FINAL REPORT

DAMIEN BELTRAN | HANNAH STANEK | ISAIAH ALVAREZ | WES GAUSE

CS-3113-01T

01

INTERACTIVE TABLE OF CONTENTS

NARO COMPANY IIC

02

EXECUTIVE SUMMARY

This cybersecurity assessment evaluates the operational, technical, and physical security state of NARO, Inc., a small yet sophisticated non-profit involved in renewable energy research and development. Their core focus lies on designing compact solar-powered EV charging stations for urban environments.

This assessment was carried out through the use of a modified version of the IDART methodology, tailored for a non-invasive, checklist-based approach that is most suitable for smaller organizations with production-only systems. Furthermore, this evaluation was conducted with the framework of the NISTER 7621r1, outlining the best practices in cybersecurity for smaller businesses.

NOTABLE ASSESSMENT ACTIVITIES INCLUDE THE FOLLOWING:

- Review over NARO's documentation, going over network diagrams, device inventories, and access protocols.
- Orchestrating interviews with key personnel to gain a better understanding of workflows, system dependencies, and risk tolerance.
- Analysis of physical layouts, access controls, and network configurations.
- The identification of attack surfaces, evaluation of security controls, and mapping out potential risks based on how practical and impactful they are.

02 CONTINUED.

CRITICAL FINDINGS DURING THE EVALUATION:

- Physical Security Gaps - The administrative office remains unlocked during business hours, as well as the existence of a shared server room with a neighboring organization. Both of these are major red flags for potential insider threat risks.
- IT GGovernance Limitations - NARO lacks an internal IT department with heavy reliance on external support. This is troublesome during times where rapid management is needed.
- Infrastructure Weaknesses - Automatic system updates occur without a staging environment which leads to an increased risk of untested changes that could impact production systems.
- Network Concerns - Guest wireless network does not require a password, leading to unnecessary exposure risks.
- Device-Level Risks - Employees are allowed to install software freely, vague policies regarding USB device usage and system logging.

IDENTIFIED STRENGTHS:

- The use of VPNs and encrypted transfer methods for remote work and lab data handling.
- Segregated Wi-Fi networks with MAC filtering business wise.
- Dedicated workstations for EV data interfacing with secure lab workflows.
- Basic physical access controls such as keypad locks and proximity badges in engineering building.

02 CONTINUED.

WHAT THIS PROVIDES:

Our goal for this assessment is to reduce risk exposure for NARO, strengthening their security posture. By understanding the flaws that are visible in NAROs cybersecurity sector, we are able to provide a groundwork of specialized recommendations that will not only strengthen security, but also allow for NARO to maintain operational by balancing our cybersecurity improvement efforts with possible resource constraints.

We would like to extend our sincerest thank yous to NARO, Inc. for their cooperation, transparency, and consistent dedication throughout this process. Your commitment towards improving security efforts is commendable; we are ever grateful for the opportunity to support your cybersecurity journey.

03

INTRODUCTION

Background

WHAT IS THE PURPOSE OF THIS ASSESSMENT?

NARO, Inc. (NARO) has many concerns over their cybersecurity measures after a known data breach that has been going around in the [state county] area. Many organizations like AOTIR, Inc. (Another Organization That Isn't Real) around the area have been suffering from breaches to their employers data, putting many in harm's way. NARO, Inc. has decided to take precautions by conducting a cybersecurity assessment.

Scope

This section will include what is being done in this assessment and the limitations to the assessment.

Report Organization

Section 4 will provide an overview of NARO's systems and facilities. Section 5 - 6 will go deeper into Section 4 by going over the technical infrastructure of NARO as well as the IT support and limitations currently at their disposal. Sections 7 - 10 describe the methodology used by the team. Section 11 - 13 showcase the activities that were conducted by the team and the result of those activities. Appendices will include more additional information related to the assessment.

04

SYSTEM OVERVIEW/DESCRIPTION

The Cybersecurity assessment focuses on the operational and technical infrastructure of NARO, Inc., a small non-profit organization specializing in R&D for renewable energy technologies. NARO's core project involves the development of a miniature, solar powered EV charging system optimized for installation in compact urban spaces, such as apartment complex parking lots.

To support this work, NARO maintains distinct administrative and engineering divisions, each with its own operational needs and system dependencies. While the organization is modest in size, its technical infrastructure supports advanced R&D activities involving both hazardous materials and remote collaboration, making security posture a critical concern.

Facilities and Operations

NARO operates from two office spaces in a research park in San Antonio, Texas:

- The Engineering facility houses cubicle workspaces, lab testing areas, hazmat storage, and vehicle bays for charger integration.
- The Administrative Office is located across a parking lot and shares common spaces including the server room, with a neighboring business, Geological Analysis and Surveying (GAS).

