterior doors to the Administrative Building are usually left unlocked. These doors are also allowed for public access during business hours (9:00 a.m. to 5:00 p.m.). Everyone can still go out without the need to check for credentials/pin.

2. Commons Areas: These areas are shared with other companies in the building (GAS company), which include storage rooms, servers, custodial and kitchen
    a. Storage room:
        i. Purpose: This space is used to store company documents, supplies, and spare equipment such as laptops and workstations.
        ii. Stored information: After interviewing the management supervisor, he said that all the company's files are stored here, sealed in envelopes, and arranged on shelves according to their area. At the same time, this place also stores old spare machines and equipment, including two old but still working laptops.
        iii. Access: Because this is a shared area, any personnel from NARO and GAS can access it with their access cards.
    b. Server room:
        i. Purpose: NARO set up the company's server in this room to store confidential documents, designs, algorithms, and process data collected from experiments and prototypes in the Engineer Building.
        ii. Structure: This room is divided into two sections. Each desk features a workstation connected to a KVM network, allowing direct access to the servers. The workstation labeled NARO is connected to the NARO network, while the workstation labeled GAS connects to the GAS network. The server racks house various switches, routers, and firewalls that provide Internet access to their network. These components include an AT&T gateway, a Juniper SRX firewall, and a Netgear ProSafe JGS524 Gigabit switch. An interview with the Management supervisor also revealed that the server room has a "kill switch" that can directly unplug the network connection to the server, which we haven't yet verified if such a mechanic exists. In addition, NARO uses total of 17 servers which are: 12 Supermicro 2U Mainstream A+ SuperServer (AS -2024S-TR). The other five (5) servers are Dell PowerEdge R940 Rack

Servers. Supermicro server are running on Ubuntu 18.04.6 LTS while Dell server are running on Windows Server 2019

iii. Access: In an interview with the company CEO, he mentioned that access to these servers is only limited to critical personnel using an access card and proper PIN. However, we have not yet determined who has access to these facilities or whether GAS employees can still access them since the server rooms are shared between 2 companies.

2.3 Overall System Review

1. Remote Access: Employees can log in to their personal computers via NARO provided VPN which will allow them to access the server and sign in their work credential.
2. Wireless Internet Network: NARO has two types of internet networks: business and guest networks. The guest network doesn't require passwords, but the business network will require authentication from employee credentials to gain access. Internet access is available in both buildings.
3. Servers: 17 servers include 12 Supermicro 2U Mainstream A+ SuperServer, 5 Dell PowerEdge R940 Rack Servers.
4. Laptops: 36 new laptops (confirmed in CEO interview) include 35 issued Window operating system for each employee, 1 MacBook in the hazmat room. In addtion, NARO also have 2 older laptops in storage for emergencies.
5. Number of personnel: 35 in total with 15 on Administrative and 20 in Engineering.

3 Assessment Methodology

Our team, group 4, will apply the NIST cyber security framework consisting of 5 parts, which are Identify, Protect, Detect, Respond, and Recover. This framework will be tailored to align with the specific system needs and structure of NARO, focusing on both technical and administrative security measures. The approach included documentation review, in-person interviews, and analysis of the overall cyber infrastructure without active system deployment to avoid disruption of production or business operation.

Assessment based on NIST framework:

1. Identify: In this step, we will start to thoroughly study the entire NARO system, which includes the working equipment, software installed on the computer, operating system, and production process, as well as information in the enterprise. The objectives of this step aim to determine the critical value of the

information and also to identify the vulnerabilities and potential risks in the system.

2. Protect: In this step, we will evaluate the security software installed in the system, such as firewalls and antivirus. We will analyze the performance of these software activities based on the report on their history of operation. Based on this analysis, we will determine if NARO needs to switch to more reliable software or if this current software is enough as a security measure.
3. Detect: In this section, we will focus on evaluating NARO practice in managing access logs. This aims to determine NARO's capabilities in detecting suspicious behavior to prevent security breaches.
4. Respond: In this section, we will focus on evaluating NARO's plans and procedures when a security breach occurs. The objective is to determine the effectiveness of NARO's reaction to such events and thus identify potential areas for improvement.
5. Recover: In this section, we evaluate NARO's data recovery and backup solution and the existing procedures regarding the recovery process. Our aim is to determine NARO's capabilities to recover and resume operations quickly after cyber events. Based on this evaluation, our company can identify areas for improvement and help NARO effectively recover information during these cyber incidents.

