Out-brief Presentation Notes

Team Introduction:

- Team names and overview of our organization
- Each team member can introduce themselves (Keep in mind this can just be done in text, since we aren't actually presenting)
    - We have been hired for the purpose of conducting a cybersecurity assessment on NARO, Inc. Among the team is Hunter who investigated vulnerabilities regarding workstations and the physical office space, Grant who was responsible for handling reporting on servers and IT support, Price who's domain was wireless and remote access, and Matthew who investigated the server room and the company's laptops.

Background and Scope:

- Include reasoning for the assessment
    - "Cybersecurity threats have been expanding targets to include energy infrastructure and energy research companies. As a result, the Department of Energy's (DOE) Office of Energy Efficiency and Renewable Energy (EERE) delivered a report to congress in May of 2021 to improve cybersecurity among energy companies. Due to this, NARO, Inc. (NARO) contracted with ShieldNet to undertake a cybersecurity assessment in the wake of increasing scrutiny from the DOE's EERE surrounding NARO's solar energy technologies."

- Brief description of what major stuff was evaluated, and what major stuff wasn't
    - ShieldNet was given a white-box perspective of NARO to conduct its assessment, which included detailed information about NARO's offices, equipment, and digital infrastructure. ShieldNet did not conduct system attacks, such as penetration testing. ShieldNet's most significant assessment methodology was phishing, used to test NARO employees' susceptibility to the tactic.

System/Organization Description :

- Describe the state of the organization and our findings
    - NARO is overall a secure organization, but has significant room for improvement. ShieldNet found vulnerabilities in both its physical and digital environments. Some severe vulnerabilities include:
        - Server room sharing/insecurity
        - Insecure File Transfer Protocol Use
        - Email Phishing
        - Allowing freedom of user applications on employee devices
- **ALSO** This section should be providing context on what NARO's cybersecurity policies look like at the time of the assessment
    - At the time of this assessment, NARO's cybersecurity policies are updated annually, but lack comprehensiveness. NARO provides an insufficient amount of vital training that should be conducted, like detecting email phishing. This causes possible liabilities to NARO through the actions of uninformed employees.

- This slide serves as context to weaknesses. It shouldn't be overfilled with text, but should justify what we found to be weaknesses
    - All of the listed weaknesses threaten NARO's Information Confidentiality, Integrity, and Availability.

Assessment Activities:

- This should include our use of NARO's overview, audit checklist and additional information (probably should name drop William Donaldson III)
    - 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 our approach
- Doesn't need to be very detailed, but should confidently state what we used to evaluate NARO
    - In addition to reviewing the documents to find vulnerabilities, ShieldNet conducted an email phishing campaign against NARO employees. No identifiable, personal, or organizational information was obtained through the campaign. It was conducted simply as a means to see how effective phishing would be as an attack vector.

Assessment Results (Meat of the presentation):

- Strengths/Weaknesses/Observations

  - **Include Strengths!** It’s important the organization knows *what they are doing right*
  - Prioritize high severity weaknesses over low severity.
  - Include all findings. They don't have to be super detailed, but they all must be present
- The information here will help form our conclusions page
- After our investigation, we have found some strengths and weaknesses present in the performance of NARO Inc.:
  - **Strengths:**
  - Interior padlocks to the vehicle bay exterior door makes the engineering building very secure from unauthorized access. A simple component of this security is that the locks to the vehicle bays’ overhead doors are located on the interior of the vehicle bay. This prevents attackers from using simple destructive means to break the locks and gain access to the vehicle bay
  - The business network utilizes MAC filtering which helps ensure unauthenticated users do not get access without a NARO device. This also helps to log attacker attempts to infiltrate the network when on premises.
  - All employees are under unified software licensing through Office 365 which keeps incompatibilities to a minimum and increases collaborative efficiency.
  - NARO utilizes laptops over desktops which provides a flexibility for employees to be able to work remotely or move offices if need be. This helps maintain productivity and allows for adaptability.
  - Cybersecurity policies are updated within an acceptable time frame.

