Cybersecurity Risk Assessment

ShieldNet Cybersecurity

The Team

HUNTER HOCH

Workstations and the physical office

GRANT PETRI

Servers and IT support

PRICE HILLER

Wireless and remote access

MATTHEW HERNANDEZ

Server room and company laptops

Background and Scope

1 NARO'S SOLAR ENERGY TECHNOLOGIES

ShieldNet was contacted to undertake a cybersecurity assessment in the wake of increasing scrutiny from the DOE's EERE surrounding NARO's solar energy technologies.

2 THE ASSESSMENT

ShieldNet was given a white-box perspective of NARO to conduct its assessment on offices, equipment, and digital infrastructure. ShieldNet did not conduct system attacks but phishing was done to test NARO employees.

System/Organization Description

NARO has **significant** room for improvement, including some severe vulnerabilities:

- SERVER ROOM SHARING/INSECURITY
- EMAIL PHISHING
- INSECURE FILE TRANSFER PROTOCOL USE
- FREEDOM OF USER APPLICATIONS ON EMPLOYEE DEVICES

NARO's current policies are updated annually, but **lack comprehensiveness.**

NARO provides insufficient training that leaves liabilities for the company when uninformed employees act with little information.

Assessment Activities

WHAT WE WERE GIVEN

ShieldNet was provided with an Overview of NARO’s operational environment. NARO also filled out an Audit Checklist to help evaluate their current cybersecurity standard at an objective level. All of this was provided by William Donaldson III, and shaped ShieldNet’s approach to the assessment.

HOW WE ACTED

In addition to reviewing the documents to find vulnerabilities, ShieldNet conducted an email phishing campaign on NARO employees.

No identifiable, personal, or organizational information was obtained through the campaign.

SHIELDNET'S

Assessment Results

Strengths

INTERIOR PADLOCKS

Interior padlocks to the vehicle bay exterior door makes the engineering building very secure from unauthorized access

Strengths

MAC FILTERING

The business network utilizes MAC filtering which helps ensure unauthenticated users do not get access without a NARO device

Strengths

UNIFIED SOFTWARE

All employees are under unified software licensing through Office 365, reducing incompatibilities and increasing collaborative efficiency

Strengths

LAPTOPS

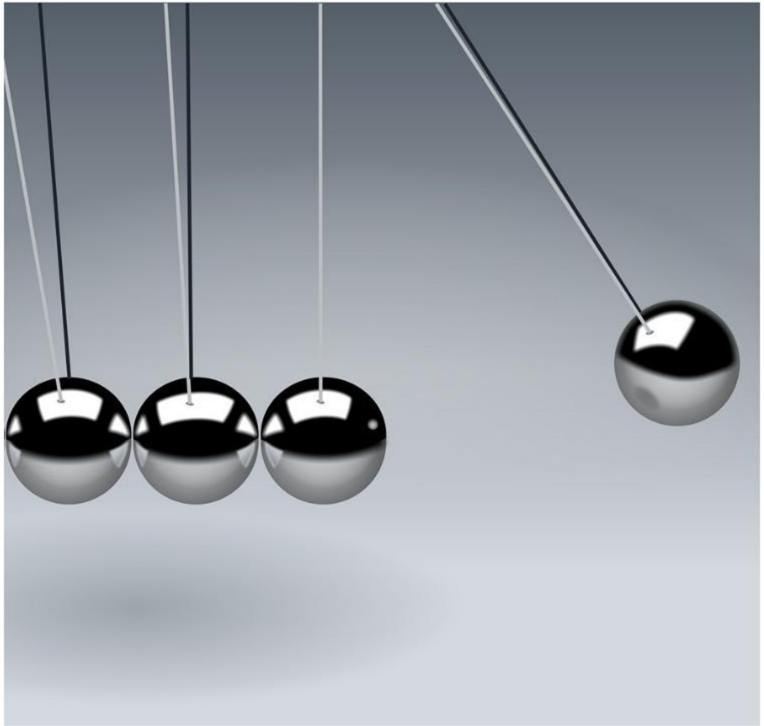
NARO utilizes laptops over desktops providing flexibility for employees to be able to work remotely or move offices

Strengths

POLICIES

Cybersecurity policies are updated within an acceptable time frame

Weaknesses



NARO AND GAS SHARE SERVER ROOMS

RISK: SEVERE

The security of NARO and GAS is dependent on either's ability to maintain the security of the space.

