Research paper on approaches to cyber security programs and public awareness and ...

Approaches to Cyber Security Programs

The first answer is correct since it clearly answers the question on risk management framework. This is through the clear definition of what goals are involved in establishing a risk assessment framework. An analysis of the assets and systems that are involved is equally crucial in the determination and mitigation of possible risks. The framework also comprises of establishing a platform for assessing the various risks that may arise from terrorist attacks and other possible hazards. After a critical analysis of the risks, sufficient control can then be implemented to help in mitigating these risks. Implementation is carried out through well set programs that aim at protecting the systems from the risks identified thus far (DHS, 2013).

The use of these kinds of frameworks in organizations is especially handy since they are generally applicable in a variety of infrastructural setups. The use of this framework allows for implementation of the programs that will mitigate cyber security risks. Furthermore, it is possible to carry out an assessment of how effective these programs are while they are in operation (Hart, 2011).

Public Awareness and Education of Cyber Security Doug's Response

The second answer is also correct and answers the question posted very well. This is because the answer identifies a specific effort in the education and awareness of the public. One such area is cyber security. This is especially crucial since the world is now in a digital era and is bound to progress even further (Newhouse, 2012). Effort should be made to come up

with efficient technologies that will promote cyber security. The intended audience is large and may encompass a national scope. Companies have stepped into the scene by offering information on cyber security hence promoting this awareness (UMUC, 2013).

References

Newhouse, B. (2012). Securing America digital infrastructure through education. Retrieved from https://www-hsdl-org. ezproxy. umuc. edu/? view&did= 738571

UMUC (2012). Implementing cyber security programs within and across organizations: Module

5. RetrievedFromhttp://tychousa9. umuc. edu/CSEC670/1306/9023/class. nsf/MenuOpen

frameSet&Login

DHS. (2013). www. dhs. gov/xlibrary/assets/NIPP_RiskMgmt. pdf. Retrieved June 17, 2013, from

www. dhs. gov. Hart, S. R. (2011). A Guide for Homeland Security Instructors Preparing Physical Critical

Infrastructure Protection Courses. Homeland Security Affairs, Volume 7, 1-26.