Marshal Harris

Bora Aslan

Cybersecurity and the Social Sciences

14 April 2025

Social Science Principles Found in the Role of an Information Systems Security Manager

The position of an Information Systems Security Manager (ISSM) doesn't only require technical aptitude involving policy development, strategic planning, as well as network security but they also rely heavily on their understanding of social science principles like objectivity, parsimony, and ethical neutrality for decision-making that keep their network operating efficiently, with minimal downtime and most important, safely. ISSMs need to ethically manage their information systems, navigate their workplace's social dynamic, and address risks that might affect marginalized communities that may fall within their purview.

The Use of Objectivity in Threat Assessment

Objectivity when used by an ISSM is the idea of conducting an impartial analysis and having no bias with the results that are presented. ISSMs can do this by creating security practices or implementing protocols that are based on facts rather than having any influence that may come from social stigma or assumptions. "They separate fact from value and are concerned with perfecting methods and techniques to collect value-free, unbiased facts." (Cecez-Kecmanovic 25). ISSMs will have to make sure when identifying threats, that unfair practices and profiling aren't being implemented especially if non-human tools or poorly trained technicians are being utilized for risk assessment and threat identification.

Designing Systems and Solutions with Parsimony in Mind

With the use of the principle of parsimony; keeping things simple and minimizing complexity when able is at the forefront of an ISSMs mind. Their network architecture should be able to mimic the principle. Creating simple yet effective cybersecurity solutions will enable repeatability and measurable results that can be scaled up or down to fit the criteria that can be used by underfunded non-profit organizations or companies that have been continually in the black. With the use of parsimony-styled solutions, the division between security practices can be lessened to ensure equitable access to secured systems for marginalized populations.

Evidence Drives Security Practices Through Empiricism

An ISSM has to monitor many things within their environment. Being able to employ empiricism to rely on data that can be seen or experienced is crucial to making sound decisions when security vulnerabilities are identified. The human element that can cause a phishing attempt to succeed or for a user to have a lapse in judgment allowing an uncleared executable file to be ran that introduces malware into the network isn't something that will always happen as the textbooks write it. "The stronger the intention to comply with information security policies is, the more likely it is that the individual will actually comply with the information security policies" (Siponen et al. 136). Behavior-based security practices such as phishing simulations, or testing group policies before and after they have been implemented can be very effective in targeting where more focus will need to be placed to ensure users that have less digital literacy, but more prominent roles to play can still be effective within the organization.

Ethical Neutrality within Systems

Ethical Neutrality requires an ISSM to make sure they stay fair and non-discriminatory with their execution of security practices. This can become tough depending on where their system is located and what the purpose of their system is. With a system designed for public safety, it would be tough for an ISSM to challenge the authority of superiors when elevated privileges are requested without using the proper channels, though it can become a slippery slope into the violation of an individual's privacy and civil liberties. It maintains the role of the ISSM to enforce policies that have been implemented that will balance the safety of all and respect all the rights that are available to all persons.

The role of the ISSM is vast and ever-changing, just the same as the landscape cyber practitioners find themselves in. The skills needed will continually need to be advanced as technologies change, and practices advance. However, with the use of operational necessities such as social science principles like objectivity, parsimony, and ethical neutrality, ISSM can continue to be effective members in ensuring network security, proper training, sound judgment, ethical practices, transparency, and equity among all individuals they serve.

Work Cited

Siponen, Mikko, Pahnila, Seppo, and Mahmood, Adam. “Employees’ Adherence to Information Security Policies: An Empirical Study.” *IFIP International Federation for Information Processing*, vol. 232, 2007, https://doi.org/10.1007/978-0-387-72367-9_12. Accessed 10 April 2025.

Cecez-Kecmanovic, Dubravka. 2005. “Basic assumptions of the critical research perspectives in information systems.” Pp. 19-46, https://doi.org/10.4337/9781845426743.00009. Accessed 11 March 2025.