

Shamya Curtis

Professor Diawkar Yalpi

CYSE 201S

November 13th 2025

Cybersecurity Analyst

Introduction

A cybersecurity analysts responsibilities consists of watching for threats, responding to security incidents, protecting networks and data by using firewalls and encryption. This job also deals with performing risk assessments to identify vulnerabilities in systems and networks. According to Indeed.com a cyber analyst must have strong planning, organization, and analytical skills, with attention to detail. These professionals must have great communication skills written or verbal and interpersonal skills. This job relies on social sciences and principles such as psychology, behavior economics, sociology. In this job requirements analyst must work with a team of individuals in order to meet their objective when its to train no technical users or collaborate with the organization on data or observations collected. In order to work in a team that requires social skills which ties into this class objective. A cybersecurity analyst has many aspects where they apply social sciences and principles day to day.

How Social Sciences and Principles are applied

One of the daily tasks performed is monitoring network traffic for security incidents and events (*What Does a Cybersecurity Analyst Do?*, 2025). In order for them to know what to look for they have to understand relativism which is all things are related. Security analyst understand how societal behaviors can influence how technology is interacted with. Another task may be when analyst have to coordinate with a security team and document the process of investigation

and recovery. May be tasked with training your fellow employees in best security practices. (*What Does a Cybersecurity Analyst Do?*, 2025). These professionals conduct investigations by monitoring network traffic to detect suspicious behavior and using social science research strategies such as surveys, experiments, field studies, and case studies. These research methods are used to allow analyst to keep up on current trends and how human factors play a role in security incidents. For example analyst might use surveys to collect data on employees to create training or identify potential risks in security practices.

Critical thinking is a soft skill a security analyst must have according to the New England Institute of Technology A cyber security analyst must have strong critical thinking abilities to identify information security risks and threats in a sea of complex codes and software. They must be able to understand the issue and troubleshoot it efficiently. To identify risks and threats in systems an analyst has to understand what to look for on the technical side and socially. Observation of individuals behavior online and in person is the social aspect of it and this is used to detect patterns that indicate a threat.

How do analyst interact with marginalized groups and society

Cybersecurity analyst interact with society and marginalized groups by ensuring cybersecurity awareness training is culturally sensitive and accessible to people from all groups and people from different backgrounds. For example the military conducts annual cybersecurity awareness training that has captions and different language options for individuals who might need those options. This ensures that people who have hearing disabilities or individuals who speak a different language have the opportunity to receive training. Another way these professionals interact with society is they study online trends such as cyberbullying to be able to identify strategies to stop it. Analyst also monitor social media to identify negative content or

cyberattacks aimed towards marginalized individuals in groups LGBTQ+ to collect data on how to create solutions to protect them from cyber abuse.

Conclusion

Cybersecurity analysts draw on multiple social sciences to conduct research, work effectively with an organization and in teams. Their daily responsibilities can deal with “Empowering employees with knowledge is another crucial responsibility. Cybersecurity analysts develop engaging training materials, conduct informative workshops, and cultivate a culture of security awareness within the organization.” (Clark, 2024). Another daily responsibility can be risk management which encompasses identifying threats and vulnerabilities. These daily tasks require a good understanding of social science principles such as sociology when understanding the mind of hackers and their patterns to identify risks. They also use aspects of psychology to understand a hacker’s motivation to prevent future attacks. Analysts rely on social sciences and social principles to better understand human behaviors, interactions with technology or systems to do their daily tasks.

Works Cited

What does a cybersecurity analyst do? 2026 job guide. (2025, October 28). Coursera.

<https://www.coursera.org/articles/cybersecurity-analyst-job-guide>

Clark, J. (2024, June 5). *What does a cybersecurity analyst do?* Merit America.

<https://meritamerica.org/blog/what-does-a-cybersecurity-analyst-do/>

Byrne, S. (2022, January 18). *Cyber security analyst responsibilities*. NEIT.

<https://www.neit.edu/blog/what-does-a-cyber-security-analyst-do>