Career Paper

Ray Montes Jr.

6 August 2025

Being a cybersecurity analyst is a technical job that is normally perceived as being a technician with one task of watching over threats, security logs, and firewalls. Nevertheless, the players in this industry also rely extensively on the impact of social sciences. Knowledge of human behavior, social interaction and ethical decision making is essential to the development of safe digital environments. This paper investigates the way social science concepts, i.e. human behavior, organizational culture, and ethical frameworks are applied in the everyday life of cybersecurity analysts. Such concepts are essential to not only success in technical terms but also encourage the ethical and inclusive security practices that can be more relevant to marginalized populations.

Among the important aspects that I have learned is the fact that most of the cybersecurity failures are through human error and not merely technical breakdowns. Psychology and behavioral science are helpful tools to the cybersecurity analyst since they determine why users are fooled by phishing emails, use weak passwords more than once or flout security protocols. According to Bada and Nurse (2019), the human element is still the greatest vulnerability used in breaching cybersecurity. Analysts use this information in carrying out phishing exercises, behavior-based alerting, and assist organizations create user friendly policies that take into consideration the natural tendencies of people.

An example of this would be that an analyst may realize that the same person is causing repeated failed log-in attempts and this may not be a brute force attack but rather, a struggling staff. They should suggest user training or login assistance instead of giving them a penalty. Here they

should include empathy and behavioral understanding into the solution. These everyday choices illuminate how social science assists reporters to translate settings, not only code.

Security culture is another concept that encompasses attitudes, values, and practices shared by people that determine their perception of cybersecurity in an organization. Analysts also tend to contribute to the creation of this culture since they analyze the staff attitude, promote reporting, and develop communication strategies. The Uchendu et al. (2021) note that technical controls on their own are not sufficient to support effective cybersecurity because leadership involvement and user engagement are important.

This is implemented in a cybersecurity analyst since it entails assisting both HR and IT departments in conducting awareness campaigns, conducting training, and maintaining nonconfrontational language. As an example, as opposed to shaming employees who might have clicked on a malicious link, an analyst could promote the concealed reporting and instruction-oriented reactions. They also localize communications to address the demand of various departments, levels of education and even cultures to make it inclusive throughout the organization.

The other social science concept that is deeply incorporated in the role of the analyst is ethical decision making. Whether it be striking a balance between user privacy and network surveillance, or when to upscale an occurrence, the decisions an analyst makes have far reaching ethical connotations. De Bruin and Mersinas (2024) did an empirical study using more than 37,000 behavioral records data and reported that the determining factors in inducing secure behavior were national culture, security awareness, demographic factors as well as their previous experience. According to them, knowledge of these variables permits organizations (and

cybersecurity analysts) to design interventions and communications to various employee groups with no bias and enhance results among varied populations.

To give a specific example, in the design of the security procedures, analysts will need to think about the disproportionate impact that monitoring tools could potentially have on nonnative speakers or employees of different cultural backgrounds. By accident a pattern detecting system may pick out such individuals. Methods of social science, informed analysts tend to be more inclined to detect these risks and promote accessible practices that promote inclusivity regardless of the type of training material in the form of texts or accessible formats, hence equity and respect towards marginalized groups.

As it is done in reality, the day of a cybersecurity analyst begins with checking the messages related to the systems such as Security Information and Event Management). In case of the missing authentication, the suspicious log in, or the user behavior, the analyst will use the knowledge of psychology and sociology to determine whether the action is rogue or unintentional. They could then report it to the non-technical/management staff, which would need clear culturally sensitive language. During the day they will work with others on enhancing awareness training and formulating policies that consider not only the security requirements, but also the welfare and fairness of the employees.

In conclusion, cybersecurity analysts are not only specialists in the technical sphere, but they are also behavior sciences, communicators, and ethical decision makers. The course helps demonstrate precisely how social science concepts such as human behavior, organizational culture, and ethics can be used in the day-to-day practice of cybersecurity experts. The analysts that adopt these principles are placed in a better position to safeguard systems in a manner that is efficacy, equitable and all inclusive. With cyber threats increasingly becoming more humanized,

that is more human and social based, the importance of social science in cybersecurity will continue gaining value.

REFERENCE

de Bruin, M., & Mersinas, K. (2024, May 29). *Individual and contextual variables of cyber security behaviour -- an empirical analysis of national culture, industry, organisation, and individual variables of (in)secure human behaviour*. arXiv.org. https://arxiv.org/abs/2405.16215

Bada, M., & Nurse, J. R. C. (2019, September 29). *The social and psychological impact of cyber-attacks*. arXiv.org. https://arxiv.org/abs/1909.13256

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021, June 28). *Developing a cyber security culture: Current practices and future needs*. arXiv.org. https://arxiv.org/abs/2106.14701