A Cybersecurity analyst is one of the most important cybersecurity specialists that any organization can have. Analysts play a large role in maintaining, upgrading, and repairing any network or cyber operation for any organization. A cybersecurity analyst's job is to understand the cyber infrastructure of a network, monitor and analyze the network further, analyze the weaknesses and threats, and understand the tools that can be used to make sure the network is better prepared and maintained. There are also a number of secondary responsibilities that will be associated with these duties. For one, the analyst needs to know how to conduct, read, and respond to reports for the network and infrastructure. The analyst may also need to understand and be able to implement certain tools such as antivirus protection, intrusion detection, and other relevant tools.

One important quality that would enable a successful analyst to succeed, would be a good understanding of the adversaries that willingly or unwillingly will harm the network. This can be divided into two separate groups, the internal adversaries, and external. Externally, the cyber analyst will obviously have to understand the actions of those that wish to do the network harm, such as scammers, state terrorists, fraudsters, and other malicious agents. One important analysis that the cyber analyst will need to make is to understand the type of malicious agent they are most likely to see. For most companies with assets, it's probably going to be more likely that they will have to deal with scammers and thieves who wish to steal assets and commit financial damage. Perhaps in another religious or political organization though, the analyst will be expecting to see more terrorists, hacktivists, and state agents. The analyst can then use sociological principles to better understand the motives and driving agents behind a person's actions. A more common thief for instance will likely be deterred if the defenses are strong enough to make attacks have no financial incentive left for the attacker. If the attackers are more political or religious in nature, though, a different approach may need to be taken. The intense radicalization from a certain specific religious or political affiliation may make it easier for the effects of neutralization to go into effect. Without a proper sociological perspective on the motives of attackers, a cyber analyst would not properly be able to understand attackers and thus implement the correct defenses.

Internal threats are just as important as external ones for a cyber analyst. Internal threats can be active malicious threats, such as a disgruntled employee or ex-employee. In these cases, the same sociological perspective used for external threats can also be helpful here. Disgruntled employees are more likely to be radicalized and exhibit the same relentlessness as some external threats. The far more nefarious threats, though, are the internal threats that are not malicious, and are harming the network due to ignorance, mis-education, or negligence. It's a classic saying that the most dangerous threat to any network is not behind the screen, but what's sitting in the chair. For cyber analysts this means a lot of analysis and understanding needs to be put towards understanding user behavior, and implementing the proper tools, policies, and guidelines to deal with that behavior. An important step for cyber analysts is to always account for human elements, and to craft an analysis and design that accounts for such things. One important concept often brought up is that of cyber hygiene. Most people would not leave the house if they had a massive stain on their shirt, or dirt on their face, or smelled very bad. This is due to the societal nature of how certain hygiene standards are shared. It becomes second nature, and we expect others to act the same way we do. This second hand nature often does not apply to cyber behavior and cyber hygiene, however. Users will often commit the cyber equivalents of not brushing their teeth or washing their clothes without any thought or consideration. Cyber analysts will have to keep this in mind and attempt to guide users towards proper cyber hygiene in order to keep their systems safe. By stressing the medical cleanliness of cyber hygiene to users directly, and working to build on that concept through policy and training, cyber analysts can promote a more thoughtful culture based more on human elements. Some cyber hygiene activities can include proper phishing responses, proper authentication and/or password protocols, proper web application practices, etc. These are but a small few of the tasks a cyber analyst will need to take up when it comes to dealing with internal threats. No matter the implementation the analyst comes up with on paper, without accounting for culture and human elements, the implementation will surely fail. This is why human elements are so important and a sociological perspective on your users is so important. For instance, most users would not imagine a cyber analyst would not have anything to do with cyberbullying. While certainly many analysts do not, many may also need to understand and deal with it as a large issue. Depending on the network, cyberbullying and cyber victimization behaviors may be extremely detrimental to a network's security. Even disregarding schools and religious institutions, even regular for profit businesses may need to deal with this issue in some way. To illustrate this, imagine a business where one user is using the network to bully and victimize a junior employee. This could have intense negative impacts on the system. Legal fees, lost productivity, detriments to work culture, lost resources, and other effects could all be seen. The bullied employee may even be radicalized into becoming a malicious agent themselves, either bullying others, or striking against the network as revenge. The cyber analyst may even need to understand concepts like diversity and marginalization to properly address the issues present in a network. Certain groups and individuals may be more likely to be victimized than others. If a cyber analyst doesn't understand this, how could they ever hope to combat the issue and help promote a secure and well maintained network. This illustrates how important it is that even victimization behaviors have to be understood from a good sociological perspective for many cyber analysts. This even gets us started on another important topic that must be understood from an interdisciplinary perspective for a cyber analyst to succeed - teamwork.

Teamwork is not only important for a cyber analyst to understand on a professional level, but on a personal one as well. Cybersecurity professionals are not often isolated individuals, each with their own self-contained corner of business. Most work on teams with others, or must work closely with other teams with separate responsibilities of their own. A cyber analyst, just like with any job for the most part, would benefit heavily from a good sociological education and understanding of the world around them. This will help them heavily in working with their team and others. One such team that may be worked with is some sort of criminal or legal team. This can be a law enforcement team itself, or a legal specialist team within the organization. Having a proper sociologically informed understanding of the law, the courts, law enforcement, and criminal behavior can immensely help when a cyber analyst needs to work with their legal team or law enforcement at large.

In conclusion, a cyber analyst is one of the many careers one can take up within the wider field of cybersecurity. Cyber analysts are responsible for understanding and analyzing the system, which allows them to determine the best methods for which proper procedures, tools, practices, and roles can be implemented to best ensure the success of a network or system. Because of this, the cyber analyst benefits heavily from having an interdisciplinary background that can provide a good sociological basis for their analyses of the various social systems in cyberspace. Despite being a virtual environment, cyberspace was created by humans, is maintained by humans, and used by humans, thus cyberspace is a fundamentally social environment. With this in mind, a proper sociological perspective is vital for a cyber analyst if they wish to succeed.

Source:

https://www.wgu.edu/career-guide/information-technology/cybersecurity-analyst-career.html#close
https://www.cisa.gov/cyber-hygiene-services
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6252333/pdf/fpsyg-09-02133.pdf