**Cybersecurity Career Paper: Chief Information Officer (CIO)**

David R. Allen

Department of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Professor Diwakar Yalpi

November 24, 2024

**Introduction**

Cybersecurity isn’t only about how technology should be protected. In fact, many other disciplines are utilized in the realm of cybersecurity, including social science. One example of this is a chief information officer. This paper will analyze the roles of the chief information officer and how they relate to the principles of social science, key concepts from the course, marginalization, and how the career connects to society.

**Social Science Principles**

 Many social science principles are used within the duties of the CIO. The first principle that relates to a CIO’s duties is parsimony. With parsimony, scientists, or in this case the CIO, should keep explanations as simple as possible. One task of the CIO is to report their technical findings to the chief executive officer (CEO) (Stephens et al., 1992, p. 465). This must be done in a language that the reporting officer might understand, so CIO’s must be avoid using technical jargon when reporting to those not familiar with technology (Stephens et al., 1992, p. 465).

 The second principle is objectivity. CIO’s take a lot of information in from other aspects of the company and write reports (Stephens et al., 1992, p. 465). This information used in written reports must be factually correct without a strong bias. Opinions should not shape their conclusions of this research done within the company.

 The third principle that relates to a CIO and their duties is determinism. A CIO has to be able to delegate tasks to lower managers and conduct meetings (Stephens et al., 1992, p. 465). This might involve getting to know how workers behave based on feedback from lower management based on meetings. Since determinism is about why individuals engage in certain behaviors, this might be important to a CIO to lower management in order to utilize their workers in a technological department more effectively.

 The fourth principle important for CIO’s is relativism. The CIO is responsible for everything IT related in the company and utilizes technology to support an organization’s business strategy (Gottschalk & Taylor, 2002, p. 7). Looking at relativism from a systems perspective, a change in one system can lead to a change in another system. This is where a CIO must adapt with an organization’s business strategy to utilize the proper technological enhancements when necessary, so that the business can function properly (Gottschalk & Taylor, 2002, p. 7).

**Concepts**

Many concepts from class can be utilized in the CIO role. The first concept is human systems integration. Human systems integration focuses on human behavior and understanding the impact and consequences of technological systems. Many CIO’s show attributes based on four different types of CIO’s, those being the landscape cultivator, innovator & creator, triage nurse & firefighter, and opportunity seeker (Chun & Mooney, 2009, p. 329). CIO attributes of a landscape cultivator are a good communicator and being able to lead change (Chun & Mooney, 2009, p. 329). CIO attributes of the innovator & creator are able to make empowered decisions and being ethical (Chun & Mooney, 2009, p. 329). CIO attributes of the triage nurse & firefighter are capable of problem solving, able to lead change, and technical experience (Chun & Mooney, 2009, p. 329). CIO attributes of the opportunity seeker are highly analytical, good at prioritization, understanding of process improvement, and experienced at outsourcing (Chun & Mooney, 2009, p. 329). All of these attributes are beneficial for CIO’s that focus on human systems integration because they intertwine with the focus on human behavior and technology, therefore making CIO’s more resourceful at their jobs who possess these attributes.

 Not only do CIO’s think about technology and their workers, but technology and society as well (Korn Ferry, 2011). The second concept is sociology. A CIO must consider how the technology and their company can benefit society alongside their workers (Korn Ferry, 2011). This relates to the sociological paradigm of structural functionalism, how cybersecurity at the societal level meets important societal functions. A CIO must understand how society makes money off of cybersecurity, or technology in general, for the better of the company and keep it in business. They must keep up with technological developments from other companies, like Apple, and use their technologies for their own improvement (Korn Ferry, 2011). A CIO of a social media platform, like Facebook, might study societal interactions with their platform to see what attracts users to the platform (Korn Ferry, 2011). A CIO that thinks like a sociologist can be a big advantage for a company.

 A third concept that a CIO relates to is personality. A job that shares similar responsibilities to a CIO, just more focused on the security side, is a CISO (LIOP, 2023). For example, a CISO or CIO might look for a potential threat with the personality of a hacker (LIOP, 2023). Some personality traits of a hacker mentioned in the course include social anxiety, introversion and extraversion, openness to experience, conscientiousness, and agreeableness. Another trait that could also be considered is low self-esteem, where individuals might have greater tendencies to look for vulnerabilities (LIOP, 2023). Higher ups, including a CIO, might want to watch over those who show these personality traits to make sure policies are being met to standard and avoid security breaches (LIOP, 2023).

