**Title:** The Exploit Complexity Impact Rating Scale: Addressing the Growing Complacency in Cybersecurity

**Abstract:** In the modern era, leaders and executives in both corporate and governmental sectors have become increasingly desensitized to cyber threats. This complacency stems from most reported and media-focused threats being low-level (Level 1 and 2) exploits. While these minor exploits are frequently mitigated, the pervasive focus on them obscures the potential devastation of higher-level (Level 3, 4, and 5) threats. My presentation introduces the Exploit Complexity Impact Rating Scale, a comprehensive framework developed to underscore the varying degrees of cyber threats and their potential impacts on national security and corporate stability. Addressing and debating the importance of focus and research on higher-level threats.

The Exploit Complexity Impact Rating Scale categorizes exploits into five levels based on six distinct impact paths:

| **Impact Path** | **Description** | **Examples** |
| --- | --- | --- |
| Technical Degradation | Hacks that directly impact system functionality. | Trojan horse, malicious file. |
| Social Degradation | Actions that cause harm to individuals' social standing or well-being. | Blackmail, social harassment. |
| Physical Degradation | Threats that result in physical harm or restriction. | Kidnapping, forced physical restriction, physical harm. |
| OSINT Degradation | Collection of sensitive and private information. | Gathering sensitive information, private information. |
| Financial Degradation | Unauthorized control over financial assets. | Unauthorized movement, holding, and freezing of funds. |
| Infrastructure Degradation | Unauthorized control and manipulation of critical infrastructure. | Unauthorized access modifications of infrastructure. |

* **Level 1:** Single impact path, limited to the compromised system.
* **Level 2:** Single impact path affecting the compromised and connected systems.
* **Level 3:** Two impact paths affecting multiple departments or sections.
* **Level 4:** Three to four impact paths, compromising the entire company infrastructure.
* **Level 5:** Five or more impact paths leading to total infrastructure compromise.

I will demonstrate how an insidious Level 5 threat could unfold: A hacker implants a dormant virus within an organization’s email server, moving undetected to gather sensitive information using AI/ML to extract information of interest (IOI). This intelligence is used to craft a local email to blackmail a person of interest (POI), leading to further information disclosure and subsequent OSINT. The attacker leverages this information to restrict POI family members physically, coercing the POIs into delaying response and repair efforts, ultimately resulting in the takedown of critical infrastructure, such as a power-generating water dam. This scenario illustrates the potential for a high-level threat to cause widespread and severe damage.

This scenario exemplifies how high-level cyber-threats can cause irreparable social, economic, and political damage. Such threats are particularly concerning given the cyber capabilities of adversaries like Russia and China, who possess some of the most dedicated and ambitious hackers. While the United States surpasses these nations in every other measure of military power, including weaponry, naval, and physical forces, our cyber defenses remain a critical vulnerability. Cyber is America's Achilles' heel and the primary advantage our adversaries hold. This underscores the urgent need for organizations to adopt proactive cybersecurity measures.

Quoting industry leaders, "Complacency is the kiss of death" - Shari Redstone and "Complacency breeds failure. Only the paranoid survive" - Andy Grove, my presentation will underscore the urgency of recognizing and preparing for high-level threats. The potential consequences of these threats are severe, and organizations must take them seriously. By adopting the Exploit Complexity Impact Rating Scale, they can better prioritize their defenses and mitigate the risks of sophisticated cyber attacks. Let us not allow our desensitization to be the downfall of our nation.

**Keywords:** Cybersecurity, Exploit Complexity, Impact Rating Scale, High-Level Threats, Cyber Warfare, National Security