The engineering space includes physical controls like proximity cards, keypad locks, and secure bays with 24/7 restricted access. In contrast, the administrative office remains unlocked during business hours to accommodate investors and construction activities, with operational magnetic lock control via reception.

05

TECHNICAL INFRASTRUCTURE

System Architecture

END USER DEVICES

- **Laptops:** All employees are issued Windows laptops with VPN software and Office 365 pre-installed. These laptops are configured with network drive mappings to internal file servers.
- **Workstations:** High-powered, stationary workstations in the vehicle bays are used to interface directly with EV's, leveraging expansion cards incompatible with mobile devices.
- **Lab Devices:** A mix of Linux and Windows laptops is used in R&D labs; these systems are not domain-joined and rely on local accounts. Secure file transfers to administrative servers are conducted using SHH/SCP/rsync.
- **Mac Systems:** One Mac laptop, used by the hazmat engineer, is connected to the domain via terminal wireless network.

05 CONTINUED.

Server Infrastructure

NARO MAINTAINS 17 SERVERS HOUSED IN A SHARED SERVER ROOM:

- 5 Dell PowerEdge R940 servers run Windows Server 2019 and provide domain services, file sharing via OneDrive (on-prem), and email.
- 12 Supermicro A+ SuperServers run Ubuntu 18.04 LTS and are used exclusively for research data processing and storage.
- Each server rack has a dedicated workstation and network KVM switch. Physical access is shared with GAS personnel, posing a potential security risk.

Networking

- Wireless Networks: Two wireless SSIDs are deployed: a secure, MAC-filtered business network, and an open guest network
- Bridge Networks: Directional antennas on both buildings from a bridged network backbone using Ethernet over wireless, connecting the admin and engineering environments.
- VPN Access: Remote work is facilitated via VPN using domain credentials, with secure access to email and files through Outlook.com and OneDrive.

06

OPERATIONAL CONSTRAINTS AND SECURITY CONSIDERATIONS

IT Support and Limitations

NARO LACKS A DEDICATED IT TEAM. ALL SERVICES ARE OUTSOURCED TO PROMPT IT ASSISTANCE (PITA), WHICH HANDLES:

- Bi-monthly maintenance and software updated
- Remote troubleshooting via TeamViewer
- Emergency support as required

Operational Constraints and Security Considerations

- **Production-Only Systems:** All IT systems are live; there is no staging environment for safe testing or experimentation.
- **Shared Server Room:** Introduces concerns around physical access control and data confidentiality.
- **Hazmat Handling:** Requires stringent data management and system reliability protocols.

07

ASSESSMENT METHODOLOGY

This cybersecurity assessment follows a modified form of IDART Methodology, originally developed by Sandia National Laboratories (*"IDARTTM." CASA, 2025)*. While IDART typically supports adversarial, red-team exercises, this version has been adapted for a non-invasive, paper-based assessment consistent with NARO's operational limitations.

The adapted methodology preserves IDART's structured approach while avoiding any active testing that could compromise production systems. It is designed to identify vulnerabilities, assess risk, and support realistic mitigation planning for small organizations with resource constraints. Following the use of the IDART, we will also follow the assessment framework for industry standards, this includes the NIST.IR.7621r1, to guide the evaluation of NARO's systems and controls (*Small Business Information Security: The Fundamentals*, Oct. 2016*)*.

07 CONTINUED.

Overview of IDART Methodology

The modified IDART methodology includes the following five core phases each of which has been tailored to NARO's context:

Methodology Phases

PLANNING

This phase includes:

- Initial engagement with NARO's leadership to understand goals and constraints.
- Development of a project timeline, stakeholder contacts, milestones, and communication protocol.
- Establishment of boundaries and rules of engagement (e.g., no network scanning or penetration testing).

08

DATA COLLECTION

During this phase:

- System documentation (e.g., network diagrams, software inventories, user roles) is reviewed.
- Interviews are conducted with key personnel, including William Donaldson III.
- Organizational context and risk tolerance are assessed.

The data collection phase helps identify critical business operations, system dependencies, and areas of concern.

Characterization

This phase condenses raw data into critical system “views,” such as:

- Physical layout and network segmentation
- User access flows
- Remote access configurations
- Shared space vulnerabilities

These views clarify how systems function in practice, which may differ from how they are documented or intended to operate.

08 CONTINUED.

Analysis

This step applies technical and contextual knowledge to:

- Identify high-value targets and attack surfaces
- Map theoretical attack paths (e.g. VPN entry points, shared server room misuse)
- Evaluate the strength of controls across administrative, physical, and technical domains

Each potential weakness is assessed based on feasibility, impact, and the presence (or absence) of mitigations.

