Career Paper: Risk Management Framework Cybersecurity

Derrick Amissah

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 11/13/2025

Introduction

Risk Management Framework (RMF) Cybersecurity Analysts play an essential role in an organization's computer systems and operations, utilizing technical and insights from the social sciences to complete their roles (National Institute of Standards and Technology, 2018). They maintain confidentiality and integrity daily while relying on knowledge from various social science disciplines to provide safe and welcoming cyber environments for all (Carnegie Endowment for International Peace, 2023). This paper will outline how RMF Cybersecurity Analysts rely on social science research in their day-to-day operations, especially working with marginalized populations and the general population.

The Use of Social Science Research in RMF Cyber Roles

RMF Analysts consider their risks through the lens of how people act and how organizations operate, relying on basic principles of social science research. Analyst psychology offers insight into how stress, fatigue, and cognitive overload lead people to make security errors (Alfadhli & Migliavacca, 2024). Analysts also incorporate motivational psychology to implement training curricula that allow employees to learn how to create safer digital footprints and avoid phishing or social engineering.

Sociology gives RMF Analysts insight into how workplace culture, peer pressure and informal groups either promote or debilitate compliance with cybersecurity policies. Analysts leverage sociological constructs for more effective messaging in cybersecurity implementation and access to solutions to report concerns or issues (National Institute of Standards and Technology, 2018). Criminology provides insight into trends with cyber threats, research on crime and patterns, and effective development of incident response plans.

Daily Application of Social Science Principles

An RMF Analyst's job is to write policies, respond to incidents, implement technical controls, and monitor security systems all day, all through the lens of social science concepts. For example, policy writing means assessing culture, values, beliefs, and regulating structures from an anthropological perspective to implement regulations that are effective and equitable for all (Carnegie Endowment for International Peace, 2023).

Incident response implements criminology to ensure evidence is collected appropriately, and threats are mitigated adequately. There is also a level of training and communication that occurs that respects multiculturalism and makes interdisciplinary training and interactions easier and therefore more effective (Alfadhli & Migliavacca, 2024).

Interaction with Marginalized Groups and Society

It's the responsibility of RMF Analysts to champion vulnerable populations who are at increased risk due to limited resources, lower tech savviness, or issues with language translation (Carnegie Endowment for International Peace, 2023). These gaps are established through social science research which enables Analysts to develop security training that's easier, with less complex controls and a more straightforward approach to reporting and response. An Analyst can also advocate policy changes that maintain privacy rights and avoid inadvertent digital discrimination.

Furthermore, championing vulnerable populations extends to community engagement and awareness programs supported through psychology and anthropological study to ensure that security isn't merely a technical application but a matter of equity, trust, and respect for all (National Institute of Standards and Technology, 2018).

Conclusion

Risk Management Framework Cybersecurity Analysts demonstrate that social science research bolsters technical security strategies, and facilitates equitable, impactful risk treatment. These professionals incorporate concepts from the fields of psychology, sociology, criminology, and anthropology to cultivate better organizations and digital equity for vulnerable populations. Therefore, by standing upon a socially scientific ideal, RMF experts ensure that cybersecurity comes naturally for today's society, safely and inclusively for all.

Citation

Alfadhli, A., & Migliavacca, A. (2024). Psychological insights into cybersecurity practices: The role of human factors. Journal of Cybersecurity Research, 10(2), 45-60.

Carnegie Endowment for International Peace. (2023). Cyber resilience must focus on marginalized individuals, not just institutions. https://carnegieendowment.org/research/2023/03/cyber-resilience-must-focus-on-marginalized-individuals-not-just-institutions?lang=en

National Institute of Standards and Technology. (2018). Risk Management Framework for Information Systems and Organizations (NIST SP 800-37 Rev. 2). https://doi.org/10.6028/NIST.SP.800-37r2