Figure 3.1: NIST framework

4 Assessment Activities

Using the methodology from the NIST cyber framework as previously described we will use in-depth activities to evaluate NARO's current cybersecurity measures. These activities strive to assess NARO's current strengths and weaknesses which be further dived into in section 5. The assessments will be Risk Management, NARO Document Review, In-person interviews, and an Audit of NARO's practices.

4.1 Risk Management

Taking into account probability, severity, and cost of potential risk can help plan for future incidents. Looking at the importance of certain data or hardware will allow for proper allocation of resources by NARO to improve cybersecurity efforts.

4.2 NARO Documentation Review

The assessment team will review how NARO outlines its policies and procedures for data backup, remote access, training procedures, incident reports, and security. Make sure there is an implementation of each document within the company as well as adequate proper outlines for each category.

4.3 Scan of Hardware and Physical Security

We will comprehensively scan all devices under the NARO inventory to collect information about vulnerabilities. For company laptops provided to employees, we will thoroughly review all applications that have been installed by employees on the work laptop. Our primary focus will be on detecting and listing non-work related or high-risk profile software, including but not limited to social media, video games, and any potentially suspicious software. Additionally, we will also perform virus and malware scans, examine all laptop specs and battery health, and verify patches to see if they are all up to date. Furthermore, in addition to laptops, we will also conduct examinations on the NARO server to gather server log information, check for configuration and security settings, and determine the overall health of the system. For physical security, we will evaluate the door's functionality for physical security based on its auto-locking function and its interaction with the proximity card.

4.4 Backup data evaluation

Our team will also perform backup data and recovery procedure examination, which will focus on verifying the quality of the stored backup, the server's capability in storing data, the frequency of how backup data is updated, and the recovery procedure in case of cyber events.

4.5 Employee Interviews

It is important to conduct effective and thorough interviews with current employees in order to identify any poor or unoptimized practices at NARO. This could be anything from employee privileges to how documenting is handled. Interviews can also feel any bad actors that may have been overlooked without background checks to see any malicious affiliations. Interviews also stand to establish training protocols are widely practiced at NARO.

4.6 NARO Audit

An Audit that spans from security measures to data management with the goal is to ensure that NARO’s practices follow the NIST farmwork of Identify, Protect, Detect, Respond, and Recover. Use our Audit document to identify that all aspects are up to date and effective with practices like physical security, sensitive information privileges, data management, data recovery, and employee training.

5 Assessment Results and Recommendations

After conducting assessment activities as identified in the previous section, we will determine some of NARO’s strengths, weaknesses, and any observations. This section will discuss the strengths that should be honed to further mitigate risks and point out weaknesses that should be improved as they pose a risk to the company. Observations are more so notes of interest that stood out with no defining weakness or strength.

5.1 Weaknesses

(Medium) Inconsistent Physical Security Controls.

Description: The administrative building's unlocked exterior doors and shared server room with GAS present a security risk. Although magnetic locks and proximity cards are in place, the open access hours during working hours and shared server resources increase the risk of unauthorized entry.

Mitigation: Implement stricter access control policies for common areas and conduct a physical security audit. Consider restricting server room access to authorized personnel and creating a visitor policy.

(High) Remote Access via Personal Devices.

Description: Employees are permitted to use personal devices to access NARO systems through the VPN and webmail. The use of unsecured personal devices presents a risk of data leakage or unauthorized access.

Mitigation: Introduce a Mobile Device Management (MDM) solution to enforce security policies on personal devices. Implement multi-factor authentication (MFA) for VPN connections.

