Project Out-Brief

NARO, INC

DAMIEN BELTRAN, HANNAH STANEK, ISAIAH ALVAREZ, WES GAUSE

CS-3113-01T
Course Project
Cybersecurity Assessment for NARO Inc.

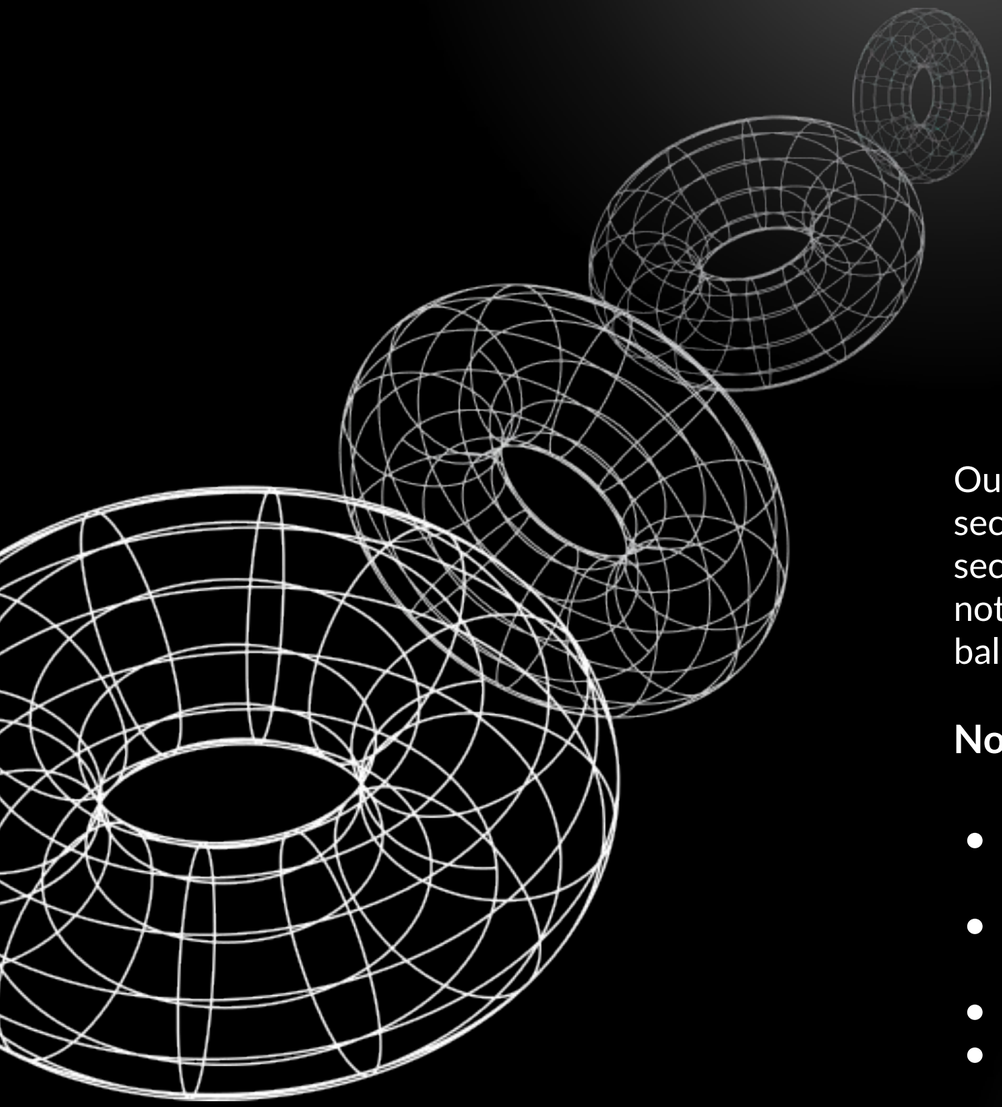
TEAM INTRODUCTION

HANNAH STANEK

DAMIEN

ISAIAH ALVAREZ

WES GAUSE



BACKGROUND AND SCOPE

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.

Notable assessment activities include the following:

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

No active penetration testing was done to verify possible vulnerabilities in a system.

SYSTEM/ORGANIZATION DESCRIPTION

System Overview

- NARO, Inc. is a small non-profit focused on renewable energy R&D, specifically the development of compact solar-powered EV systems for urban environments.

Technical Infrastructure

- Staff are equipped with Windows laptops using VPN and Office 365.
- Secure file transfers are used in R&D labs (SSH, SCP).
- Servers are split between Dell and Supermicro.

Support Model

- NARO outsources all IT services to a third party provider (PITA), with no internal IT staff on site.