- **Weaknesses:**
- The external doors to the building housing the administrative office are left unlocked because of the “off-hour” work nature of the construction crew renovating the second floor. While on its own, this wouldn’t be a significant threat to the administrative office’s security, the reception desk has a button which disables the magnetic locks to NARO’s administrative office. Assuming the reception desk is not manned outside of typical business hours, the unlocked doors and reception bypass button could be utilized by a bad actor to grant unauthorized access into NARO’s administrative office.
- NARO and GAS sharing the first floor also means they share a server room. If either organization fails to maintain the security of this space, both of their servers are at risk. Additionally, NARO keeps hard drives with unencrypted backup data in the server room. Even if these are under lock and key, if anyone were to possess those drives, any and all data on them would be easily accessible.
- File Transfer Protocol (FTP) is a known insecure protocol for copying files remotely. The FTP login can be intercepted via a Man in the Middle Attack during the login phase and during any file transfer procedures. This means an attacker can reuse the intercepted FTP credentials to login to the PITA servers and copy, modify, or destroy sensitive proprietary information.
- NARO seems to be mostly unaware of the actions of PITA which is dangerous due to the nature of PITA’s access to NARO’s systems. More specifically, it seems PITA has complete unattended access of NARO’s systems via TeamViewer, and with that access, they can remotely access all of NARO’s systems with high level

permissions. Any individual with access to PITA's systems, or even to just a particular desk at PITA, would then have access to all systems under the NARO company.

- PITA patches network devices during visits for critical issues only. If any network device were to have a vulnerability between these visits, NARO would be open to attacks to their network
- The guest network is a clear target for malicious actors who may conduct scans and attempt to gain access to any devices connected to the guest network. If any of those devices are capable of accessing any confidential data NARO possesses and are on the guest network, it's possible for them to be breached and then permit attackers access to NARO's confidential information.
- Employees are not trained to look out for phishing emails. Phishing is a major attack vector in the modern cyberspace and should be treated as such with regular phishing email training
- NARO depends on PITA to create off-site backups and it is unclear how PITA handles those backups. If something were to occur that made NARO's physical backups inaccessible, NARO would lose their own single source of backed up data. Seeing as there's no other type of backup media within NARO, there would be no place of recovery for the lost data
- NARO allows any employee to install other software without prior authorization. Allowing any employee to download and install software may result in malware being installed on their machines. Not all employees have the same level of

knowledge of cybersecurity threats and what software may or may not be safe to download and install.

- NARO's Windows Domain servers are running Windows Server 2019 and NARO's Supermicro servers are running Canonical's Ubuntu 18.04.6 LTS. Both of these are past end-of-life, meaning none of NARO's operating servers are receiving security updates and other important patches.
- Netgear no longer supports the JGS524 which are the switches being used by NARO. Netgear no longer pushes security patches and updates to these.
- The engineering lab's systems aren't in NARO's Windows Domain, but can access important information within NARO. This means they are uniquely positioned for data exfiltration and can access extensive confidential data seeing how they are on the general wireless network . The lack of pairing with the domain means these systems can have out-of-band difficult to monitor configurations and security policies cannot be easily enforced on those systems.
- The cybersecurity policies are not comprehensive, meaning that employees lack a clear and concrete guide on what is deemed unacceptable behavior. This can lead to risky and diverse practices, as well as unchecked liability risks.

Conclusions:

- Be polite, but forward.
- We should assume that no one at NARO is a cybersecurity professional, and this conclusion should reflect that.
- "Some elements of NARO's cybersecurity that can be improved are…"

- Conclusion:
    - While NARO is a fairly secure organization, it can take steps to further protect itself from attacks. Much of NARO's weaknesses come from providing too much accessibility to its organization's tools/properties. NARO can resolve this by ensuring in all situations they are providing minimum required access to their organization's resources and facilities. This includes closely monitoring actions performed by external IT sources, such as PITA. Cybersecurity policy is another important avenue to consider. Implementing frequent cybersecurity training can help employees identify and prevent phishing schemes, and locking down workstations and employee devices may assist in preventing information leakage caused by employee installed/executed applications on work devices.
- Can probably discuss knowing when to contact law enforcement here

Follow-Up Activities:

- Recommended next steps
    - Improve employee cybersecurity training to help prevent phishing attacks
    - Reevaluate cybersecurity policy and employ the property of Least Privilege wherever possible (i.e. don't let employees install external applications on work machines)
    - Investigate post-life support for outdated equipment, or replace end-of-life equipment that is no longer receiving security patches if necessary

  - 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.
- What should the company include in their cybersecurity policy after this?
- How frequently should NARO conduct cybersecurity training?
  - At least once a year, with a cybersecurity assessment at least as frequently.
    - Since training is less costly than a full blown security assessment, They should be done more frequently, like every 3-6 months.
- Any other useful notes
  -

Thanks and Questions:

- Thank NARO (Special thanks William Donaldson III for their cooperation)
  - ShieldNet would like to thank NARO’s staff for cooperating with us during the course of the assessment. We would also like to extend a special thanks to William Donaldson III, who was instrumental in providing the necessary tools for us to conduct our investigation.
- Allow a space for questions to be taken (I don’t know exactly what this should look like in the slides but I'm sure we’ll figure it out).