**Risk Management Fundamentals**

**Risk Management Fundamentals**

The infrastructure and cybersecurity security agency looks to improve the programs of vulnerability assessments. The vulnerability assessment program helps detect weakness in the digital infrastructure and develop new ways to beef up the security. The program gives insight into the infrastructure operators on the effectiveness of their cyber defense compared to others (Agrawal, Campoe& Pierce, 2014). The risk assessment involves threat integration and vulnerability information. Risk management consists of deciding which measure to take to reduce and manage risks based on the reduction strategy. The country’s critical infrastructure gives essential services that serve as the backbone of the country’s economy, wealth, and security.

Protecting the nation’s key resources and critical infrastructure from terrorist attacks is important to public health, the nation’s stability, and security. Terrorist attacks could severely affect the functionality of government operations. Terrorist attacks and other hazards could bring the country huge losses such as destruction of property, economic effects, death and citizen casualties, and damaging the publics’ morale and confidence in the country’s preparedness and risk mitigation strategies. According to Agrawal, Campoe and Pierce (2014), the critical infrastructure vulnerability assessment is controlled by a national infrastructure protection plan whose essential goal revolves around building a more secure, safer, and stronger country by improving the assurance of the country's CI/KR’. In this sense, the impacts of deliberate efforts by terrorists to destroy, hinder, or exploit them are to prevented,deterred, neutralized, or mitigated. In the end, national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster or other emergencies are enhanced.

Critical infrastructure acts as the support system of daily existence. The national system of preparedness integrates the efforts across the essential areas of preparedness, i.e., protection, prevention, response mitigation, and finally, recovery. These critical areas of preparedness must be achieved to achieve the goal of a resilient and secure country. The critical infrastructure protects the physical and cyber elements. It includes all the actions used to reduce the vulnerabilities, deter threats, and reduce the consequences associated with a terrorist attack (Lemieux, 2017). The protection of critical infrastructure is an element of resilience and security in the critical infrastructure, as detailed in the presidential directivepolicy.

Although critical infrastructures are exposed to a number of hazards such as machine and system failures, errors by humans, and natural disasters, terrorism remains the most distinctive threat to critical infrastructures. The United States, therefore, recognizes the danger posed by terrorist attacks. A terrorist attack usually infiltrates a critical infrastructure by targeting its soft targets. Soft targets in the critical infrastructure give terrorists ideal grounds to strike with plan-less and minimal efforts while at the same time causing mass casualties. Terrorism threats to critical infrastructures have two major dimensions (Brian, 2017). Number one is physical threats, and the second one is cyber threats. An example of a physical threat to critical infrastructure is the 911 bombing attack, where terrorists identified the soft targets to mess with the country’s peace.

Cyber threats are different from physical threats, but they may have the same catastrophic results. Examples of terrorist cyber-attacks include; data and system manipulation, where the attacker exploits the vulnerabilities in software and components needed for the optimal operation of critical infrastructures. Other cyber threats may include shutting crucial systems through DoS attacks and limiting access to crucial systems and information via ransomware attacks. The primary motivation of terrorists attacking critical infrastructures is to show the weakness in State institutions (Brian, 2017). The other reason would be to gain more publicity. Terrorism threats to critical infrastructures are countered by using a counter-terrorism strategy (Lemieux, 2017). The strategy emphasizes that preventing terrorism may lead to States taking measures that may limit some human rights. The counter-terrorism measures taken in this manner need States to ensure they protect the victims’ human rights.

**Reference**

Agrawal, M., Campoe, A., & Pierce, E. (2014). *Information security and It risk management*. Wiley.

Brian, B. (2017). Types of Terrorist Attacks. *Understanding, Assessing and Responding to Terrorism*, 99–136. https://doi.org/10.1002/9781119237792.ch3

Lemieux, F. (2017). Defending Critical Infrastructures Against Cyber Attacks. *Current and Emerging Trends in Cyber Operations*. https://doi.org/10.1057/9781137455550.0015