Career Paper

Chief information officers (CIOs) play a critical role in cybersecurity by protecting a business's information and IT systems and coordinating essential information flow and storage for various other company departments (BasuMallick, 2023). To carry out their responsibilities successfully, CIOs must employ many principles and ideas from the social sciences discussed throughout this class. For instance, a CIO must be able to communicate the importance of technological, informational, and security needs to many people with different, non-technical areas of expertise (BasuMallick, 2023). For these communications to be effective, CIOs need to apply parsimony to their explanations and recommendations so that non-technical stakeholders will understand solutions and be more willing to adopt and follow them (Duvall, 2024a).

Additionally, CIOs must be objective in carrying out their duties (Duvall, 2024a). Not only must a CIO be able to communicate their recommendations effectively, but they must also have an open mind and listen to the concerns of those in other departments (BasuMallick, 2023). After all, technology should be made and configured in a way that is both secure and addresses the needs and tendencies of its users (Duvall, 2024d). As a result, a CIO should be objective in being able to understand the needs of users and how these can be incorporated into new technological and information security solutions rather than solely relying on their expertise or what they think is best for the company without consulting others (Duvall, 2024a). Similarly, empiricism is an essential principle for CIOs to utilize. When designing new solutions and evaluating currently implemented ones, a CIO needs to observe the real-world effects of such solutions instead of relying only on intuition (BasuMallick, 2023). When being empirical, a CIO can more effectively do their job and serve their employer and colleagues better by creating evidence-based solutions crafted to fit an organization's specific needs instead of hypotheticals

that may or may not apply. Furthermore, CIOs must incorporate relativism in their work because they are required to act as intermediaries between the IT department and several other departments in the organization when creating IT solutions (BasuMallick, 2023). If the CIO is unable to see how the operations and needs of other departments influence the technological aspects of the organization, they will not be able to create practical solutions to keep IT systems running smoothly (Duvall, 2024a).

Another responsibility of CIOs is coordinating IT projects with other business requirements while weighing a solution's costs and risks against its potential benefits (BasuMallick, 2023). This relates to this class's discussion in module 11 of the tightly interrelated nature of economics and cybersecurity. Specifically, this duty is referred to as costs/benefits analysis and risk assessment (Duvall, 2024f). This is an essential component of a CIO's job because they are supposed to act as an intermediary between an organization's technology and business aspects, which requires solid financial literacy (BasuMallick, 2023). The significance of this duty is corroborated by the fact that profit maximization is one of the primary goals of many businesses (Doyle, 2023). Without knowledge of economics and financial skills, a CIO will not be able to predict the impacts of technology correctly and will likely have a significant negative impact on their company's profits and goals.

The need for CIOs to bridge the gap between the technical and non-technical aspects of a business through knowledge of diverse fields and communication strategies also relates to the interdisciplinary nature of cybersecurity (BasuMallick, 2023; Duvall, 2024b). Because information is needed and produced by almost every business process, it is essential that a CIO understands there are different requirements for different processes and can consult with various

specialties to create sufficiently secure and user-friendly security solutions for all business departments.

Management and finding the right people to fill positions within the IT department, which often involves working closely with human resources, is also a prominent aspect of being a CIO (BasuMallick, 2023). As a result, CIOs could benefit from knowing many of the psychological theories and concepts discussed in module 5 of this class. For instance, understanding the "Big Five" personality traits may enable a CIO to determine the tendencies of a potential candidate, such as agreeableness and conscientiousness, that would make them more likely to be ethical and thrive in a cybersecurity career (Duvall, 2024c). Additionally, if a CIO knows what motivates their employees to do their best, they could use reinforcement sensitivity theory to produce more efficient work and better outcomes. If a CIO can tailor rewards and opportunities to individual employees, they could provide employees with greater motivation and happiness in their daily activities.

Finally, another key responsibility of CIOs is to hold themselves accountable for the people they manage and supervise (BasuMallick, 2023). This is similar to Tyler Moore's (2010) ideas on how indirect liability for another person or entity's actions can be a fair solution for certain issues. Moore argues that holding internet service providers (ISPs) partly liable for damages caused by botnets is fair because it is difficult to pin down the perpetrator of such crimes, and ISPs are one of the few parties involved that can detect signs of such suspicious behavior early. Similarly, because CIOs often head IT operations, they possess the most complete picture of the organization's IT needs. As a result, they are tasked with creating solutions, leading teams, and giving directions to their employees to keep IT operations running smoothly. If something goes wrong within the IT department, it is vital for the CIO to step up and take

responsibility because employees are acting under their direction, and doing so would help ensure a quick return to normal, smooth operations (BasuMallick, 2023).

CIOs share a strong connection with society because they play a pivotal role in securing the information of social institutions, such as businesses, hospitals, and government facilities (Duvall, 2024e). For instance, if a CIO does not properly fulfill their duties to keep their organization's information secure, a data breach could occur, leading to several adverse effects on society. As a result, their job is essential to upholding the information and privacy of the customers that the business serves. Furthermore, if a data breach causes enough damage or targets a small business, it could cause a company to cut budgets or close its doors, leaving some or all of its employees without jobs (Olenick, 2019). Not only would this negatively impact the lives and families of these employees, but it could affect the economy by driving up unemployment rates.