Physical hard drives are accessible to both NARO and GAS

Weaknesses

PITA USES FILE TRANSFER PROTOCOL

RISK: SEVERE

PITA's backup procedure utilizes File Transfer Protocol (FTP). FTP is a known insecure protocol for copying files remotely, interceptable by "Man in the Middle" attacks.

Weaknesses

NARO ALLOWS ANY EMPLOYEE TO INSTALL SOFTWARE

RISK: SEVERE

All employees can install software onto NARO devices without prior authorization.

Some employees may not understand what is safe to download.

Weaknesses

NARO DOES NOT MAINTAIN A 3-2-1 BACKUP SOLUTION

RISK: HIGH

While PITA is primarily responsible for NARO’s backups, NARO should implement the 3-2-1 backup policy on its own.

Weaknesses

END-OF-LIFE OPERATING SYSTEMS

RISK: HIGH

All servers are running end-of-life (EOL) software.

NARO should consider upgrading this software, or contact the manufacturers to get support extended.

Weaknesses

EXTERIOR DOORS ARE LEFT UNLOCKED OUTSIDE BUSINESS HOURS

RISK: MODERATE

Combined with the magnetic lock override at the reception desk, unauthorized access into NARO’s administrative office is possible.

Weaknesses

PITA HAS UNSUPERVISED ACCESS TO "ALL SYSTEMS" IN THE NARO NETWORK

RISK: MODERATE

While PITA is a trusted IT source, actions performed by their organization should be logged and monitored by a NARO employee(s).

Weaknesses

NETWORK DEVICES ARE UPDATED ONLY WHEN CRITICAL ISSUES OCCUR

RISK: MODERATE

Critical patches should be installed as soon as they’re available, for optimal security/reliability.

Weaknesses

NO PHISHING EMAIL TRAINING IS CONDUCTED

RISK: MODERATE

Phishing is a major attack vector.

Phishing training can help prevent phishing incidents.

Weaknesses

SWITCHES AT END-OF-LIFE

RISK: MODERATE

The *Netgear ProSafe JGS524 Gigabit* switch is end-of-life.

This EOL network switch should be replaced with one that has ongoing security support

Weaknesses

ENGINEERING LAB SYSTEMS ARE OUTSIDE OF NARO DOMAIN

RISK: MODERATE

The systems in the engineering lab are outside of NARO's Windows Domain, but can access NARO's confidential information.

These systems should be peered with Windows Domain if possible, to ensure ease of protection.

Weaknesses

UNCLEAR IF NARO DEVICES CAN ACCESS NARO DATA ON GUEST NETWORK

RISK: LOW

If NARO confidential information cannot be accessed on the guest network, it is not a weakness. However, if the opposite is true, it should be made either impossible or require a tunnel like a Virtual Private Network (VPN) to access on the guest network.

Weaknesses

CYBERSECURITY POLICES ARE "NOT COMPREHENSIVE"

RISK: LOW

Non-comprehensive policy can lead to confusion and risk among employees.

Clear and concise cybersecurity policies reduce ambiguity and improve employee/employer confidence

Observations

WORKSTATIONS

No workstations are present in the administrative office

Laptops could still be accessed/stolen if left behind by employees

NARO should encourage employees to keep laptops on their person or provide a place to lock them in the administrative office

ENVIRONMENT MONITORING

NARO utilizes few resources for monitoring important areas and actions

The server room lacks hardware responsible for tracking temperature and humidity. Adding these could provide potentially disaster-preventing information to IT staff.

Conclusions

Conclusions

While NARO is a fairly secure organization, it can take **key steps** to further protect itself from attacks, including:

- **ACCESS**

  Providing minimum required access to their organization's resources and facilities.

- **MONITORING**

  Closely monitoring actions performed by external IT sources, such as PITA.

- **TRAINING**

  Implementing frequent cybersecurity training to help employees identify and prevent phishing schemes

- **LEAKS**

  Locking down workstations and employee devices to prevent information leakage caused by employee installed applications

Follow-Up Activities

1 Improve employee cybersecurity training to help prevent phishing attacks

2 Investigate post-EOL support for outdated equipment, or replace EOL equipment that is no longer receiving security patches

3 Reevaluate cybersecurity policy and employ the property of Least Privilege wherever possible

4 Ensure backups (or all physical storage of information) is encrypted, so even if the physical possession of data is compromised, the organization and its data can be protected.

Trainings should be conducted every **3-6 months**, with a cybersecurity audit performed **annually**.

Thank you

QUESTIONS?