Jake Modelewski

CYSE-201S

Bora Aslan

April 13, 2025

Systems and Security Engineering

There are so many different paths to choose from in cybersecurity. Each job offers many different struggles, rewards, work, and challenges. I have chosen to write about my current job in cybersecurity, IT Systems and Security Engineering or also referred to as Systems Administrator. I am currently a senior level systems engineer for Old Dominion University (ODU)/Eastern Virginia Medical School (EVMS). I will describe how my current role relates to the principles of social science and the course material we have covered thus far.

Being a system engineer includes a wide range of responsibilities. You have to cover everything from phishing attacks to building servers for intricate use to implementing new infrastructure. Beginning with phishing attacks, ODU faces countless attempts of bad actors attempting to be high ranking officials withing the company or other state/government organizations in attempt to gain credentials or monetary value. As a system engineer it your role to understand why and how they attempt to cyber victimize your users. To understand this, both archival research and in-field research is needed.

Using archival research, one would read published articles, forums, and informational sites detailing about common and/or new attacks that are gaining popularity. Using an in-field research one may either receive one of the attacks yourself or get a forwarded email from a user who received one. Using the information you've gathered from these studies; you must use objectivity and relavitism to determine the best protections to equip your organization from bad actors. Often comparing several factors such as cost, effectiveness, ease of use, etc.

As an engineer, you must connect with your users and educate them on cybersecurity and the threats that persist. "We recently conducted research about the effects of phishing training, where we compared our users' abilities to resist phishing attacks before and after participating in our training. The research showed that after continuous phishing testing and awareness training, our users had a 60% reduction in mistakes made during simulated phishing attacks. During the first test, an average of 15% of recipients submitted the personal information requested by the "cybercriminal." By the third phishing test, that number went down to only 6% of employees." (Gundersen, 2025). One must use parsimony in order to effectively educate a user. In my personal experience, the majority of users will not understand your technical jargon. "User training is a persistent challenge, particularly as new technologies and solutions are implemented. They must develop comprehensive training programs that cater to diverse user groups with varying levels of technical proficiency. Ensuring users understand and adhere to security policies is critical to prevent breaches and data loss." (Pateriya, 2024)

Aside from the victimization of the user and the organization, money and economic impact is directly related with cybersecurity and an engineer's roles to strengthen an organization's security. "In 2020, Premera Blue Cross settled potential violations of the HIPAA Rules and paid a $6,850,000 penalty to resolve its 2015 data breach of the PHI of almost 10.5 million individuals, and in 2021 a $5,000,000 settlement was agreed upon with Excellus Health Plan to resolve HIPAA violations identified that contributed to its 2015 data breach of the PHI of almost 9.4 million individuals." (Alder, 2025) While most cases of ransomware and other malicious attacks aren't costly because of organizations paying hackers, it's HIPAA fines from the Office for Civil Rights to companies for not being able to protect patient's data.

There are my direct connections between the principles of social sciences along with the practices of social science within the daily responsibilities of a system engineer. Any field of IT deals with people in some capacity or another. Understanding the many facets and practices of social science allows us to better understand threats and perform our jobs more effectively.

Works Cited

Alder, S. (2025, 4 20). *Healthcare Data Breach Statistics*. Retrieved from The HIPAA Journal: https://www.hipaajournal.com/healthcare-data-breach-statistics/

Gundersen, G. M. (2025, 1 5). *Does phishing training work? Yes! Here's proof*. Retrieved from CyberPilot: https://www.cyberpilot.io/cyberpilot-blog/does-phishing-training-work-yes-heres-proof

Pateriya, S. (2024, 7 10). *15 Biggest Issues IT Faces Today in 2025*. Retrieved from Scalefusion Blog: https://blog.scalefusion.com/top-it-challenges/