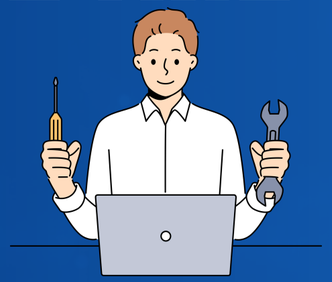
Group 4

IN BRIEF PRESENTATION

WHO WE ARE

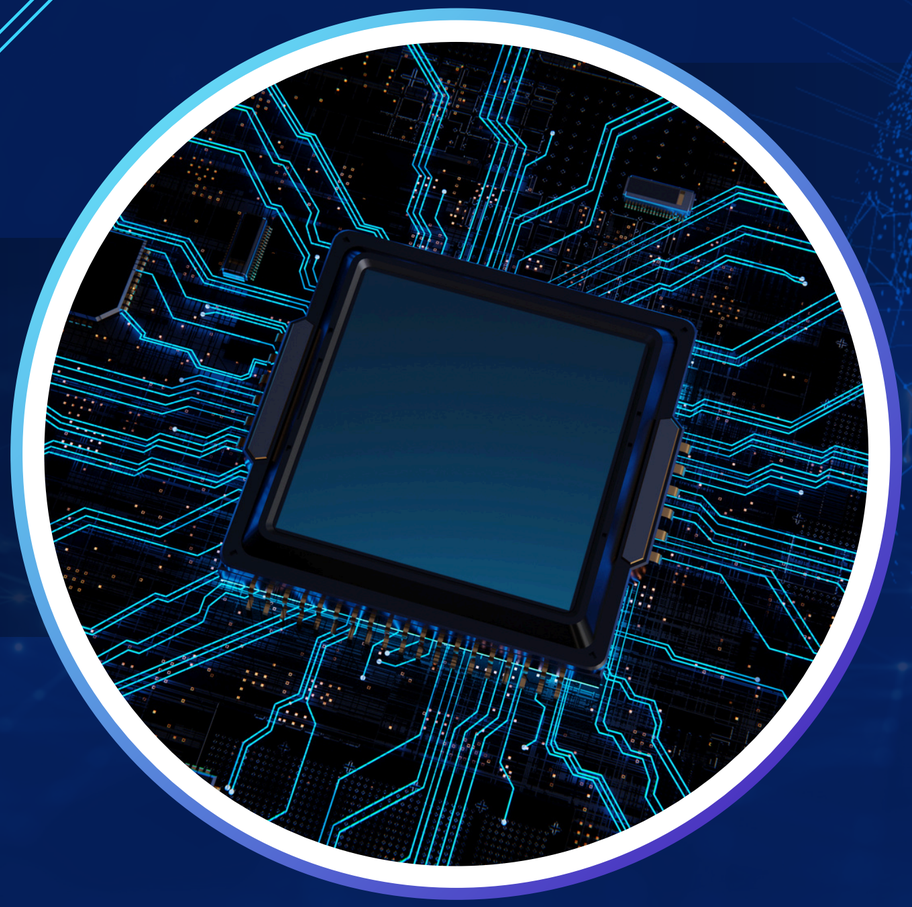
Charles Swick

Khoa Nguyen



Isaac Caldera

Ronald Dewees



WHY WE ARE HERE

- Upon researching NARO and realizing the need to set up an emergency security system, we believe that our company can meet that need and establish a defense system as well as a solid framework for the company's network security.

- We will first conduct thorough analysis on the weaknesses and strengths of NARO’s current cybersecurity posture, and find areas where it can be improved, if any, and help implement policy changes where necessary.

WHAT WE WILL BE DOING

- A full assessment using our audit checklist of your organization's security and related policies. This will be conducted from multiple angles including , but not limited to, physical access, wireless security, and best practices adherence for both customer and internal business data handling.
- We will do an exhaustive scan of all devices on all networks (excluding guest devices) in order to gather information about potential vulnerabilities. We will also look at physical security (door access, etc) and policies.
- Upon completion of the assessment you will receive an exhaustive report containing our findings and their potential impact (severity), as well as our recommendations for mitigations (where applicable), and an Out-Brief presentation.

WHAT WE WILL NOT BE DOING

- Penetration testing - This is an incredibly invasive, albeit thorough, assessment process that simulates an active threat scenario. This would inevitably cause disruptions to NARO's operations and, as such, will not be conducted.

WHAT IS A CYBER SECURITY ASSESSMENT?

Discovery

Thoroughly examining your organization’s security and related policies, and identifying potential vulnerabilities so that they can be mitigated before someone has the chance to exploit them. This saves you and your employees (and customers) time, money, and headache.

Training

Using the information obtained during the assessment to create or update policies and training for employees in order encourage good security practices at an organizational level.

OUR FRAMEWORK

UPDATED NISTIR

We base our approach on an updated version of the NISTIR fundamentals that covers **modern platforms, threats, and physical security**.
It also makes some of the more technical details available so there's less guesswork and outside hiring required.

THE FRAMEWORK

Identify

Accessing company's working environment and potential cybersecurity risks, in order to have a clear understanding of the risks involved and potential sources.

Recover

The final steps goal is to resume normal work flow by establishing backups of data how to deal with the disasters and data breaches.

Detect

Mainly revolves around the ability to detect information security or cybersecurity events.

Protect

Focus on establishing safeguards against cybersecurity issues for confidentiality and limit access of data.

Respond

This is the plan of action when disaster strikes with key roles laid out for a organized solution.

RISK MANAGEMENT

Risk Assessments

Ensuring that you are aware of the risks is the first step toward avoiding them. Nobody can predict the future, but regular risk assessments can at least plan for the present.

Policy Development

Developing effective S.O.P's for employees to adhere to based on risks is the first line of defense. Intelligent policies and proper training can stop a risk from becoming a real threat.

OUT BRIEF

Assessment and Reporting

During the assessment, our team will document the process in each phase. A detailed final report will be prepared and presented to NARO leadership regarding the vulnerabilities and security risks found along with the solutions.

Remediation for these vulnerabilities

Our engineers will directly remove any critical vulnerabilities only with full approval from NARO leadership and management

Collaboration with IT provider on updates

We will collaborate with your IT provider to ensure that these solutions are properly integrated with your current system smoothly without disrupting the production

Group 4

THANK YOU FOR YOUR ATTENTION

If you have any questions,
feel free to ask!!

END

In Brief