Cybersecurity Workforce Management's Position in Society and its Relation to the Social Sciences

Gregory S. Oehm

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Prof. Diwakar Yalpi

April 13, 2025

Introduction

Cybersecurity is inherently interdisciplinary. Consequently, cybersecurity, and the many careers one might obtain within it, are typically closely related to the social sciences. One such role is that of cybersecurity workforce management. Though the title and precise responsibilities of this kind of job might vary from organization to organization, as described in the NICE workforce framework, some common duties are present, including creating security strategies for the organization, writing policies, providing cybersecurity awareness and training to employees, hiring the necessary personnel, and overseeing compliance with organizational and government regulation (*NICE Workforce Framework for Cybersecurity*, 2025). The actions required of cybersecurity workforce managers are closely associated with the research, principles, and concepts of the social sciences, as well as society as a whole, with their relation to marginalized groups being of particular interest.

Connection to Social Science Principles and Research

Though nearly all careers within the field of cybersecurity require at least some knowledge of the social sciences and related research, cybersecurity workforce management is perhaps one of the roles within cybersecurity most connected to the social sciences. Major components of the job involve effectively managing and understanding the people within an organization and their needs. Cybersecurity workforce managers would be partly responsible for much of the personnel in an organization, and must communicate the need for training and funding related to the organization's cybersecurity (*NICE Workforce Framework for Cybersecurity*, 2025). As such, those with this job need to know how social interactions are facilitated and impacted by outside factors, and how the behavior of individuals can be influenced in order to create better outcomes. This, of course, cannot be done effectively without

the insight the social sciences can provide. Cybersecurity workforce managers can rely on social science research to determine what training methods are best for encouraging safe behaviors, with those that are engaging, and relate closely to the work of those being taught, perhaps being the most effective. Existing research can also help cybersecurity workforce managers determine how to fill open cybersecurity positions within an organization, which is especially important given the high number of job openings in the field (Mashudi et al., 2024, p. 1109). The principles of the social sciences themselves are useful in furthering one's understanding of cybersecurity as it relates to the workforce of an organization, as well. Determinism, for example, highlights that behavior is not inflexible, and can be shaped by external factors, particularly important in this role. Relativism would also indicate that social systems are related to the use of technology, and vice versa. Making alterations to social factors, then, can allow for increased security. Skepticism, empiricism, and objectivity, too, if applied together in this context, can allow decisions to be made based on proven facts, rather than feelings or conjecture, the results of which may be detrimental. Parsimony, as a principle, would also encourage solutions to problems to be as simple as possible, as to avoid creating unnecessary complications. These principles support the implementation of the policies and procedures that are most likely to support the organization's security objectives. Plans relatively simple in nature, backed by objective facts, which support the desired behaviors among the workforce, are likely to be some of the most effective. The knowledge provided by the social sciences seems to relate in some way to almost all of the recurring daily responsibilities these individuals may have. Thus, social science research and principles are, clearly, related closely to the role of cybersecurity workforce management.

Associations With Other Social Science Concepts

Several key concepts within the social sciences can be applied to the job of a cybersecurity workforce manager. Insights from psychology are one important part of this. Cybersecurity workforce managers, among other duties, must work with people to ensure that users are engaging in safe behaviors. Thus, the use of information relating to human factors and human-centered cybersecurity is critical to effectively complete these duties. One of the most important components of cybersecurity within an organization is the humans within it, with human-enabled errors frequently allowing attackers access to organizational systems and sensitive data. Understanding human factors, and focusing on the people in an organization, can allow cybersecurity workforce managers to create better and more engaging cybersecurity training, given this fact. This may help the behaviors, attitudes, and perspectives of users to align with the security interests of the organization, which is an incredibly vital task. Simply providing information is unlikely to meaningfully influence behavior over longer periods of time. In addition, those with this career can also work to foster an organizational culture supportive of cybersecurity. Organizational leaders play a crucial part in establishing the culture within a workplace, helping set norms and standards for how individuals act, which might further encourage safe behaviors. Combined, these two insights from the social sciences can enable individuals to value safety, rather than the speed at which work is completed. Economic concepts, too, apply to the work of cybersecurity workforce managers. These individuals may need to determine whether additional personnel, policies, and systems are needed, and whether they would be worth the additional resources that must be allocated to them. This can be done through a cost-benefit analysis of different potential choices. Solutions that have a high benefit or a low cost, naturally, would be more appealing than others. This allocation of funding for necessary programs is also partially based on risk, with the benefit of mitigating certain threats

being higher than others. A threat with a particularly high level of risk, a great likelihood of being realized, and a relatively low cost to mitigate would merit the most immediate action, in most cases. Cybersecurity workforce managers may be responsible for creating organizational policies related to their workforce that are legally compliant, as well. There are many regulations or standards that may apply to the organization, depending on how it operates and where it is located. These help to protect both the organization and those that interact with it from having sensitive information accessed by attackers. While solely doing what is legally required is likely a poor choice for the organization, it is, of course, necessary to guarantee that the minimum requirements are met, making this a key responsibility among both some cybersecurity workforce managers and others.

