Network Administrators

Network Administrators are the titans of the cybersecurity realm. They carry the weight of managing, securing, and setting up an organization's networks. I have been a network administrator in the United States Marine Corps for about 3 years, and I have learned so much about the field. The average person sees networking as a hands-on, tech heavy job, but its roots are deeply intertwined with social science and human behavior. Network administrators use social science ideals such as human behavior, criminology, and workplace readiness to prepare for and counter cybersecurity threats.

A networker's daily life can look like many different things; tasks can include, but are not limited to, monitoring the network for suspicious activity, configuring security(firewalls, passwords, etc.), upholding good security practices, configuring networking devices, and many more. These tasks take a lot of training and careful refining of skills, and most notably, they require the person to put in crucial time and effort to complete the task.

When it comes to upholding security, human behavior and psychology play a major role. Network administrators must be alert and predict future attacks or weaknesses by pointing out flaws. Networkers also need to understand policies and strategies and adapt them to their own situation. In the networking field, the most common mistakes are human errors, whether it's clicking a link or messing up configurations; human errors are the leading cause of cybersecurity attacks. Networking isn’t just technical; it’s behavioral. For example, often people will choose the easier alternative and neglect security. This ties into criminology theories such as rational choice, or people will utilize unsafe methods and habits from others, which ties into the social learning theory. That being said, network administrators must focus on being technologically

proficient while also maintaining good practice through proper training, annual awareness training, updating response plans to reduce threats, and countering attackers.

As mentioned previously, Criminology theories play a major part in helping network administrators identify behaviors, but also understand and defend against threats. Routine activity theories and strain theories are two major theories that explain why cybercriminals commit crimes, and they also give critical insight into the 5 W's. This overall allows network admins to better predict attacks and allows us to reduce losses drastically.

Leaning into the sociology aspect of networking administrators, having a productive team and workplace environment contributes to the success of the mission. Networkers are the backbone of communications; they allow communication to flow throughout the workplace. A workplace that protects good cybersecurity practice and upholds the CIA triad is going to prevent human error and mitigate losses. Oppositely, if the workplace environment is reversed, it can cause employees to not hold each other accountable and neglect protocols, leading to higher risk. When we tie these ideas into sociological concepts, we can start to see how firm dynamic and cyber-centered workplace culture contributes to fewer vulnerabilities and threats.

Network administrators serve at the front lines of protecting the users. Network breaches can be devastating, exposing things such as passwords, financial info, personal info, and more. Marginalized groups such as old people, low-income, low-IQ individuals, kids, and more are consistently left vulnerable to cybercrime. Networkers serve as their protectors, protecting the people's sensitive information. Most importantly, networkers hold society together by restoring and maintaining trust in critical infrastructures such as banks, healthcare, schools, businesses, and more.

In my personal experience, social sciences are used on a daily basis in the life of a network administrator. It all starts with training; we train every day and learn how to communicate effectively as a unit and how to identify weak areas in our configurations as well as our people. I often find myself consistently assisting my peers in after-work studying to make sure that my unit is proficient to the expected standard. During training exercises, we study and monitor networks. We also act out incident response plans that are set up. By practicing these training exercises in garrison, we are better able to understand our attackers' behavior and become more proficient in incident response. These training exercises help us better understand the human and technical side of networking and assist in elevating our proficiency to the next level.

In conclusion, Networker administrators are the backbone of the cyber world. They are burdened with managing, securing, and setting up an organization's networks, and oftentimes are tasked to assist in cybersecurity operations. Networker administrators rely on social sciences such as psychology, sociology, and criminology in order to acheive max job proficiency. Network administrators aren’t just all technical; a networker must understand how to think, act, and respond to the attackers and fellow coworkers. By utilizing social science principles, networkers are better equipped to handle the ever-evolving cyber threats and to protect critical infrastructure and civilian assets.

Work cited

Bureau of Labor Statistics, U.S. Department of Labor. “Network and Computer Systems Administrators.” *Occupational Outlook Handbook*, 28 Aug. 2025, www.bls.gov/ooh/computer-and-information-technology/network-and-computer-systems-administrators.htm.

“15-1244.00 - Network and Computer Systems Administrators.” *O*NET OnLine*, National Center for O*NET Development, 24 Feb. 2026, www.onetonline.org/link/summary/15-1244.00

Coursera Staff. “What Is a Network Administrator? A Career Guide.” *Coursera*, 27 Oct. 2025, www.coursera.org/articles/what-is-a-network-administrator-a-career-guide

“Network Administrator Job Description And Salary.” *Western Governors University*, 26 Nov. 2019, www.wgu.edu/blog/network-administrator-job-description-salary1911.html