RUNNING HEAD: CULTURE

Visually annotated bibliography

[Name of the Student]

[Name of the Institution]

Visually annotated bibliography

***Question Number 1***

The history of cybersecurity dates back to the time when the internet was not even launched. The first antivirus was invented by Robert T. Morriss, while he was designing a program. In the late 1980s by the name of the computer worm, the virus was formed to measure the internet connections and their sizes(Tang et al., 2016). This was a bug virus which infiltrated the Unix terminals and copied information. Later in the 1990s, millions of computer systems were infected by different types of viruses. Furthermore, in 2000, a fifteen-year-old boy named Michael Calce attacked high commercial websites. This is where an era of viruses started to originate the idea of cybersecurity (Warner, 2012).

***Question Number 2***

Cybersecurity is needed because the protection from cyber-attacks is possible only through the safety of interconnected systems, which include software, hardware, and data. Occurrence or origination of cybersecurity took place due to the viruses and infarctions done through bugging system into the private data(Tang et al., 2016). Threats to the security of websites, internet and personal data of the people sharing it online, are the ultimate causes for the need or necessity of cybersecurity as dated back to 1980s, the start of Morris worm was the moment which urged this need. Cyber threats or attacks are the reason for system failure, security breaches, and theft of valuable information, making it important causes for cybersecurity(Stevens, 2018).

***Question Number 3***

Taking it 20-30 years back, the origination of cybersecurity was a head-turning task for information technology. Whether talking about Morris's worm or wave of the 90s, cyber security became game-changer after the invention of such malicious things in late 1990s. It is this time that big antivirus companies dominated the industry of cyber security for 20 years, but then in 2014, more cyber threats and attacks originated new solutions to new challenges. Then 2014 onwards, new technology got invented and is still evolving with further innovations, i.e., behavioral detection, artificial intelligence, and machine learning. As cybersecurity is evolving, so is the complexity of cyber threats and attacks (Singer & Friedman, 2014).

***Question Number 4***

Many things have differed according to the evolution of threats and attacks by cyber terrorists. Communication environment, business activity, threat landscape, and information technology all have changed or grew into more enhanced and wider levels. The theft is not restricted to hacking into someone's account just for the sake of bullying; as this is the era of smart devices, it has increased the chances for data breakage and infiltration. The emergence of cloud computing has given access to the common man for using data and services from any side of the world through web interface (Rasekh et al., 2016). The sameness of cybersecurity lies in the fact that no matter ways and styles of cyber-attacks have changed, but the cause and reason are still the same to steal or intrude into the data of other people which is either or not useful by the malicious party. Other than the electronic environment, nothing has changed in cyber attacking as well as the security (Stevens, 2018).

***Question Number 5***

The leaders who helped in growing and evolving the phenomenon of cybersecurity are mostly linked to the business industry and information technology. It is the leaders of companies like, cybersecurity and malware protection, which took part in changing and evolving the phenomenon and characteristics of Cybersecurity. The leaders who were involved in the movement of cybersecurity were from government organizations and other corporations, i.e., digital enterprises (Tang et al., 2016).

**References**

Stevens, T., (2018). Global Cybersecurity: New Directions in Theory and Methods.

Warner, M., (2012). Cybersecurity: a pre-history. *Intelligence and National Security*, *27*(5), 781-799.

Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What everyone needs to know*. OUP USA.

Rasekh, A., Hassanzadeh, A., Mulchandani, S., Modi, S., & Banks, M. K. (2016). Smart water networks and cybersecurity.

Tang, Y., Chen, Q., Li, M., Wang, Q., Ni, M., & Fu, X. (2016, October). Challenge and evolution of cyber attacks in Cyber-Physical Power System. In *2016 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC)* (pp. 857-862). IEEE.