Career Professional Paper

By: Sarah Vakos

Old Dominion University

CYSE 201S 23181

Cybersecurity as a Social Science

Dr. Leigh Armistead

11 November 2022

Introduction

In this career professional paper, I will be going over how a cyber analyst requires and depends on social science research and social science principles in the cybersecurity industry. Key concepts learned in this class will be reviewed and demonstrated on how those concepts are applied to cyber analysts. Certain marginalized groups will be discussed to show how cyber analysts are related to those groups and the challenges they face. Then, I will go over how cyber analysts are related to society.

Background information of a cyber analyst includes job duties, what qualifications and or kind of computer knowledge they need to have and personal traits or skills they should have in the work force. As a cyber analyst you can work for enterprises like private businesses, a government agency, or a non-profit organization. The job duties are studying reports, data, and analytics to point out unusual activity and threats. They use the collected data to form safeguarding and inform their company's choice of security software. Giving advice to the company's management on actions to improve their security and organizing training programs to help non-IT employees understand and adhere to the businesses security policies.

On a normal day, a cyber analyst might overlook computer networks and systems for threats and breaches. They could be installing, modifying, and updating security software and firewalls. Testing systems for possible bugs or vulnerabilities and creating systems or operations for security best practices all through the company are other possible duties. Writing reports on security incidents and changing acknowledgements is a major responsibly for a cyber analyst.

The qualifications for this career profession are a bachelor's degree in computer science along with experience in the field or other applicable work experience. Sometimes, experience in

the field is acceptable without any degree. Computer knowledge includes penetration testing, network security and techniques to expose and rectify weaknesses. Soft skills are required, along with thinking analytically, problem solving, attention to detail, and critical thinking. A cyber analyst also needs to be able to work with others in a team to get a task done. As a cyber analyst, being able to think like a hacker, thinking outside the box, and innovate security ideas are key abilities to have besides the technical and cooperative skills.

Social science research is something cyber analysts depend on in their field so that they know what is currently happening and what kind of issues people come across in their everyday lives specifically concerning computer technology for social, economic, educational and political grounds. Social science principles are also important to cyber analysts, so they know how to read research properly without having their own bias or opinion for example, is called objectivity. Knowing that changes in one system will lead to changes in another system is crucial and is called relativism. Keeping explanations in simplest terms so that an average person understands and can comprehend is critical and is known as parsimony. Following ethical standards when managing research by keeping privacy of individuals is required and is known as ethical neutrality. Finally, keeping in mind that behavior is caused or influenced by previous events should be taken into consideration but shouldn't be the answer for all circumstances is also important for cyber analysts.

The concept empiricism is a term talked about in class and it relates to the cyber analyst profession by studying behavior that is real to the five senses. Occasionally, honey pots are created to lure attackers onto a site that looks identical to the real one they want to snoop around in where they should not be on like a confidential site or forum and by observing their actions can help cyber analysts collect data on them and what kind of information they are trying to obtain. By observing a honey pot in real time, the actions taken by an attacker can give cyber analysts ideas on how to protect that data better. Diversity is another concept talked about in class and is important in the cyber security field regardless of what job you have. Having women and men along with different ethnicity is key in this work force since everyone can share their perspectives and viewpoints on how to solve a problem or fix a bug on a system. Women think

differently than men do so by having women in the field invites different mindsets and can offer new ways of looking at issues that arise with producing better decision making.

Victim Blaming is a concept discussed in class and relates to cyber analysts because their job is to not victim blame but to find whether there are things that individuals or organizations can do to make themselves safer. The last concept that has been discussed in class is a white hat hacker. These hackers are good guys because they find vulnerabilities in a system and notify the appropriate person or team of the issue along with the steps they took to find that bug and how to fix it. A cyber analyst can appreciate a white hat hacker for letting them know and be aware of bugs or issues in their network but maybe would not like the idea that they got into their system in the first place.

According to the European institute for gender equality, marginalized groups are defined as, “Different groups of people within a given culture, context and history at risk of being subjected to multiple discrimination due to the interplay of different personal characteristics or grounds, such as sex, gender, age, ethnicity, religion or belief, health status, disability, sexual orientation, gender identity, education or income, or living in various geographic localities” (Marginalized Groups, n.d.). Children and the youth are a marginalized group that cyber analysts take into consideration when securing a system so that their information is not leaked. Challenges that arise with children under the age of thirteen who are on the internet and on sites where they should not be when they disguise themselves as someone older than what they really are. Another challenge is when someone takes advantage of a minor and exposes them whether it be inappropriate pictures or videos. The third challenge is data being leaked from minors that contain their address and their parent's information along with billing information. All the

challenges that this marginalized group faces are one of the most important tasks for cyber analysts to keep an eye on to prevent a hacker from exposing minors.

A cyber analyst is related to society in everything they do in their day-to-day job activities. “A cybersecurity analyst protects company hardware, software, and networks from cybercriminals. The analyst's primary role is to understand company IT infrastructure in detail, to monitor it at all times, and to evaluate threats that could potentially breach the network. The cybersecurity analyst continuously looks for ways to enhance company network security and protect its sensitive information” (What Does a Cybersecurity Analyst Do?, 2022). A cyber analyst strives to maintain and protect consumer and user data and without cyber analysts, society would be in great danger with their information exposed and in the hands of someone else. “Any act of hacking on the IT infrastructure puts everything at risk. These days, even government agencies are reported to be the victims of hacking attacks. During these attacks, information sensitive to national security can be stolen, putting an entire country at risk” (Imarticus, 2022). Cyber analysts are an important asset that every enterprise and government agency needs to protect society and their information.

References

marginalized groups. (n.d.). European Institute for Gender Equality. Retrieved November 4, 2022, from https://eige.europa.eu/thesaurus/terms/1280

What Does a Cybersecurity Analyst Do? (2022, April 30). Western Governors University. https://www.wgu.edu/career-guide/information-technology/cybersecurity-analyst-career.html

Imarticus. (2022, July 26). *3 Ways A Cyber Security Analyst Can Give Back To The Community*. Finance, Tech & Analytics Career Resources | Imarticus Blog. https://blog.imarticus.org/3-ways-a-cyber-security-analyst-can-give-back-to-the-community/