Cyber security Training at the Department of Homeland Security

Student’s Name

Institution

**Cyber security Training at the Department of Homeland Security**

For the last decade, the cyber security training ha resolved and a lot of programs update has been included to reflect the current challenges. During the early days, the homeland security training programs captured mostly preparedness to address natural disasters, homeland terror and other minor crimes. With the rise of technology, the training programs have been upgraded and cyber security trainings focus on the investigation, prevention and compiling evidence on major technology related crimes. The current cyber security training at the department of homeland security focuses on the infrastructure protection. As stated by () the cyber security trainings also focus on the financial frauds focusing on crypto currency, dark web, social media analysis and network infrastructure. The current training is conducted to equip law enforcement officers with knowledge and skills on how to investigate and detect various cyber frauds using computer technology.

**Benefits of cyber security trainings**

The current trainings benefit law enforcement officers and other individuals in the cyber security field. It is pointed that the Department of Homeland Security signed private –public partnership with several private companies to provide help in designing programs and also to train personnel. Therefore, the current cyber security training programs help in improving the understanding of some of the challenges in cyber security and provide individual candidates with knowledge and skills on how to detect, prevent, investigate and persecute various cyber security cases both local and international. () pointed out that cyber security training offered by the Department of Homeland is well elaborate and therefore, the trainings have helped in conducting cyber security cases. It is therefore, important to state that the training has helped in solving cyber security issues faster and efficient with limited errors. The current cyber security training has also helped in reducing errors. It has also enhanced security, protect organizational reputation, and increase compliance as well. The training has also helped in securing that businesses are secure. The fact that current training covers almost all the industrial challenges a trained an individual would be able to solve several security related issues in the country.

**Cost incur**

The cyber security training is an elaborate training method in the technology field. It offers several security solutions and therefore, the training cost must be expensive. The individual who pursue a course will cyber security training to become a fully trusted to set the condition for the proper without much different. Therefore, the cost of cyber security training ranges from $5000 to 15000. The cost is based on the units taken by individuals and the content which are being studied by an individual. Mostly pure technical and some of the lasts security challenges are expensive. Since the department of homeland have partnered with other institutions and other interested parties to address the challenges in the market, the problems have been addressed through cost sharing. In the past the department of homeland security has partnered with other institution to ensure that cyber security trainings are affordable.

**Recommendation**

The current trainings of cyber security focus on several issues especially challenges experienced in the cyber security industry. According to (Evans, 22018) the trainings put a lot of focus on the jobs in the market, the technical aspect in the cyber security, and the methods which are used to investigate fraud and other related major crimes. The training, which are being provided by the Homeland Department with the police offices focus on crime scene analysis to obtain enough evidence and also to prevent a crime as well. Though cyber security training is more practical and focus on providing a proof, there is needed to work with relevant bodies and authority to analyze some of the challenges in order o come up with solutions. First, it recommended for the training to focus on some of the latest security related challenges. Therefore, the trainings address the training cover areas such as the Phishing Landscape Evolves, BYOD Enhances the Workplace, but at a Steep Cost, Surge in Ransomware Attacks Targeting Local Governments, and Strict Cloud Security Measures Lead to End-User Trust. These are key elements in technology and therefore, security training should focus on improve their performance.

However, the current training method does not have a clear method which can be used for the performance of evaluation of the result of trainings which are offered by the departed if government. There must be a clear methods which are used to establish whether the current system support the survey. According to Beyer and Brummel (2014), survey is one of the tools which are used for that analysis and representation and therefore, it is important to plan fruit of discipline and department heads

It is also established that the new training equips law enforcement officers on how to investigate and detect cyber fraud and other cybercrime-related through the use of computer technology (Nathan & Givens, 2015). According to Beyer & Brummel, (2014), the new challenges in technology are cybercrime and some of the cyber crimes are new and of high tech. therefore., lack of without training on law enforcement on social media, network architecture, network infrastructure a computer of system protection (Evans, 22018). Cyber security training should be more transparent. It also needs to involve training on how to assess the need for a company so that trained personnel can be able to provide necessary and needed cyber security protection, the law related to cyber security and other performance

In conclusion, with 85% a budget of nations’ infrastructure is under privacy protection, the private-public partnership is critically important for the governmen (Beyer & Brummel, 2014)t. It also willing to support advantages and other family activities Security in partnership with private sectors has developed training courses to develop the capacity of the private sector to protect infrastructure from unauthorized access and violation of privacy and cyber terror attack which one of the latest terror attacks being used to caused problems. It is, therefore, evident that the improvement is based on the current challenges resulting from advance technology (Busch & Givens, 2012, p. 21). Therefore, the current training in cyber security covers most current challenges being faced in the cyber security system

# References

Beyer, R. E., & Brummel, B. J. (2014). Implementing Effective Cyber Security Training for End Users of Computer Networks. *Society for Human Resource Management and Society for Industrial and Organizational* , 2-18.

Busch, N. E., & Givens, A. D. (2012). Hard National Security Choices SUPPORT. *https://www.hsaj.org/articles/233* , 2-15.

Evans, H. (22018). Summary: The Department of Homeland Security’s Cybersecurity Strategy. *Hard National Security Choices SUPPORT* , 2-15.

Nathan, B., & Givens, A. (2015). Public-Private Partnerships in Homeland Security: Opportunities and Challenges. *Dudley Knox Library* , 2-15.

Directives

Recommendations