Career Paper

Joshua Taylor

CYSE 201S

Professor Duvall

A career that stands out to me as a career that requires, utilizes, and depends upon various elements of social science research, utilizes the social science principles, has an impact on society, and incorporates many elements of the material we have learned throughout this course is a Cyber Defense Infrastructure Support Specialist. The NICE framework describes the role of this position as someone who "tests, implements, deploys, maintains, and administers the infrastructure hardware and software that are required to effectively manage the computer network defense service provider network and resources. Monitors network to actively remediate unauthorized activities." (National Initiative for Cybersecurity Careers and Studies, n.d.).

This career is impactful and utilizes social science research and adheres to the social science principles in the day-to-day tasks that they conduct. A Cyber Defense Infrastructure Support Specialist, in my opinion, leans heaviest into the principles of empiricism, parsimony, and relativism. An individual in the role uses the principle of empiricism when they look to develop, test, and/or implement any new hardware or software. When making the decision on whether or not a specific solution will enhance the security infrastructure, these specialists must compile data, test the products in real world scenarios, and understand the capabilities of these products as they truly are. The analytics and real-world application of data help to eliminate the potential for opinions. In this role, a specialist would more or less be tasked with the overall security of a cyber system(s). They would also be responsible for briefing various parties on the functionality of new products/services, briefing executives on what would be in the best interest of the company in terms of infrastructure security, etc. Parsimony plays a large role how the specialist relays potential extremely technical information to those without the technical know-how. To be successful in this position, it would stand that those in this role must be able to communicate complex cyber information to potential decision makes effectively. A Cyber Defense Infrastructure Support Specialist must also understand the relation of the components of the infrastructure and how, if a change occurs in one component, what will the effect be on the relationship with other components. Will advances in hacking software's require changes in the software/hardware infrastructure of the network? Individuals in this role must always be cognizant of how components of their systems and the outside world are related.

Professionals in this role must be well-rounded and well-versed in various concepts that we discuss in this course. A vital role these professionals play is in maintaining the confidentiality, integrity, and availability of the infrastructure and the data stored within their systems. They must understand, develop, implement, and properly maintain the infrastructure that houses data and understand what bad actors might do to try to penetrate that infrastructure. Also, in doing that it requires a deep understanding of the human factors involved on both sides of the infrastructure. Understanding the impacts of newly implemented hardware/software, and how they are perceived by the employees and company they are used for, is critical to the success of those products, If the specialists develop to complex or difficult software to operate, there is a possibility that employees may find a less secure work around and improperly use that software. Human factors are truly something vital that this position must focus on. These professionals also must understand psychology behind victimization in the cyberspace and be aware of victim behaviors, what may lead people to become victims of cybercrime while using their infrastructure. In order to create viable infrastructure, knowing what may be a potential point that leads to victimization is important. The importance of this job can also be seen in the interest in smart cities, and the mass adoption of IoT, AI, etc. Cyber Defense Infrastructure Support Specialists are and will continue to be on the frontlines of the implementation and development of these systems because the systems will not be trustworthy without the proper

defense infrastructure in place to ensure the safety and security of everything that uses the products/services.

The impact this profession has on society, and the importance that the position is inclusive to all walks of life is vital to the success of the position as well. This specific profession has a large impact on the day-to-day operations of many businesses out there today. The security of cyber services that people use both personally and professionally (i.e., AWS cloud services, VPNs, etc.) have all been contributed too by people in this profession. The management of defense infrastructure in place at a cloud services facility is managed in part by individuals like a Cyber Defense Infrastructure Support Specialists, although potentially with a differing title. Those kinds of services would not be trusted to be safe and secure without the proper defense infrastructure in place, which this profession helps to provide. The IC3 report of 2023 states that financial losses are on the rise, drastically, year over year. An example being data breach losses in 2021 were $151,568,225 and in 2023 they were $459,321,859 (Internet Crime Complaint Center, 2022). The IC3 Elder Report also states that data breaches accounted for losses totaling $17,681,749 for individuals over 60 (Internet Crime Complaint Center, 2022). This highlights the societal importance of professions such as this one because Cyber Defense Infrastructure Support Specialists manage and develop and help administer hardware and software that is designed to defend cyber infrastructure against these kinds of crimes and the occurrence is only increasing.

Cyber Defense Infrastructure Support Specialists play a vital role in ensuring the safety and security of the cyber networks and infrastructure we use on a daily basis. The societal impact his position can and does have is notable. Cyber Crime in the United States remains high, and losses are growing, which highlights the importance of having strong cyber defense infrastructure as a frontline defense against these crimes. This role will also play a large role in the implementation of many new ideas (i.e., smart cities) due to the required need for strong defense infrastructure for the success of ventures such as that. This profession utilizes many of the social science principles routinely, in the course on ensuring that infrastructure remains secure. Those in this position must routinely take stock on the human factors at play when developing and administering hardware/software, look at weak points that could lead to victimization, and always must be striving to ensure that the confidentiality, integrity, and availability remains intact when they are fulfilling the roles of this position. Overall, this position is a key component in the overall cybersecurity landscape and is an intriguing career path.

References

Internet Crime Complaint Center. (2022). Elder Fraud Report. Federal Bureau of Investigation. Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3ElderFraudReport.pdf

Internet Crime Complaint Center. (2022). *Internet Crime Report.* Federal Bureau of Investigation. Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

National Initiative for Cybersecurity Careers and Studies. (n.d.). *Cyber Defense Infrastructure Support*. Retrieved from https://niccs.cisa.gov/workforce-development/nice-framework/specialty-areas/cyber-defense-infrastructure-support