OLD DOMINION UNIVERSITY
CYSE201S

Career Paper

Madelene McFarlane

#01096496

In the world of the present day almost everyone is dependent on technology in some type of manner. Therefore, the security that is needed to keep the social cyber system safe is continuing to grow as well. Within cybersecurity there is many varieties of roles that one can take on in order to keep those in society safe from cybercrime. The role that will present as the main focus of this paper is the role of a Cybersecurity analyst. Discussing the nature of the role and the responsibilities that are required. As well as the ties within social sciences that remain principles within the career.

Cybersecurity analysts commonly work for company's and businesses and provide protection over that company's hardware, software, and networks. Cybersecurity analysts' roles on a day-to-day basis will vary depending on the company however a rough idea of the daily tasks to be performed include monitoring network traffic for suspicious events, looking into reports in real time, install and operate firewalls, fix vulnerabilities, and conduct threat research. This role also requires the analyst to remain up to date on the latest cybercrimes in threat to be the first line of defense with a company's cybersecurity.

As stated, cybersecurity analysts are the first line of defense when it comes to a company's or network's cybersecurity. This is due to the analysts being the ones that monitor data and information coming in and out of the network for any suspicious activity and any vulnerabilities that could cause a breach into said company. The role requires a lot of attention to detail and critical thinking along with a natural sense of curiosity. As for technical skills, data security, intrusion detection, and endpoint management are crucial within this genre of role though the additional of other skills are needed to compete with the growing risk of cybercrimes throughout society.

While most roles withing the cybersecurity umbrella are technical there is still a heavy element of social science principles that are applied. Within the cybersecurity analyst field some of the factors that are included are human factors, social media, economics, and psychological aspects. Behind every cybercrime there is a human somewhere in the mix. The human factor of a cybersecurity analyst position is to be sure that their team is educated on how to keep themselves and the company safe from breaches. Along with striking down risks that are looking to exploit human factors such as phishing emails.

An extension of the human factor is that of social media. Sometimes analysts' will be required to look over social medias that are public reached. These social medias could be that of the company's or employees within the company. Making sure to monitor for factors that could aid in a potential breach of information. Such as a company photo that was taken to celebrate someone's anniversary in the company and the photo including a small sticky note on someone's computer that has written user information on it. The analyst would then have to report the incident and take the needed steps to resolve the situation.

Another factor that an analyst has to keep in mind is the psychology factor that cybercriminals use within social engineering. Keeping up to date on the scams and crimes and being able to inform their team to keep everyone safe. As well as being able to clearly view what the criminals are attempting to gain from the company and tracing back how the attackers would go about reaching their goal. Often times criminals will attempt to breach a company's network in order to gain economically. Through methods of directly taking money from the company or taking information that can then be sold. Either way the economic factor plays a part in an analysts' limits, procedure, motivation, and proactive mindset in preparation for the next cybercrime attempt.

References

Adetoye, B., & Fong, R. C.-wai. (2023, January 3). *Building a resilient cybersecurity workforce: A multidisciplinary solution to the problem of high turnover of cybersecurity analysts*. SpringerLink. Retrieved April 3, 2023, from https://link.springer.com/chapter/10.1007/978-3-031-20160-8_5

Chudasama, D. (2021). *Why choose cyber security as a career*. Current Trends in Information Technology. Retrieved April 3, 2023, from https://www.researchgate.net/profile/Dhaval-Chudasama/publication/352121113_Why_Choose_Cyber_Security_as_a_Career/links/60ba059e92851cb13d752488/Why-Choose-Cyber-Security-as-a-Career.pdf

Ganesan, R., Jajodia, S., & Cam, H. (2017, February 24). *Optimal scheduling of cybersecurity analysts for Minimizing Risk*. ACM Transactions on Intelligent Systems and Technology. Retrieved April 3, 2023, from https://dl.acm.org/doi/abs/10.1145/2914795

Wall, T., & Rodrick, J. (2021, March 5). *The demand for cybersecurity and soc analysts*. SpringerLink. Retrieved April 3, 2023, from https://link.springer.com/chapter/10.1007/978-1-4842-6904-6_1