Kevin McFarland

Professor Diwakar Yalpi

CYSE 201S

23 November 2024

CISO Career

BLUF: *The Chief Information Security Officer (CISO) plays a critical role in safeguarding the digital infrastructure of an organization, yet the scope of their responsibilities, authority, and position within the organizational hierarchy is still not fully understood. CISOs continue to face challenges in defining their positions and managing both internal and external security threats. As noted, many CISOs report feeling unsupported by upper management and struggle with stress and job insecurity, particularly after security incidents. CISOs are tasked with a range of responsibilities, including developing security policies, managing risk, and ensuring business continuity, often within the framework of industry regulations. However, the complexity of their role goes beyond technical expertise, touching upon various social science principles.*

Introduction

The Chief Information Security Officer (CISO) is a very significant role in any organization and in the world of Cybersecurity. However, even though the role was established back in 1999 the understanding of the scope of power, responsibilities and place withing an organizations command structure is hardly understood. It may be that despite how important the role has been recognized as, research is lacking into the role, the problems they face within an

organization and the challenges and opportunities facing a CISO. According to Western Governors University's career description page,

> "CISOs work alongside company officers, business managers, cyber security teams, and IT managers to effectively monitor and maintain the security of their organization's applications, databases, computers, and websites. They're also tasked with establishing enterprise-wide security policies, developing data breach resiliency plans, overseeing system update communications, and managing the information security financials (WGU)."

Primary duties and responsibilities of a CISO on the size of the organizations enterprise and the industry regulations that need to be complied to. A comment was made at the 32nd USENIX Security Symposium 2023, about the concerns CISO's have in their role, "There is growing evidence that many CISOs struggle to define their role, lack support from upper management, suffer from enormous stress, and are afraid that they might be fired after security incidents occur (Hielscher)." This makes for many challenges that a CISO must contend with, how do they do their job, how do they stay ahead of threats and how do social science principles affect their actions?

Social Science Applications

Unfortunately, the scope of threats that a CISO must be aware of and concerned with are not just external to the system they are responsible for, but also internal threats as well. According to Dave Stapleton, CISO at CyberGRX, on the primary goals of a CISO and the social science impact thereof, "However, cyber criminals are unrelenting and continue to keep Tim and his industry peers on their toes. As a result, "we have to put at the forefront the criminal actor

and their motivations (cybergrx).” This can lead to the application of several social science principles and theories to this career below are a few chosen to be discussed. The cost-benefit approach and the deterministic view on cyber criminals can directly affect a CISO’s decisions throughout their career. The CISO must take the time to consider how a cyber-criminal thinks and where the cyber-criminal is coming from in their lives. What drives their decision-making process and how or why they might attack a system. They must take the time to consider One of these applications is Maslow’s Hierarchy of Needs, this theory suggests that individuals have needs that form a hierarchy from physiological to self-actualization. This can apply to how a CISO structures an enterprises security program. Both customers or clients and employees need feel that their safety and security are protected via the organizations IT systems, which would also align to a CISO’s goal to ensure business continuity via robust security measures. Once these basic needs are met, this will help the CISO foster an environment that furthers the hierarchy, because employees will then feel empowered to take on greater responsibility in protecting data. Another theory that could apply is Social Learning Theory, wherein learning through observation, modeling and imitation can promote secure behavior. So, if respected leaders, such as the CISO, are modeling behaviors and adopting strategies that foster a culture of security, other employees are likely to adopt those same secure behaviors, which increases compliance security protocols and reduces risky behaviors. One such way that employees can learn and improve their self confidence is via simulated phishing emails, however there is a potential negative impact. Daniele Lain et al describe the use of this method, ”This is based on the principle that learning next to one's mistake is an effective teaching strategy; however, this practice has been under scrutiny due to unclear performance in field studies and potential side effects on employees' morale and well-being (Lain et al).” Now these are only some of the social

science principles and theories that prescribe some of the challenges a CISO must deal with, but there certainly is more.

Conclusion

The role of the Chief Information Security Officer (CISO) has become increasingly pivotal in today's cybersecurity landscape, yet its full scope, power, and responsibilities remain underexplored and misunderstood. Despite the role being established as far back as 1999, many organizations still struggle to define its place within their leadership structures and recognize the challenges faced by CISOs. As highlighted by the limited research and experts, CISOs are often under immense pressure, balancing the need to stay ahead of cybercriminals with managing internal organizational dynamics and external security threats. These challenges underscore the need for a more comprehensive understanding of the social science principles that influence CISO actions and decisions. Ultimately, while CISOs operate at the intersection of technology, strategy, and human behavior, their effectiveness hinges not just on their technical knowledge but also on their ability to navigate the complex social dynamics within their organizations. Their role demands a blend of technical expertise, strategic thinking, and an understanding of the human factors that drive security behaviors. As the cybersecurity landscape continues to evolve, so too must the understanding of the CISO's role, ensuring that these leaders are better supported, empowered, and equipped to meet the growing demands of cybersecurity.

References

Hielscher, Jonas & Menges, Uta & Parkin, Simon & Kluge, Annette & Sasse, Angela. (2023). "Employees Who Don't Accept the Time Security Takes Are Not Aware Enough": The CISO View of Human-Centred Security. https://www.researchgate.net/publication/369977198_Employees_Who_Don't_Accept_the_Time_Security_Takes_Are_Not_Aware_Enough_The_CISO_View_of_Human-Centred_Security. Accessed 22 November 2024.

Lain, Daniele et al. (2024). Content, Nudges and Incentives: A Study on the Effectiveness and Perception of Embedded Phishing Training. DOI: 10.48550/arXiv.2409.01378. Accessed 22 November 2024.

Stapleton, Dave and Rohrbaugh, Tim. CyberGRX. *How the Role and Priotieies of a CISO are Changing.* Blog. December 2022. https://www.processunity.com/how-the-role-and-priorities-of-a-ciso-are-changing/. Accessed 22 November 2024.

Western Governors University. WGU. Information Technology Career Guides. 2024. https://www.wgu.edu/career-guide/information-technology/ciso-career.html. Accessed 22 November 2024.