BY BYTEMUNCHERS CYBER GROUP: KHOA NGUYEN, ISSAC, RONALD DEWEES

NARO, INC OUT-BRIEF REPORT PRESENTATION

BYTEMUNCHERS PROFILE

ByteMunchers is a cybersecurity company founded by Charles Swick with the goal of empowering small local businesses with advanced cybersecurity practices at a low and affordable cost.

Khoa Nguyen

Professional Cyber Detective

Isaac Caldera

Lead software Architect

Ronald

CEO

Background

With the recent increase in cyber incidents, including data breaches, NARO Inc. recognizes the need to assess its vulnerabilities to potential cyber incidents.

Our team, ByteMuncher, will aim to identify weaknesses in NARO's cybersecurity framework as we align with the NIST framework and recommend improvements.

SCOPE

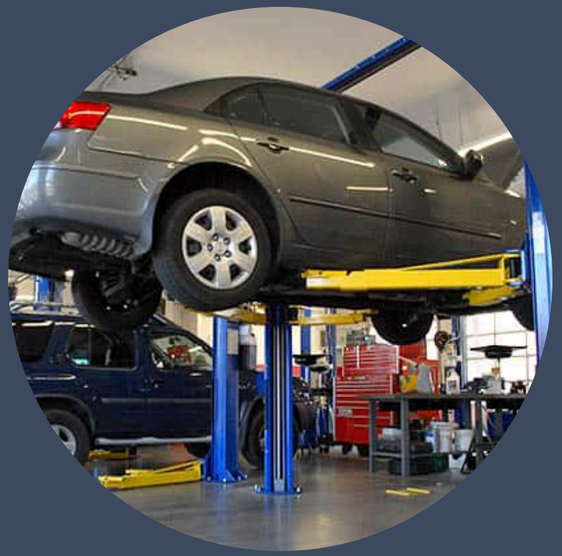
- Our assessment will analyze NARO’s security policies, focusing on management areas in general, security, software control, and data handling.
- We will then evaluate access based on the least privilege principle and review policies to reduce phishing risks.
- Vulnerabilities in physical and system security will also be assessed, but penetration testing will not be conducted due to its disruptive nature.

System Overview

- NARO's office consists of two main buildings, the Engineering and Management buildings.
- The NARO Engineering Building will serve as the central building designated for conducting production, research, design, and testing of technology.
- The administrative building handles paperwork, interacts with customers, and manages the overall information flow.

ENGINEER BUILDING

- **Office Space:** Workspace for engineers to handle documentation, analysis, design, and research.
- **Lab Space:** workplace for Testing and analysis for battery, solar, and EV technologies.
- **Hazmat Storage Area:** Stores hazardous materials for electric battery and solar panel manufacturing.
- **Vehicle Bays:** Conducts EV testing and charging system evaluations

