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:

**Don't wait for disaster to strike!** Take proactive steps to protect your organization:

* **Implement strong cybersecurity measures:** This includes firewalls, intrusion detection systems, multi-factor authentication, and regular security updates.
* **Educate your employees:** Train them to recognize phishing attempts, practice safe browsing habits, and report suspicious activity.
* **Develop a comprehensive incident response plan:** Know what to do in the event of a security breach, including how to contain the damage, recover lost data, and notify relevant authorities.

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

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

* **Isolate the affected system immediately:** Prevent further spread of the attack.
* **Contact your cybersecurity team:** They will assess the damage and guide the recovery process.
* **Report the incident to law enforcement:** In some cases, a cybercrime has occurred, and reporting is crucial.

**Cybersecurity is not just an IT issue; it's everyone's responsibility.** By taking these steps, you can strengthen your organization's defenses and minimize the impact of cyber threats.