Security Posture Strengths

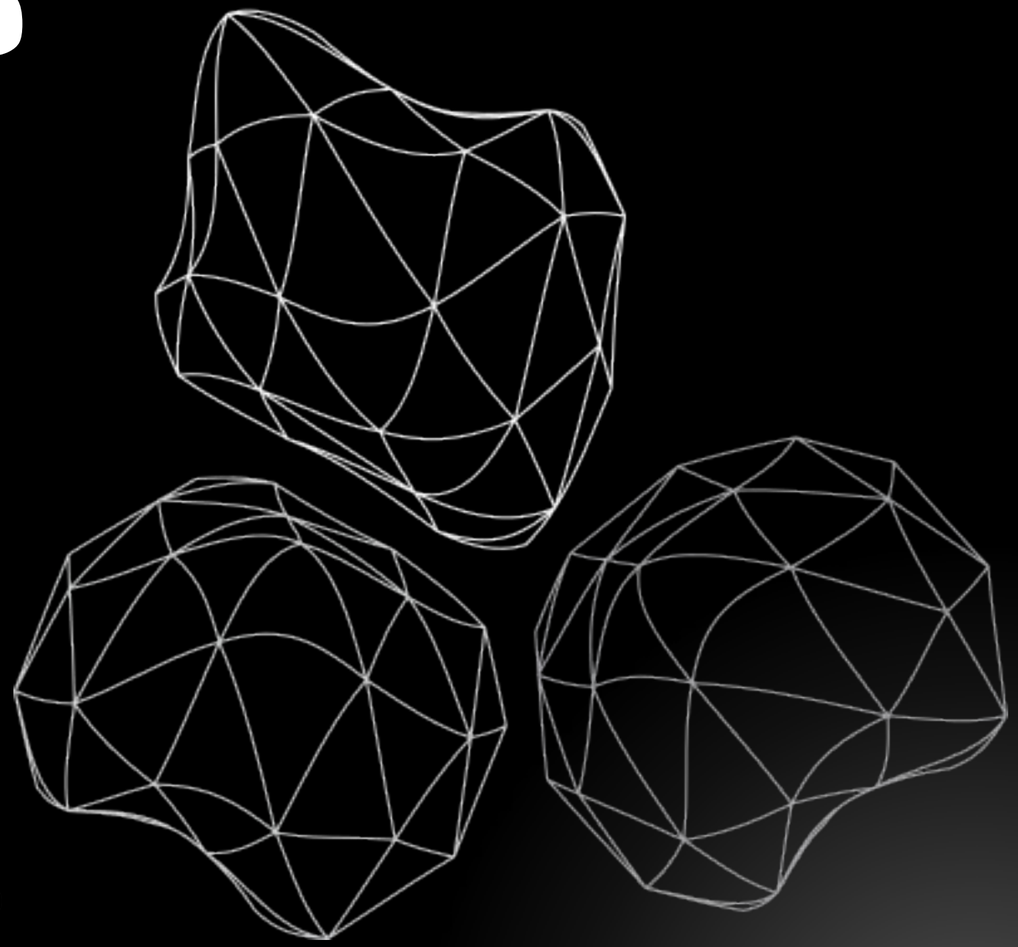
- Encrypted remote access (VPN), segmented networks, and secure lab workflows.
- Use of MAC filtering and user specific Windows domain accounts.

Security Gaps Observed

- Weak physical access control at the admin building.
- Open Wi-Fi increases network exposure.
- Lack of Formal policies on USB devices or software installation.
- No staging environment for testing updates before deployment.

ASSESSMENT ACTIVITIES

- Reviewed company overview provided by NARO
- Compared practices to NISTIR 7621 (Small Business Cybersecurity Framework)
- Analyzed policies on:
  - Workstations and laptops
  - Remote access and VPN
  - Wireless and physical security
  - IT support and server infrastructure
- Reviewed internal documentation provided by NARO



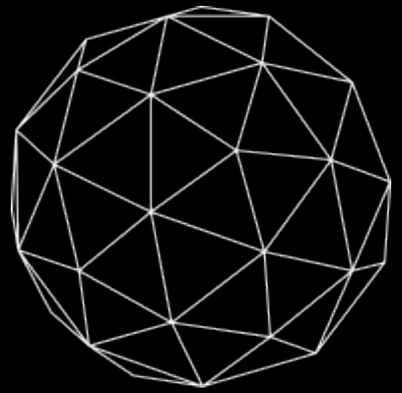
ASSESSMENT RESULTS

Strengths	Weaknesses
VPN and encryptions used for remote connections	Guest WiFi currently has no password. Adding one would help protect against unauthorized access.
Workstations kept up to date	Employees are able to install their own software. Implementing software approval policies could reduce risk.
Segmented wireless network with MAC address filtering	Some physical areas are left unsecured during business hours. Introducing stricter access controls could prevent unauthorized entry.
Use of badges and PIN to access sensitive areas	The server room is shared with another entity. Separating access could reduce the potential of an insider threat.
	No clear USB usage policy exists. Defining clear USB guidelines would strengthen endpoint security.

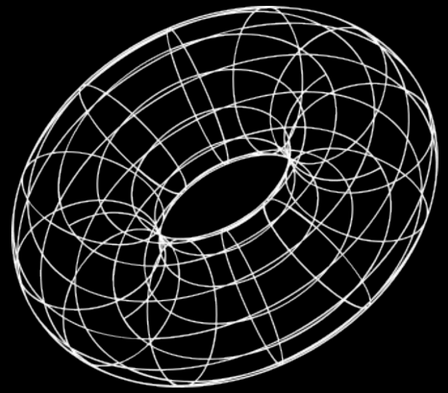
CONCLUSION

- Financial ratios offer insight into NARO’s current health
- Liquidity shows ability to cover short-term needs
- Profitability reflects income efficiency
- Some ratios are strong; others need attention
- Results support smarter planning and strategy
- Context and long-term tracking are key

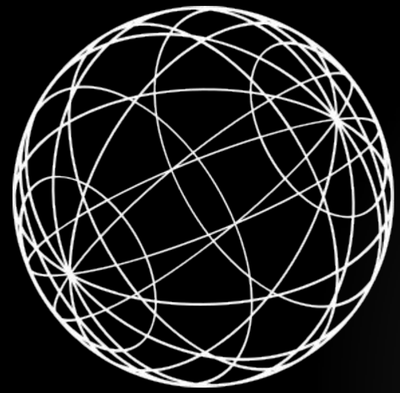
FOLLOW UP ACTIVITIES



Launch Phishing Awareness Campaign



Annual Cybersecurity Training



Keep Software Updated

THANK YOU

LET US KNOW OF ANY

QUESTIONS!