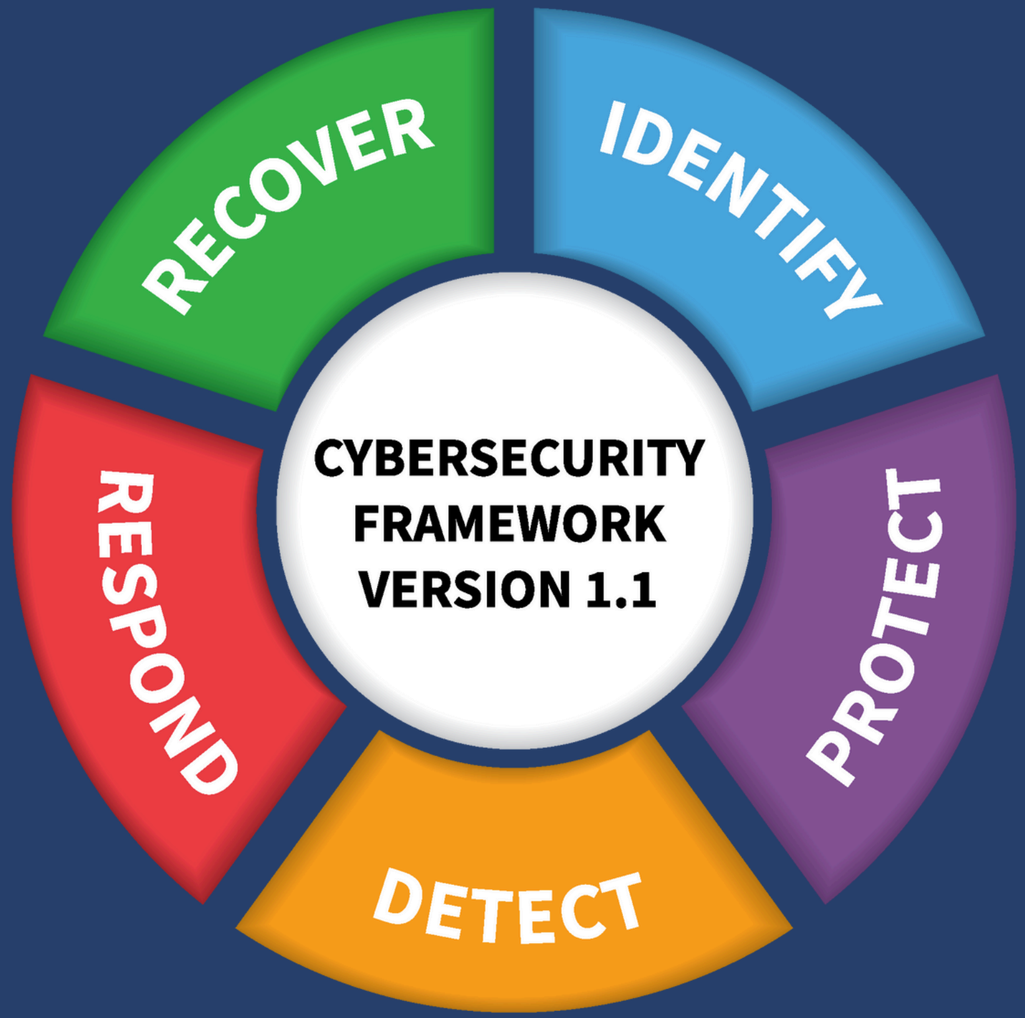


MANAGEMENT BUILDING

- **Office Space:** Workspace for staff handling grant writing, financial accounting, and sales.
- **Common Areas:** Includes **storage rooms**, **server room**, custodial areas, and kitchen, shared with GAS Company.
  - **Storage Room:** Stores documents, supplies, and spare equipment (e.g., laptops, workstations)
  - **Server room:** includes servers to store confidential documents, designs, and process data collected from experiments and prototypes in the Engineer Building

Assessment Activities

- Our team, group 4, will apply the NIST cyber security framework in assessing NARO.
- This framework will be tailored to align with the specific system needs and structure of NARO, including:
  - Risk Management
  - NARO Documentation Review
  - Scan of Hardware and Physical Security
  - CEO, Management, and Employee Interviews

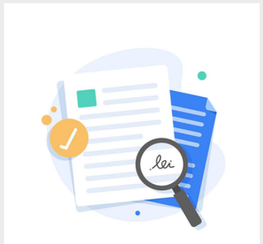


OTHER ACTIVITIES

Physical environment inspection

Backup data evaluation

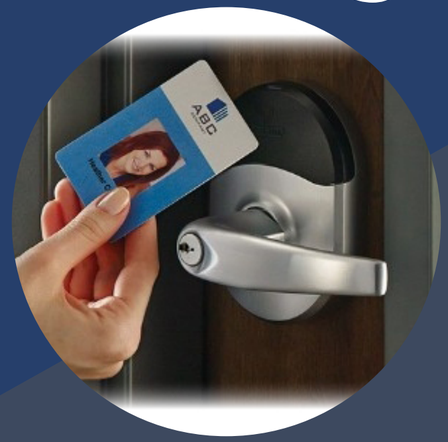
IT documents review



NARO Audit

Assessment Results: Strengths

Many things looked amazing!



- **Engineering Facility Security:** Proximity card access, keypad locks, and restricted hazmat areas ensured a very strong physical security at the site.

- **Automated Data Backup Procedures:** Occasionally, encrypted backups with hash verification prove very effective.