(Medium) Lack of Centralized Account Management for Lab Systems.

Description: The engineering lab systems are not part of the NARO Windows Domain, relying instead on local accounts with varying security standards.

Mitigation: Centralize account management for all systems, integrating lab systems into the Windows Domain where possible. Conduct regular audits of local account policies.

(Medium) Lack of Proper Training on Phishing email.

Description: Currently, NARO does not have a suitable program for training employees to handle Phishing emails; the only training program that NARO offers is simply an instruction-taking training course on LinkedIn without proper training or mock practice in NARO.

Mitigation: Implement routine in-person training on watching out for phishing emails, suspicious calls, and text. Make sure to stay up to date with possible scams technology.

(High) Software Control on Company Work Device.

Description: Based on the information collected on the Checklist, we have learned that NARO does not have strict controls on the software downloaded on employees' work computers. This oversight leads to various security vulnerabilities, as employees are

permitted to download and access any software of their choosing. Even unintentionally, employees can inadvertently disclose confidential information on social media or download pirated software, which can pose a massive security risk for NARO, including information leakage, malware, and viruses.

Mitigation: Enforce software restrictions on the company laptops so that only approved software can be downloaded and set up by employees. The employees can submit a ticket for software approval directly to the administrator.

(Medium) Limited Incident Review Process:

Description: According to the information documented in the Checklist, NARO has encountered cyber incidents which come from Phishing email. However, the incident was simply recorded through informal communication and any updates to the policy were just merely communicated through email exchanges to employees. These simple measures are insufficient to ensure effective security for NARO, which suggests that incidents like this are likely to reoccur.

Mitigation: Establishing a formal review process after every incident. Specifically detailing what happened and analyzing how the employees can do differently to prevent it. Furthermore, it is imperative to develop detailed procedures, actively update policies for these scenarios, and regularly conduct employee training.

(High) Potential environmental hazards in Server room:

Description: Based on a recent email with the CEO of NARO, it has come to our attention that the bathroom located on the second floor of the administration building frequently has plumbing issues, resulting in water leaks that affect both the kitchen and the server room. This could potentially damage NARO's IT infrastructure, as water dripping from the ceiling could damage NARO's servers. NARO's entire system will be shut down indefinitely if these devices are damaged.

Mitigation: NARO servers' equipment to a safer location, such as a storage facility or engineering building. In addition, NARO can also set up humidity monitoring equipment to detect potential water leaking hazards and ensure that the server room is consistently maintained and operated in an ideal environment

(Medium) Low frequency of backing-up data process:

Description: In an interview with William Donaldson III, the Chief Executive Officer of NARO, it was indicated and implied that NARO conducts its own backup procedure approximately "every few weeks." In addition, NARO also relies on PITA (IT service provider) to conduct the backup procedure weekly. For a company like NARO that specializes in EV and solar technology development, data is essential and is the foundation for NARO to continue operating. Such a gap is insufficient for such a research-driven company. If the primary data is damaged (due to a virus, cyber attack, malware, etc.), the data can only be partially restored by backing up the data from the last time it was backed up, which can be up to a week prior. For instance, if NARO made a breakthrough discovery two days ago, but the most recent data backup was a week ago, this could detrimentally impact NARO. In this case, if the system is compromised and the primary data is corrupted, NARO could potentially forfeit crucial research data they just discovered, which can set the progress back by weeks, months, or even years.

Mitigation: increase the frequency of regular data backup to ideally daily like most other tech companies. This will ensure that crucial research data is backed up regularly, reducing the risk of losing valuable data.

5.2 Strengths

Physical Security in the Engineering Building:

- The secure access controls and keypad locks for the engineering facility ensure that critical research and development spaces are well-protected.

Automated Backups:

- The use of automated scripts by PITA for regular backups, combined with encryption and verification processes, demonstrates a proactive approach to data resilience.

Hardware check:

- Inventory checks are usually conducted every 6 months, this will ensure that the products are stored in an efficient state, minimizing the risk of equipment damage.

