Cyber risk essay examples

Sociology, Violence

Cyber Risk.

Cyber crime has become an issue in the US since most of the infrastructures are being controlled through the internet. Therefore some individuals or group of people nowadays get involve in cyber crime activities in order to cripple the normal operation of the state.

According to the discussion, most students concluded that the type of hacker that is most worrisome is the malicious code (Janczewski, L. 2008). The malicious code category includes viruses, worms, and Trojan Horses. Viruses spread from one computer to another without the consent of the user while worms require you to perform some action before they infect your computer. Trojan Horses are very dangerous since they send confidential information to an intruder while you are working on your computer.

Another worrisome hacker is the theft of identity and using it to perform criminal activities. According to the discussion, the risk mitigation strategies that can be taken to prevent cyber crime are making sure that all computers and networks have an ample amount of protection. It was also agreed that with all the technological advancements and relationships that China and Russia have with the United States, China is more of a threat to the US. This is because they have very high technology(Janczewski, L. 2008). It also has a history of dealing with nuclear weapons. The first infrastructure they would attack first is the power grid so that there is no access to any information. What should be done to curb this is through awareness and cooperation.

The critical infrastructures that are likely to be targeted are energy and water. This is because there have been a number of attempted attacks and successful cyber attacks against critical infrastructure such as dams, energy

and water systems in 2010 and 2011.

In conclusion, the students resolved that all sectors are responsible for protecting these critical infrastructures because it is a very big and complex process that cannot be done successfully by one sector (Janczewski, L. 2008). Considerably, it should not vary based on who the attacker is because an attack will eventually results to a damage no matter how you look at it.

Reference.

Janczewski, L. (2008). Cyber Warfare and Cyber Terrorism. New York: Idea Group Inc. (IGI)