Relation to the Challenges of Marginalized Groups

The duties of a cybersecurity workforce manager also bear particularly noticeable connections to the concerns of marginalized groups in the context of employment within the cybersecurity field. Marginalized groups still account for a comparatively small percentage of cybersecurity professionals (*Labor Force Statistics From the Current Population Survey*, 2025). Cybersecurity workforce managers are in a position to alleviate this issue, at least within their own organization. These individuals can encourage diversity within an organization, thus bringing the myriad of benefits such diversity can provide. Beyond simply ensuring fair hiring practices and supporting diversity these individuals could, in some cases, also allow younger individuals who might not otherwise seek out a career in cybersecurity or other technical fields to obtain an internship or other educational position in their organization. Experience with a role model that one can identify with, or even experience in the field at all, can encourage them to pursue cybersecurity as a discipline (Jethwani et al., 2016, p. 17). While not applicable to all

organizations, this could allow a greater number of individuals from marginalized groups to gain experience and skill in cybersecurity, perhaps encouraging a future career in the field. As a result of these actions, the organization might become more equipped to solve the problems that occur daily in the cybersecurity field, through gaining new perspectives and insights. Beyond making up a comparatively smaller segment of cybersecurity professionals, marginalized individuals may also receive a lower salary in comparison to their peers, in some situations. This is possibly due to biases in the organization or in society at large. Cybersecurity workforce managers might help reduce or entirely bridge this gap, ensuring that the salaries of each employee are identical, or based solely on impartial factors like the length of time employed. Additionally, these individuals may be responsible for preparing necessary accommodations for those employed by the organization who require them. Those with disabilities may need alterations to be made either physically or socially to ensure that they can work in an efficient manner. Beyond the motivations related to productivity and legal requirements for providing these accommodations, doing so might incidentally help keep the organization's systems and data secure, in a way. If employees, marginalized or not, find that their needs are not being met by their employer, resentment might be built towards the organization. This, in turn, could lead to apathy towards the security of the organization, or even an insider attack. As the most important aspect of security in an organization is often in its people, working towards a fair and inclusive environment can help to provide a greater level of security.

Interactions Between Cybersecurity Workforce Managers and Society

Given the high degree to which social interactions affect the work of a cybersecurity workforce manager, it is clear that societal changes can quickly alter the tasks these individuals must perform. Social systems can alter each individual's behavior, their perspective, and thus

their security. Interactions may change within the workplace constantly, as a result of personal and social factors, which might also influence the security of the organization. Social forces can remarkably influence how the workplace operates, too. The development of new technology, or modifications to the use and security of existing technology, can play a role in this. Objectives might continually change every day as new vulnerabilities are discovered and are patched by others outside the organization. New applications and devices are developed consistently, each of which might play a role in the workplace environment. The way people communicate could be changed, either as a result of social or technical developments, leading to differences in attack methods from one week to the next. Each of these also has the potential to change the foundation of how work occurs. The use of smartphones and online meetings, for instance, has very quickly become the norm in many organizations, opening the door to both productivity boosts and security concerns. The requirements of cybersecurity workforce managers are also subject to change as external regulations are implemented, altered, or removed. Laws may be created based on the needs of certain groups or society as a whole, some of which may apply to the operation of an organization and its cybersecurity. Each of these alterations in society bring new things to ensure users are made aware of. Cybersecurity workforce managers must keep on top of all of these changes, so as to not be caught off guard by some new threat or obstacle that was missed. Just as society might have an influence on an organization, and thus the people employed within it, so too can those in an organization, including those responsible for its cybersecurity workforce management, exert at least some influence on the rest of society. The exact form of this influence would naturally depend on the type of organization the cybersecurity workforce manager is employed in. No matter the kind of organization, though, these individuals will almost certainly have an influence on the users who interact with it. The security of systems and the sensitive

information within them is incredibly important for the users this information belongs to. Society at large depends on the reliability of information systems in order to function. If there was no trust in the ability for organizations to keep sensitive information safe, humanity would not be able to reap many of the benefits of this influential technology, as the risk of bringing harm upon oneself would likely be too great. The biggest challenge that exists to current systems and networks is that of human error. As such, the role of cybersecurity workforce managers is crucial in helping protect against the threats that most endanger the systems and infrastructure almost all individuals in society make use of. The rapid changes felt within the field of cybersecurity as a result of external societal shifts are highly influential to the work that cybersecurity workforce managers must perform, and there is certainly a notable influence these individuals exert on others, as well. The consistent interactions between cybersecurity professionals such as these and society as a whole are in no way insignificant.

Conclusion

Given the undeniable relationship between cybersecurity and the social sciences, it is understandable why careers in this field would bear strong connections to social science research and principles, and have dynamic interactions with society as a whole. Cybersecurity workforce managers have the unique ability to touch both the technical and the social dimensions of the workplace, playing a major role in both. Consequently, these individuals can have a large effect on the way in which social interactions take place in the organization, thereby influencing its security, along with society as a whole.

References

Jethwani, M. M., Memon, N., Seo, W., & Richer, A. (2016). “I can actually be a super sleuth.” *Journal of Educational Computing Research*, *55*(1), 3–25. https://doi.org/10.1177/0735633116651971

Labor Force Statistics from the Current Population Survey. (2025, January 29). U.S. Bureau of Labor Statistics. Retrieved April 13, 2025, from https://www.bls.gov/cps/cpsaat11.htm

Mashudi, Fauziah, L., Windriya, A., Kurniawati, N., & Kholidin. (2024). Optimizing human resource management strategies for cybersecurity workforce development in the era of digital transformation. *International Journal of Communication Networks and Information Security*, *16*(4), 1109–1125. https://www.ijcnis.org/index.php/ijcnis/article/view/7312

NICE Workforce Framework for Cybersecurity. (2025, January 17). National Initiative for Cybersecurity Careers and Studies. Retrieved April 13, 2025, from https://niccs.cisa.gov/workforce-development/nice-framework