Employee Background Checks:

- Background checks are conducted before hiring employees. This strict screening process will minimize the possibility of insider threats and increase the security of the company.

Incident Respond:

- NARO has a plan to respond in the event of an incident. Although it hasn't been updated in 18 months, it will still be useful in helping the company prepare for situations and avoid system and administration management paralysis.

Remote Management of Company devices

- NARO administrative management has the ability to monitor remote work devices once they are connected to the NARO network or working station. This will control the information employees have access to and prevent unauthorized access to other websites.

5.3 Observations

Guest Network Security

Although the guest network does not require a password, the use of MAC filtering adds a layer of control. However, potential vulnerabilities remain due to the ease of spoofing MAC addresses.

Server room security

The server room is shared between GAS and NARO Inc., granting employees from both organizations unrestricted access. Given the critical nature of data to NARO, this also poses a significant risk. Employees from GAS can potentially damage the server, whether accidentally (spilling coffee or water) or intentionally (insider threats).

Mitigation: Relocate the server devices to another room that is only under NARO ownership. Security cameras also should be added 24/7 to comprehensively monitor the servers for any unauthorized access.

Hazmat Handling and safety:

Interviews with hazmat staff highlighted well-defined safety protocols, but no digital record of these procedures was available for review. This may limit the safety measures that are handled by employees.

Mitigations: Making sure there is an accessible well-defined procedure both online and paper can offer a better understanding for staff when conducting both low-risk and high-risk procedures.

Incident Response Planning:

NARO has established an incident response plan for certain scenarios; however, the plan lacks sufficient detail and is not regularly updated. Our team is prepared to assist in the development of comprehensive policies to address these deficiencies effectively.

6 Conclusions and Follow-on Activities

Our team found NARO's focus on physical security in their engineering facilities and automated data backup procedures to be more than substantial in nature. These measures directly correlate with NARO's commitment to protecting its critical research and development efforts. However, a thorough assessment also revealed vulnerabilities in many currently present attributes. There are issues with remote access policies, physical security in shared spaces, and the lack of centralized management in lab systems, which present risks that could impact their security. Addressing these vulnerabilities will ensure that NARO continues to secure its operations and intellectual property effectively.

The cybersecurity assessment highlighted both the strengths and vulnerabilities of NARO, Inc.'s current security framework, providing what is a very clear and beneficial path to success for the parties at play. The actions going forward should prioritize improving remote access security and reviewing physical access policies as highlighted throughout the report. Additionally, integrating the lab systems into a central domain would provide better security and viewing with policy enforcement. ByteMunchers believes in NARO's efforts in proactively address these challenges. We extend our sincere gratitude to the NARO staff for their invaluable cooperation and transparency throughout this process. BM stands ready to assist NARO with implementing these recommendations and conducting future assessments. Together, we can build a robust and resilient cybersecurity framework to safeguard NARO's innovative research and operations.

Follow-Up Activities

1. **Enhancing Remote Access Security:**

   Deploy a Mobile Device Management (MDM) solution to enforce security policies on personal and corporate devices used for remote work. Require mandatory encryption, password protection, and security updates for all devices. Also consider introducing Multi-Factor Authentication (MFA) for VPN access to ensure even more secure connections.

2. **Physical Security in Shared Areas:**

   Establish a stricter access control for shared spaces, especially the server room. Use a visitor management system for external personnel. Use access logs to track all access of entry. Implement stronger physical barriers for critical spaces too, like fences.

3. **Centralize Management:**

   Integrate all lab systems into the NARO Windows Domain or consider using centralized account management software to use uniform security policies. Standardize password policies amongst all users and conduct regular audits to verify compliance.

4. **Guest Network Security:**

   Require password authentication for guest network access and use monitoring tools to detect unauthorized activity. Fully segment the guest network from the business network and employ intrusion detection to identify potential threats.

5. **Hazmat Protocols:**

   Create a centralized digital repository for hazmat safety procedures and all other important information, accessible to authorized personnel only. Use secure document systems with revision tracking and controlled access.