Over the course of my career paper, I will discuss the organizational roles and responsibilities of a chief information security officer (CISO), describe how CISO's require and depend on social science research and social science principles, how key class concepts of social science research methods, cognitive theories of cyber offending are applied in the CISO field and their daily routines. Additionally, I will discuss how the CISO career field relates to marginalized groups and society in general.

A CISO is a senior-level executive responsible for developing and implementing procedures and policies designed to protect an organizations enterprise communications, systems, and assets from internal and external threats. CISO's routinely report to and work alongside with the organization's chief information officer to ensure their information security program aligns with the organizations strategic objectives and meets regulatory compliance rules dependent on the type of data processed. With the overall responsibilities of a CISO delineated, how do CISO's depend on social science research and principles to be effective at their job and maintain relevance in the field?

A CISO's depend not only on existing security frameworks, implementation of policy and procedures based on NIST or ISO compliance standards to secure their organizations data, systems, and assets but also an understanding of human factors and behaviors of both attackers and authorized users. Understanding what drives and influences human factors and user behavior is a critical component of a mature cybersecurity program. Social science disciplines like psychology, sociology, and behavioral economics can reveal important answers as to why social engineering attacks are so successful, how risk is perceived by individuals and expose motivations behind online behaviors. In particular, these types of research have informed CISO's of the negative consequences of implementing technological solutions to enhance cyber security

without first taking into consideration social and behavioral dimensions. Noting that when behavioral changes are made: mandatory password changes and implementation of onerous security procedures, perceptions of security technology as an "obstacle" may form, subsequently users "may mistrust, misinterpret, or override the security" (Pfleeger & Caputo, 2012). Understanding social and behavioral dimensions can assist CISO's in tailoring existing technological solutions to fit a more human-centric design, implement training programs that increase user buy-in and reduce the likelihood of human error and cognitive overload contributing to potential cybersecurity breaches: "by both understanding the role of human behavior and leveraging behavioral science findings, the designers, developers and maintainers of information infrastructure can address real and perceived obstacles to productivity and provide more effective security" (The Psychosocial Dynamics of Cyber Security, 2016). In establishing the need for CISO's to apply social science research in concert with existing technological measures and solutions to be effective and relevant in their field, we must consider that social science principles are also relevant and integral to a chief information security officers' day to day routines and continuing education. Over the course of the next paragraph, we will discuss how they apply these principles.

When we consider the social science principle of relativism it is understood to mean that all things are related. From a CISO's perspective, understanding that changes in one system leads to changes in other systems can influence decisions on strategic security policies and effective business continuity plans. This can be applied by using historical trend analysis, and case studies from similar organizations. Learning from past security incidents, breaches failures, and successes to inform current decisions. Second, the principle of objectivity involves looking at facts by separating personal viewpoints and interpretations. An application of this principle

applies to the inevitable investigation that follows a cyber incident or breach. CISO's must retain objectivity in the face of facts that may implicate friends or colleagues or have negative connotations for individuals with which they have a personal or professional conflict. Third is the principle of parsimony which advocates for keeping a level of explanation as simple as possible. CISO's apply this principle to security architecture and design, risk assessment and mitigation, and incident response and recovery favoring easily explainable, efficient, and simple solutions over elaborate measures and designs. CISO's apply the third social science principle of ethical neutrality through actions of transparency and disclosure. Disclosure of cybersecurity risks must be accurate and timely but also truthful and complete (Securities Exchange Commission, 2023) The last principle determinism means that behavior is caused, determined, or influenced by preceding events. They apply this using by conducting risk assessment and behavior modeling using social dynamics prompting them to consider organizational hierarchies, communications, and culture, along with employee behaviors. This influences resource allocation, mitigation strategies and overall collaboration efforts.

This next section delves into how key class concepts apply to the chief information security officer field and their daily routines. First would be the use of common social science research methods that CISO's rely on to inform their decision making. Using surveys to collect data about employee's security policy adherence and perceptions of an organizations security statues helps gauge security awareness and identify potential vulnerabilities. Controlled experiment to test the effectiveness and impact of new authentication methods could be applied. CISO's can also utilize field studies by participating in incident response exercises and audits or apply a multimethod research approach through a mix of surveys, interviews, archival data, and field observations to validate findings and ensure a broader view of their organization's

cybersecurity status. Second is the application of cognitive theories of cyber offending to build risk mitigation strategies. Neutralization theory gives CISO's insight into how cybercriminals use denial of responsibility or victim injury to justify their behavior. They can then apply these concepts to better understand insider threats, by educating employees about ethical norms and potential consequences of unethical behavior, encouraging an ethical organizational culture to better detect and counter potential insider threats.

Finally, how does the chief information security officer field contribute to both marginalized groups and society in general. Being a chief information security officer isn't about making decisions in a vacuum or retaining a narrow worldview. It requires a broader viewpoint that leverages a collective knowledgebase, to be truly effective. This includes people of different backgrounds, genders, and ethnicities to foster creativity, innovation and bring fresh perspectives to complex problems encountered in the field. Promoting this type of environment encourages a culture of digital literacy and ensures that everyone can protect themselves, their community and society from cyber threats.

References

The Psychosocial Dynamics of Cyber Security: An overview. (2016). *Psychosocial Dynamics of Cyber Security*, https://doi.org/10.4324/9781315796352-10

Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, *31*(4), 597–611. https://doi.org/10.1016/j.cose.2011.12.010

Securities Exchange Commission (2023, July 26). https://www.sec.gov/news/press-release/2023-139