The Significance of the Systems Administrator

Gabrielle Gaston

CYSE 201S Career Paper
April 13, 2025

Delve into the System Administrator Universe

In society's current digital age, cybersecurity is an essential support for protecting individuals, organizations, and government infrastructures. Within this industry, Systems Administrators play a vital role, often working behind the scenes to ensure the stability, security, and efficiency of computer systems and networks. This is a role I would be interested in pursuing. I am aware that the technical expertise required is extensive, but what is less discussed is the reliance on social science research and principles in this role. Social science, particularly sociology and psychology, showcases not only how Systems Administrators manage workflows but also how they respond to cyber threats, train end-users, and interact with diverse and marginalized populations. This career paper explores how key social science concepts such as cognitive theory, human systems integration, and social engineering influence the daily operations of cybersecurity professionals, particularly Systems Administrators.

To begin, social science research focuses on understanding human behavior and improving societal systems. Cybersecurity professionals, including Systems Administrators, analyze perception to interpret how individuals interact with technology. According to CYSE 201S course material, the purpose of social science research includes testing theories and identifying ways to improve society. In cybersecurity, this translates into evaluating how organizational behavior, communication patterns, and cognitive processing influence security vulnerabilities. In the role, Systems Administrators must understand cognitive theories that explain how users justify risky behaviors online, such as clicking on phishing links or reusing passwords. Recognizing these tendencies allows administrators to create targeted training programs that address faulty thinking and reinforces the importance of ongoing, adaptive cybersecurity training.

Equally important, the Systems Administrator's role also integrates Module 4's principles of Human Systems Integration (HSI). This interdisciplinary approach focuses on optimizing both technology and human interaction. By designing systems that are user friendly and accessible, administrators can reduce user errors and security breaches. This aligns with parsimony, referenced in module 2, the social science principle that advocates for simple, efficient solutions in complex systems. Simplifying user workflows and implementing practical protocols fosters safer environments for all users, especially those from overlooked groups who may lack advanced digital literacy. For this reason, human factors play a critical role in security fatigue, a phenomenon where users are overwhelmed by security protocols. Systems Administrators, influenced by psychology and sociology, must recognize signs of fatigue and adjust systems or training accordingly to maintain compliance and engagement. Human oriented design becomes a form of inclusive cybersecurity by bridging the gap and reducing barriers for underrepresented users through ensuring fair access to secure systems.

Similarly, effective communication is another key area where social science intersects with the Systems Administrator's responsibilities. Cybersecurity professionals must communicate technical information to individuals from executives to everyday users. This requires understanding audience perspective, conforming your tone and the delivery to engage your audience, while also recognizing social dynamics. Administrators frequently write reports, deliver presentations, and listen to user concerns, all of which require interpersonal, and communication skills grounded in social science methodologies. For this reason, social engineering attacks including, phishing, highlight the necessity of psychological insight. Understanding how hackers manipulate human behavior allows Systems Administrators to build

more robust defenses and inform users of these threats. These efforts are particularly important for individuals that may be targeted due to lack of access to cybersecurity education or resources.

Hence, the practice of risk assessment exemplifies how social science contributes to strategic decision making in cybersecurity. Systems Administrators conduct risk assessments not just through technical audits, but by evaluating how social behavior influences vulnerability. They assess who is most at risk, what behaviors need adjusting, and how to deploy resources effectively skills rooted in sociology and psychology. Furthermore, Module 12's inclusion of cybercriminology serves as a reminder that cybercrime has real world consequences that often reflect societal inequalities. Systems Administrators who recognize these patterns can advocate for policies and procedures that protect vulnerable users and ensure access to secure systems.

The role of a Systems Administrator in cybersecurity is far more than a technical occupation. It serves as a discipline deeply interconnected with social science principles. From understanding cognitive biases and social behavior to enhancing communication and supporting marginalized communities, Systems Administrators rely on sociology and psychology to inform their daily tasks and broader cybersecurity strategies. Through integrating human-centered approaches with technical expertise, these professionals build safer, more inclusive digital environments that reflect the goals of protecting people and improving society in both cybersecurity and social science.

References

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. MIS Quarterly, 39(4), 837–864. https://doi.org/10.25300/MISQ/2015/39.4.5

Mitnick, K. D., & Vamosi, R. (2021). The art of invisibility: The world's most famous hacker teaches you how to be safe in the age of big brother and big data. Little, Brown and Company.

National Institute of Standards and Technology (NIST). (2023). Framework for improving critical infrastructure cybersecurity (Version 2.0). https://www.nist.gov/cyberframework

Coursera. (2025). What Does a System Administrator Do? Your Career Guide https://www.coursera.org/articles/what-is-a-system-administrator-a-career-guide