- **Cybersecurity Awareness Training:** Employees receiving regular training on phishing, strong passwords, and secure handling of sensitive information is masterfully done.

- **Segmentation of Networks:** Business and guest networks are segmented, with authentication to streamline security.

Assessment Results: Priority Weaknesses

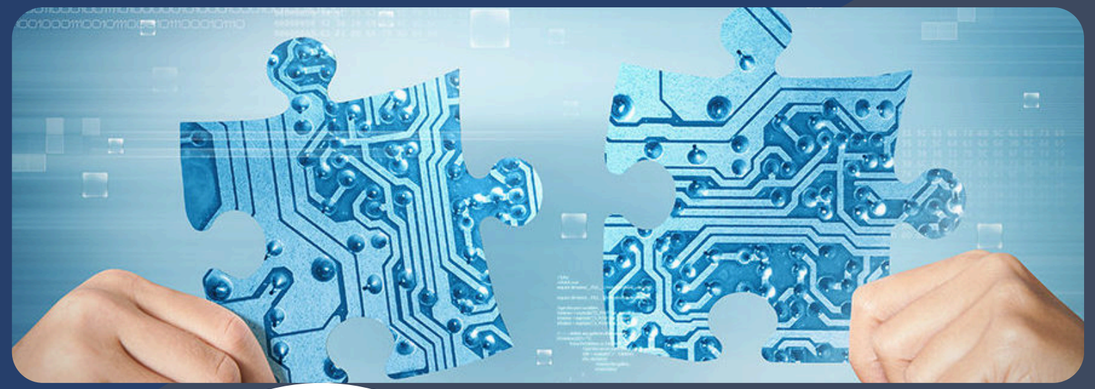
- **Remote Access via Personal Devices:** There is risk for allowing personal devices without enforced security policies to access the VPN.
  - **Mitigation**: Implementing a Mobile Device Management System and Multi-Factor Authentication.
- **Lack of Software Control on Company Device:** NARO does not have strict controls on the software downloaded on employees' work computers.
  - **Mitigation**: Enforce software restrictions on the company laptops
- **Environmental hazards in the Server room:** the bathroom located on the second floor of the administration building frequently has plumbing issues.
  - **Mitigation**: NARO should transfer servers' equipment to a safer location

Assessment Results: Additional Weaknesses

- **Unmanaged Lab Systems:** Some lab systems are not integrated into centralized management, leading to inconsistent security throughout processes.

- **Limited Incident Review Process:** NARO has experienced network issues stemming from phishing emails.

- **Guest Network Security:** There is open access with MAC filtering. This is insufficient against sophisticated threats. Adding password authentication and improving monitoring of these systems could improve security.



Assessment Results: Observations

Shared Server Room:
Physical proximity to GAS tenant increases risk. Maybe consider enhancing physical barriers or additional restrictions to combat this.

Hazmat Protocols:
Comprehensive safety protocols exist but are entirely paper-based. Digitizing these files would improve accessibility and regulatory compliance.

SSH Data Transfers in Labs:
Secure copy is used, but inconsistent configurations could introduce vulnerabilities in usage processes.

Conclusions

Our team found NARO’s focus on their engineering facilities' physical security and automated data backup significant. Although these measures show a commitment to protecting data and critical research, a deeper look revealed vulnerabilities in remote access policies, consistent physical security, and centralized management in lab systems. Addressing these vulnerabilities will ensure that NARO conducts secure its operations and intellectual property.

Through our cybersecurity assessment, we were able to highlight strengths and vulnerabilities in NARO, inc.’s current framework, providing a clear and beneficial path for future development. The next steps should prioritize remote access security along with a review of future physical access policies, additionally integrating the central domain would improve policy enforcement. ByteMunchers believes in NARO to proactively address these challenges, and BM stands ready to assist NARO with implementation along with future assessments. We thank the NARO staff for their cooperation and transparency throughout this process, and together, build a robust and resilient cybersecurity framework to safeguard NARO’s innovative research and operations.

Follow-on Activities

- **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.
- **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.
- **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.
- **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.
- **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.

THANK YOU

Let us know if you have any question

We look forward to more future cooperation with NARO