09

REPORTING

The final phase includes:

- Compilation of findings into an actionable assessment report
- Recommendations prioritized by impact and complexity
- Delivery of an executive summary and technical appendix
- An Out-Brief session to discuss key risks, proposed mitigations, and next steps

10

ASSESSMENT ACTIVITIES

Death Star Consulting performed an audit over the following critical areas according to the key principles of the NISTIR 7621 Small Business Information Security Framework.

NARO DOCUMENT OVERVIEW

Death Star Consulting studied the current overview of NARO Inc.'s cybersecurity policies and compared them to the NISTIR 7621 standard of best practices for small businesses. This overview provided detailed information on NARO's current employee and departmental makeup, workstation and laptop use, remote access and server policies, as well as wireless technologies and IT Support capabilities.

11

ASSESSMENT RESULTS AND RECOMMENDATIONS (WEAKNESSES, STRENGTHS, AND OBSERVATIONS)

WEAKNESSES

- Laptops (Medium) - Employees can install any additional software – such as Matlab – on their systems.
- Laptops (Low) - The Hazmat Engineer only has WiFi access. This can be useful for workers that are mobile, but WiFi is not as reliable as ethernet.
- Wireless (High) - guest network does not require a password. (Guest WiFi should still have a password to ensure non guests do not abuse the service).
- IT Support (Medium) - There is no IT support on premises at Naro.
- Physical Spaces (High) - The Administrative building being left unsecure during business hours leaves sensitive areas exposed.
- Physical Spaces (High) - The shared Server room with GAS creates the opportunity for an insider threat to conduct malicious activity.

11 CONTINUED.

OBSERVATIONS

- IT Support (Low) - All of the systems have been configured to automatically update as necessary. (This can be good for workstations, but bad for servers to automatically update without testing first)
- Server Room and Physical Office Spaces (Medium) - Does not mention the use of access logs or surveillance technologies
- Server Room (Low) - There is no specification on the use of uninterrupted power supplies (UPSs)
- Laptops (High) - No mention of USB policy outlining whether they are restricted or monitored
- Wireless (Medium)- There is not any information regarding intrusion detection systems or certificate based authentication.

STRENGTHS

- Laptops - All employees have their own accounts for the Windows Domain (Makes it easier to track user activity)
- Laptops – Non domain accounts for engineering lab use SSH, secure copy (scp), or rsync to transfer research data from the labs to the NARO servers (use of encryption for data in-transit
- Laptops - To allow for flexibility in working remotely, NARO provides every employee with a Windows laptop with VPN software (Encryption of data in transit from outside the network. Also gives employees access to internal servers from an outside network)

11 CONTINUED.

- Wireless - wireless network is split into 2 parts – the NARO business network; and the NARO guest network. (Separation of traffic)
- Wireless - business network requires authentication, and applies MAC address filtering (Authentication, plus MAC filtering can ensure that only allowed devices are on the network. For such a small company I would like to see the use of certificates, but MAC filtering is better than nothing)
- Server Room - has the power and cooling necessary for multiple server racks. (Mentions power, but not the use of UPSs)
- Server Room – Separate KVM for NARO and GAS.
- Server Room - NARO and GAS are on separate networks
- Remote Access - The use of VPNs for laptops to access internal servers.
- Workstations - The use of dedicated workstations in the vehicle bays allows for specialized data capture from electronic vehicles (EVs).
- Physical Office Spaces - The use of badges and PIN access in order to access sensitive areas.

12

CONCLUSIONS

After reviewing Naro's financial ratios, we've gained some valuable insights into its current financial health This shows us how efficiently it's operating. The liquidity ratios covered shows how well the organization can handle short-term responsibilities like bills. The Profitability ratios continued to explain how efficient it is at generating income from its given activities as well. In culmination, it's apparent that certain ratios fall within healthy industry standards, while others identify areas that need more attention. The results clearly portray where organizations position themselves financially and can aid us in making smarter decisions moving forward. It's of utmost importance to perceive these ratios in a context associated with their general surroundings and follow them over time to truly understand the core tenants of progress, risks, and trends.

13

APPENDICES (INCLUDES ALL ADDITIONAL INFORMATION, DATA COLLECTION REFERENCES/RESULTS, OTHER VIEWS AND ATTACK GRAPHS, ETC.)

"IDARTTM." *CASA*, 2025, casa.sandia.gov/idart/

Paulsen, Celia, and Patricia Toth. "Small Business Information Security: The Fundamentals." *Small Business Information Security: The Fundamentals*, Oct. 2016, nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf, https://doi.org/10.6028/nist.ir.7621r1.

Schumacher, R. and Lowry, S. (2010), (NISTIR 7742) Customized Common Industry Format Template for Electronic Health Record Usability Testing, NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.IR.7742, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=907312 (Accessed July 18, 2025)