 The fourth concept from class that relates to a CIO is cybersecurity awareness and its relationship with psychology. One responsibility of a CIO is to be the overhead for training (Wilson & Hash, 2003, p. 15). They must be able to plan the awareness and training program and make sure the organization understands the processes of the program (Wilson & Hash, 2003, p. 15). When increasing awareness about cybersecurity, training must occur, be ongoing, evolve to new cyber risks, and focus on human behavior as the main cause of security incidents. Some examples that an organization might use as techniques and materials for cybersecurity awareness include posters, newsletters, screensavers, web-based sessions, and teleconferences (Wilson & Hash, 2003, pp. 44-45). Some examples of techniques for training material might include interactive videos, web-based training, non-web training, or onsite training (Wilson & Hash, 2003, p. 46). Repetition of these messages and training can help maintain employee retention of the program material so that the correct behaviors can be enforced in the workplace (Wilson & Hash, 2003, p. 45) A CIO could use tracking system to monitor compliance and the effectiveness of awareness and training programs, which can give the CIO an idea on how to revise the program if certain aspects are ineffective (Wilson & Hash, 2003, p. 48).

**Marginalization**

The CIO position has had issues getting people of color and women to sign on in these positions in some higher education institutions (Maringe & Ojo, 2017, p. 131). Many women tend to go the adjunct professor route due to their roles in society, like as a mother or to serve out a marriage, for example, and are often discouraged to go the executive route (Maringe & Ojo, 2017, pp. 132-133). The ethnic and gender imbalance in many executive positions is made up of a lot of white males, contributing to the discouragement of ethnics and women in this role (Maringe & Ojo, 2017, p. 139). A lot of these roles have power over the hiring process and promotions, hindering women and ethnic groups from being hired or advancing into higher roles as an executive (Maringe & Ojo, 2017, p. 139).

 My first challenge leads into my second challenge, which is diversity hiring (George & Baskar, 2024, p. 9) Because of the lack of representation of women and minorities, the IT industry must focus on diverse hiring and inclusion in the workplace (George & Baskar, 2024, p. 9). Organizations must utilize non-biased practices to govern AI and their algorithms to make sure marginalized groups don’t face discrimination due to an algorithm (George & Baskar, 2024, p. 9). Training should involve empathy building to reinforce retention and psychological safety (George & Baskar, 2024, p. 9).

 The last challenge relates to the LGBTQ community and those that work in STEM, including a CIO. LGBTQ professionals that work in a STEM career are 30% more likely to encounter workplace harassment compared to non-LGBTQ workers (Langin, 2021). The LGBTQ community is also more likely to experience other challenges, like social exclusion and professional devaluation (Langin, 2021). This might cause LGBTQ workers to leave the STEM field altogether (Langin, 2021). This data can provide a better focus on LGBTQ careers and the STEM field, and possibly lead to ways to include the community in the career and make them feel safer in their line of work (Langin, 2021).

**Connection to Society**

A CIO can help push boundaries and provide great digital change when it is necessary. They can provide great technological advancements for future educators, for example, especially in a time of crisis, such as the COVID-19 pandemic. A case study talks about an interim CIO that also wants to become a university’s chief digital officer, or CDO (Panteli, 2024, p. 1). She believes that she can be a great influence for digital transformation if given this position (Panteli, 2024, p. 1). The university decides to give her a role that is a combination of the two, since they believe that it would be beneficial to have a role that can provide digital change, along with typical CIO duties that university needs as well (Panteli, 2024, p. 1). This CIO shows great initiative that every CIO should have in order to make changes. Being able to have initiative can then promote a better future for society in general by providing universities the best technological advancements to both students and faculty, giving them higher quality education.

 A top management position, like a CIO, can have a huge reflection on the company. A concerning issue within an organization is white-collar crime, specifically fraud (Zahra et al., 2007, p. 122-139). Committing fraud can have severe consequences on an organizations’ shareholders, employees, and ruin the company’s reputation and credibility (Zahra et al., 2007, p. 123). Stock prices can plummet and then the public might not trust the company anymore (Zahra et al., 2007, p. 123). Not only that, but when one person in a company commits this kind of behavior, more would be likely to do so (Zahra et al., 2007, p. 124). If a company is involved in unethical and illegal behavior, society will more than likely want to distance themselves from the organization.

