Cybersecurity Training at the Department of Homeland Security

Student’s Name

Institution

**Trends in Cybersecurity training**

Though the state and provides guidelines and programs that are used in Cybersecurity training, the concept is developed based on the current challenges we face in cybersecurity. For the last decades, methods and techniques used in cybersecurity training have improved. Traditionally, the training was focused on terror and counterfeits to establish methods that can be used to defuse these problems. However, a lot has changed ad cybersecurity training focuses on how to detect, prevent and also eliminate some of the cyber threats. The Social Media for Law Enforcement, dark web, and CryptoCurrency are some of the new courses which are being covered in cyber training. According to Nathan & Givens (2015), social media cybersecurity law has become embedded into the cybersecurity training courses because of the challenges related to social media bully and other frauds that law enforcement officers are addressing. The social media for law enforcement is designed to training law enforcement officers on how to use social media to gather, prevent, and solve crimes as well.

The current cybersecurity training also involves training in infrastructure protection. With 85% of nations’ infrastructure is under privacy protection, the private-public partnership is critically important for the government. Homeland Security in partnership with private sectors has developed training courses to developed 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). Therefore, the current training in cybersecurity covers most current challenges being faced in the cybersecurity system. 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.

Therefore, the new training equip law enforcement officers on how to investigate and detect cyber fraud and other cybercrime-related through the use of computer technology. According to Beyer & Brummel, (2014), the new challenges in technology are cybercrime and some of the cyber crimes are new and of high tech. Without training on law enforcement on social media, network architecture, network infrastructure a computer of system protection (Evans, 22018). Cybersecurity 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 cybersecurity protection.

**Training methods in cybersecurity**

Cybersecurity is an important aspect of government and organizations as well. It involves process, design, and practice to protect the network infrastructures. It is, therefore, required to be ethically done to ensure that the knowledge and skills gained and be used effectively. Cybersecurity should involve both theoretical and technical aspects of training. The training can be provided in house and at a designated place for the efficient provision of information. The training should be in person with experts in the field. It is also essential to training employees on what they do not know so that they can sharpen their skills and experience in the field. The training should be specific and based on the weak areas which should be addressed. The training needs to cover what is needed to be captured to build evidence of any cases. The training method should be evidence-based to explore the psychological, technical, and environmental factors which cause suspension and should be analyzed in the process of evaluating security.

The cybersecurity training currently focuses on the job available and the objectives of the training which is being conducted. There are several job positions available in the market which an individual train in cybersecurity can get. The training should, therefore, be more technical to ensure individuals who have been trained can proceed to conduct a good job in the protection of network infrastructure. However, the jobs which can be secure with training in cybersecurity are a data manager, ICT security manager, information security analysts, and others. There important aspect here is that the training of cybersecurity is conducted by specific objective and goals which must be achieved. This is why Homeland security provided training to members of the public on Ransomware Attacks and other common cyber attacks.

In conclusion, cybersecurity training has changed and there are more challenges in the current society related to cybersecurity. Some of the current trends are the latest attack through Ransomware, which disbarred to the computer system. However, the methods of training which are being used include physical instruction which can conduct in the classroom and online services. The training involves practical and theoretical aspects to improve the knowledge and understanding of cybersecurity issues. The training is conducted based on the objectives and goals set and the current challenges in the market and therefore, the training being done is based on the current challenges and geared towards providing a solution to the problem.

# 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.