Introduction:

Hello, everyone, my name is Raymond Vejar, and the purpose of this video is to educate and bring awareness of the increase of cyberwar attacks. Specifically to those organizations and individuals that are associated within what is considered our critical infostructure.

First, cyber warfare is a cyberattack, or series of cyberattacks launched against a country or state with the aim of gaining a strategic or military advantage. Acts of cyber war typically involve infiltrating or damaging networks, sabotaging infrastructure, and disrupting the operations of organizations and institutions vital to the target nation’s interests. These attacks, have the potential to cause widespread chaos and corruption, it is critical to take proactive measures to prevent them.

Second, no two cyber warfare campaigns are identical, and the list of potential attack vectors is endless. But, specific cyber warfare operations tend to fall within one of the following attack methods:

State a minimum of three potential security threats any organization may face:

• Malware Attacks -Viruses and Worms are now used as cyberweapons to attack critical infrastructure networks, or industrial control systems.

• Ransomware Attacks – By holding critical networks or data hostage, to cause disruption to the target country, which can lead to financing future attacks.

• Distributed Denial-of- Service DoS Attacks – The use of botnets to overload a website with fake request, which is designed to overwhelm systems and take critical operations or services offline

• Insider threats – Hacktivist, whistleblowers, and domestic leakers can divulge sensitive information, either unwillingly or intentionally. This information can aid in external attacks on a country’s national security.

Describe appropriate countermeasures organizations may employ against security threats:

To reduce these risk, organizations must use a combination of these top countermeasures to implement a layered Defense:

• Risk Assessment – identify potential vulnerabilities in your systems or infrastructure

• Cybersecurity Training – Employees must be trained on how to identify and prevent cyber-attacks. • Access Control – This should be limited to authorized personnel only

• Backup and Recovery – These options will help minimize a cyber attack’s impact

• Regular updates -Software and systems must be regularly updated to patch known vulnerabilities • Collaboration – Organizations should work with the government to share information about potential threats and mitigation strategies

• Testing – Against these type of attacks will ensure really how ready is your company prepared.

Describe appropriate measures to be taken should a system compromise occur:

Finally, the following steps should be taken on a compromised system:

• Identify Symptoms – Research Malware that you are dealing with

• Quarantine infected system(s) – Disconnect from networks

• Disable System Restore – Delete all restore points – Malware infects restore points • Remediate: Update Anti-virus software -Signature and engine updates

• Remediate: Scan and Remove – Depending on what anti-virus software your company is using.

• Remediate: Scan and Remove – Safe mode -Load the bare minimum operating system

• Schedule Scans and Run Updates - Automated signature updates, Task scheduler to provide system updates

• Enable System protection – Create a restore Point

• Educate employees or users -Personal Training -Posters and Signs -Message Board -Login Messages -Intranet Page -Always available