Societal norms and expectations could also affect a CIO's role within an organization. For example, Japan does not provide nearly as much funding for cybersecurity as the United States (Montgomery et al., 2023), indicating that their culture places less value on cybersecurity. Combining this with the notion that security and convenience are usually inversely proportional (Young, 2015), a nation like Japan may view a CIO's primary job duties as ensuring that information is easily accessible and useful to those who need it to complete their jobs. In contrast, a country that invests heavily in cybersecurity, like the United States, may believe that a CIO's responsibilities skew more toward cybersecurity, thus requiring them to balance the accessibility of information with protecting it from unauthorized access and alteration.

As a career that involves executive management and cybersecurity, there are several challenges that members of marginalized groups may face as CIOs or on the path to becoming

one. After his tenure as CEO of Aetna, Ron Williams (2024) notes that, even in positions high up in a company, such as sitting on a board of directors, members of the C-suite often have the most influence in a meeting. Consequently, if a company has a diverse board of directors but a homogeneous C-suite, there could still be a lack of influence and fair representation of marginalized groups within the organization. However, the author also notes that having minority members as senior management present in board meetings can facilitate more diverse board members speaking up and sharing their ideas and opinions, resulting in greater weight and consideration. If more CIOs were members of marginalized groups, it could help broaden the number of perspectives present in cybersecurity and related IT fields by encouraging openly sharing and considering the perspectives of all groups.

Another potential challenge for minority groups in senior management that Williams (2024) brings attention to is that many people think diversifying the workforce makes it less competitive by selecting applicants based primarily on their minority status. These people may feel that a minority CIO is unqualified and did not obtain their position through knowledge, hard work, and experience, thus leading them to disregard the CIO's direction and expertise, even though expanding the applicant pool to be more diverse will usually result in better outcomes and more qualified candidates.

Members of marginalized groups in cybersecurity also face stereotyping from their colleagues and employers (Drolet, 2021; Morrow, 2018). A stereotype could arise from how minorities often work in more technical or operational fields rather than business-focused ones (Williams, 2024). If this stereotype arose, it would likely make it more difficult for a minority CIO to attain their position because such fields often do not offer clear paths to landing a career in an organization's C-suit. Additionally, once in the position of a CIO, a member of a minority

group may have difficulty carrying out their duties because others may assume just because of their gender or race that they have a particular background and are thus not qualified for the position. As a result, colleagues and employees may unfairly disregard a minority CIO's expertise, suggestions, and directions.

References

BasuMallick, C. (2023, September 28). *Chief information officer (CIO): Meaning, job description, key skills, and salary in 2023*. Spiceworks. https://www.spiceworks.com/tech/it-careers-skills/articles/chief-information-officer/

Doyle, M. (2023, December 13). *Profit maximization: Definition and strategies for business success*. American Express. https://www.americanexpress.com/en-us/business/trends-and-insights/articles/profit-maximization-definition-and-strategies-for-business-success/

Drolet, M. (2021, December 23). *Diversity in cybersecurity: Barriers and opportunities for women and minorities*. CSO. https://www.csoonline.com/article/571811/diversity-in-cybersecurity-barriers-and-opportunities-for-women-and-minorities.html

Duvall, T. (2024a). *Module 2* [PowerPoint slides]. Canvas. https://canvas.odu.edu/courses/153102/files/31795368?module_item_id=5902879

Duvall, T. (2024b). *Module 3* [PowerPoint slides]. Canvas. https://canvas.odu.edu/courses/153102/files/31795407?module_item_id=5902881

Duvall, T. (2024c). *Module 5* [PowerPoint slides]. Canvas. https://canvas.odu.edu/courses/153102/files/31796456?module_item_id=5903248

Duvall, T. (2024d). *Module 7* [PowerPoint slides]. Canvas. https://canvas.odu.edu/courses/153102/files/32167084?module_item_id=5946276

Duvall, T. (2024e). *Module 8* [PowerPoint slides]. Canvas. https://canvas.odu.edu/courses/153102/files/32245180?module_item_id=5954715

Duvall, T. (2024f). *Module 11* [PowerPoint slides]. Canvas. https://canvas.odu.edu/courses/153102/files/33461881?module_item_id=5977998

Montgomery, M., Furukawa, S., & Knie, C. (2023, August 10). *Japan's cyber resilience: Key to US security in the Pacific*. Foundation for Defense of Democracies. https://www.fdd.org/analysis/2023/08/10/japans-cyber-resilience-key-to-us-security-in-the-pacific/

Moore, T. (2010). Introducing the Economics of Cybersecurity: Principles and Policy Options. In *Proceedings of a Workshop on Deterring Cyberattacks* (pp. 3–23). National Academies Press. https://nap.nationalacademies.org/read/12997/chapter/3

Morrow, S. (2018, May 30). *Minorities in cybersecurity: The importance of a diverse security workforce*. Infosec. https://www.infosecinstitute.com/resources/professional-development/minorities-in-cybersecurity-the-importance-of-a-diverse-security-workforce/

Olenick, D. (2019, October 29). *Data breach causes 10 percent of small businesses to shutter*. SC Media. https://www.scmagazine.com/news/data-breach-causes-10-percent-of-small-businesses-to-shutter

Williams, R. (2024). *Path to the C-suite: Increasing black representation at the executive level & boards*. SHRM.

https://www.shrm.org/executive-network/insights/people-strategy/path-to-c-suite-increasing-black-representation-executive-level-boards

Young, C. S. (2015, February 11). *The enemies of data security: Convenience and collaboration*. Harvard Business Review. https://hbr.org/2015/02/the-enemies-of-data-security-convenience-and-collaboration