 With both good and bad instances in consideration, a CIO might want to have high ethical standards, along with a drive for change. These are important for a successful CIO in society. A CIO who does good and promotes change can lead a company to greater success and be beneficial to society. On the other hand, one with lower ethical standards could lead to a life of crime within the organization. This lifestyle can spread to others in the organization, poisoning the organization as a whole, which can result in a society that looks down on the individual that caused this and even the organization for encouraging criminal behavior. It’s up to the CIO how their image is represented in society, along with the company they are hired by and represent.

**Conclusion**

 In conclusion, the CIO is a vital role for technology in the company. They share many responsibilities that relate to the social science principles, including parsimony, objectivity, relativity, and determinism. Social science concepts related to the CIO are shown such as human systems integration, sociology, personality, and the psychology of cybersecurity awareness. Marginalization challenges related to this career are gender and ethnicity in higher education, diversity hiring, and including the LGBTQ in STEM careers. The connection between the CIO and society is also discussed in the aspects of morals, beneficial traits, and criminal behavior.

**Works Cited**

Chun, M., & Mooney, J. (2009). CIO roles and responsibilities: Twenty-five years of evolution and change. *Information & Management*, *46*(6), 323-334. <https://doi.org/10.1016/j.im.2009.05.005>

George, A. S., & Baskar, T. (2024). Driving business transformation through technology innovation: emerging priorities for IT leaders. *Partners Universal Innovative Research Publication*, *2*(4), 1-14. <http://www.puirp.com/>

Gottschalk, P., & Taylor, N. J. (2002). *Strategic management of IS/IT functions: the role of the CIO*. In *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences* (pp. 1-10). IEEE. <https://doi.org/10.1109/HICSS.2000.926956>

Korn Ferry. (2011, April 19). *We are all sociologists now*. <https://www.kornferry.com/insights/briefings-magazine/issue-6/140-we-are-all-sociologists-now>

Langin, K. (2021, January 15). *‘This deserves our attention.’ New data highlight LGBTQ scientists’ workplace challenges*. Science. <https://www.science.org/content/article/deserves-our-attention-new-data-highlight-lgbtq-scientists-workplace-challenges>

LIOP. (2023). *How a CISO uses social science research*. Critique. <https://vocal.media/critique/how-a-ciso-uses-social-science-research>

Maringe, F., & Ojo, E. (2017). *Sustainable transformation in African higher education: Research, governance, gender, funding, teaching and learning in the African University*. Springer. <https://d1wqtxts1xzle7.cloudfront.net/57592087/2017_Book_SustainableTransformationInAfr-libre.pdf?1539929579=&response-content-disposition=inline%3B+filename%3DSustainability_of_Higher_Education_Credi.pdf&Expires=1731005742&Signature=PT9qUJhfChAtl6DkFJzSQXBBVvFKEj5w1N7kNhbIv9Azmm4li4zQ4z0o-G3hmkzQjeBnsbCg9q6OgTLJaIj2hrGYCp7c1apGOWSWlW4EkZB2gOARIPsAAO9Ebhypxk4fFrPIPNDRSvlezP4EQip3DvuONNb7XokoVGP3kGkN5XGhUHg1JuESTXnmryFfjWLwWx6lYWORulDjgDTTTDQO4P9~QzyqK-My1zTRae7IIO2d4J~FcDmbMn0geTaqeWmBXzxRYlBqGNLdEa72ViObslat39Ep847PhuhYlchLImTkvx4RZlu2d67F3t~1iNQ2okXmCJJUXnfCQfKqRy5~DA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA#page=133>

Panteli, N. (2024). Leading digital transformation: Dilemmas of a chief digital and information officer. *Journal of Information Technology Teaching Cases*, *0*(0), 1-4. <https://doi.org/10.1177/20438869241248198>

Stephens, C. S., Ledbetter, W. N., Mitra, A., & Ford, F. N. (1992). Executive or functional manager? The nature of the CIO's job. *MIS Quarterly*, *16*(4), 449-467. <https://doi.org/10.2307/249731>

Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. *NIST Special Publication 800-50*, 1-71. <https://doi.org/10.6028/nist.sp.800-50>

Zahra, S., Priem, R., & Rasheed, A. (2007). Understanding the causes and effects of top management fraud. *Human Resource Management International Digest*, *15*(7), 122-139. <https://doi.org/10.1108/hrmid.2007.04415gad.001>