Brendan Marcelo
CYSE201S
Career Paper

The role of Cybersecurity Administrators and the influence of social sciences on Cybersecurity

In today's world of technical careers, the role of a cybersecurity administrator is essential in preventing threats against networks and safeguarding confidential information in computer systems. These specialists utilize social sciences to alleviate risks and vulnerabilities dealt with human behavior. This essay will demonstrate the responsibilities, use of social sciences, and the understanding of human behavior in cybersecurity and how they are used to provide effective skills in the role of a cybersecurity administrator.

A cybersecurity administrator specializes in safeguarding and defending an organization's IT infrastructure. Their core responsibilities include monitoring network systems, developing and executing security policies, and managing firewalls. With specializing in protecting IT systems, these professionals must mitigate from internal and external threats to ensure the integrity of infrastructure and data. A crucial measure of their role is analyzing vulnerabilities, monitoring systems, and establishing threat monitoring protocols. In order to establish an effective threat monitoring protocols also known as intrusion detection systems, they must manage security logs and deploy measures to block unauthorized access attempts. Furthermore, admins are responsible for providing security awareness training to educate employees on the importance and safe use of cybersecurity tools and practices. These efforts promote the importance of employees and their role in data protection.

The daily responsibilities of a cybersecurity administrator may differ depending on the organization they work for, but they typically share a common foundation. This involves the installation and management of technical tools within their organization used to troubleshoot cybersecurity issues. Installation of software and hardware equipment include antivirus programs, user authentication systems, and firewalls. They are also required to perform mandatory updates to devices and perform troubleshooting protocols when issues occur. Probing is an essential responsibility in their day-to-day activity. Probing refers to the process of actively scanning a network, system, or application to obtain information about its structure, vulnerabilities, and weaknesses. Common types of probing are port scanning, network mapping, and service enumeration. Port scanning identifies which network ports are active, exposing open ports that may be vulnerable to threats. Network mapping identifies network structure like end-point devices, servers, and routers within the network. Service enumeration gathers information on active services, applications, and open ports running on a specific system or network. Cybersecurity administrators are also responsible for developing security policies to ensure best practices by staff members of their organizations. Policies include access control policies, password management policies, network security policies, data classification policies, data retention policies, acceptable use policies, incident response plans, patch management policies, remote access policies, BYOD policies, and physical security policies.

While technology forms the foundation of cybersecurity, social sciences such as sociology and psychology are equally critical in ensuring effective safety practices. According to Kirwan, Cyberpsychology examines how we interact with others using technology, how our behavior is influenced by technology, how technology can be developed to best suit our needs, and how psychological states can be affected by technologies. Psychology provides critical perceptions on human behavior which is commonly known as the weakest link in cybersecurity. Through an attacker's lens, they often exploit human vulnerabilities like curiosity, fear, and trust. Cybersecurity administrators utilize psychological ideologies to create user friendly security solutions and implement training programs that raise awareness of social engineering attacks. Behavioral cybersecurity also known as the human factor presents the social scientific perspective. Multiple topics like awareness, behavior, policy, and compliance are covered under cybersecurity behavioral research. Furthermore, sociology studies the social norms and behaviors that shape human behavior. Utilizing the principle of sociology, cyber and IT professionals are able to comprehend the importance in the social aspect in which protocols are applied. Sociology reveals employee behavior, motivations, and incentives, which are essential in encouraging compliance with security strategies. Cultivating a positive secure environment within the organization leads to increased trust, improved collaboration, and greater productivity.

As mentioned previously, the weakest link in cybersecurity is human error. Although this is a considerably significant vulnerability, it is also a defense mechanism. According to Verizon's 2023 Data Breach Investigation report (DBIR), 74% of data breaches involve the human element, with phishing attacks at 98% of social engineering attacks. Cybersecurity administrators protect against threats due to human behavior like phishing attacks, social engineering, and insider threats. Phishing attacks involve hackers impersonating trustworthy sources to manipulate victims into disclosing personal information that can lead to identity theft or financial loss. Social engineering refers to impersonating cybersecurity professionals to gain access to private information or network/computer systems. Insider threats include mishandling data or the use of weak passwords to exploit vulnerabilities resulting in security breaches. With the use of understanding human behavior, cybersecurity administrators are able to combat against these threats and vulnerabilities by providing regularly updated training on safe password practices, security awareness training on social engineering attacks, and practices on reporting suspicious activity.

Cybersecurity administrators play a role in protecting information, devices, and our digital wellbeing from harm. Marginalized groups like women, elderly population, and low-income communities. Women are subject to face online abuse like stalking and exploitation in public and professional spaces. Women in Cybersecurity (WiCyS) a non-profit organization supporting the advancement of women in cybersecurity encounter online harassment and underrepresentation in the workforce. Cybersecurity administrators can play a critical role in developing safety protocols to address these threats including privacy tools, harassment reporting systems, and educational awareness training on online safety. The elderly community are common targets of phishing scams, fraud, and identity theft due to lack of digital literacy. Cybersecurity administrators can implement user-friendly security measures and develop educational programs to improve cybersecurity awareness in places like senior living homes or assisted senior living homes. Low-income communities are more vulnerable to cyber-attacks like phishing, and identity theft due to limited access to education, tools, and resources. A cybersecurity administrator can develop affordable and easily accessible security measures specified to people in this category.

With that being said, the role of a cybersecurity administrator is essential in protecting the technical infrastructure of organizations and preventing threats associated with human behavior. The utilization of advanced technical skills and principles of social sciences provide the expertise needed to mitigate from threats and protection of data. Insights from psychology and sociology help cybersecurity administrators promote security awareness and create better trust and productivity within the workplace. The impact of cybersecurity administrators goes beyond their immediate organization and raises awareness of the similar challenges faced by marginalized groups promoting cultural awareness in the virtual world. With the rapid advancement of online threats, the skill of cybersecurity administrators continues to create a secure environment for all.

WORKS CITED

EC-Council University. (2024, August 22). *The Junction Between Cybersecurity and Social Psychology*. Eccuedu. https://www.eccu.edu/faculty/at-the-intersection-of-cybersecurity-and-social-psychology/

A Day in the Life of a Security Administrator | Main Responsibilities. (2022, September). Explore Cybersecurity Degrees and Careers | CyberDegrees.org. https://www.cyberdegrees.org/careers/security-administrator/day-in-the-life/

A Decadal Survey of the Social and Behavioral Sciences. (2019). National Academies Press. https://doi.org/10.17226/25335

Labs, K. (n.d.). *What is Human Behavior in Cybersecurity | Keepnet Labs - Keepnet*. Keepnet Labs. https://keepnetlabs.com/blog/the-complexity-of-human-behavior-in-cybersecurity

Brass, D. M. (2024, September 9). *Strong interrelationships between academia and information security, in all its various guises, stretch back decades. However, it is only recently that the intersection between the much of the social sciences and information security has come to the fore.* Linkedin.com. https://www.linkedin.com/pulse/intersection-between-social-sciences-information-security-brass-eduse/

Melanie. (2024, May 31). *Deciphering the Role of an IT Security Administrator*. Data Science Courses | DataScientest. https://datascientest.com/en/deciphering-the-role-of-an-it-security-administrator

Wikipedia Contributors. (2024, August 27). *Women in CyberSecurity*. Wikipedia; Wikimedia Foundation.

Knafo, J. (2018, February 8). *Top 10 Password Policies and Best Practices for System Administrators*. The Devolutions Blog. https://blog.devolutions.net/2018/02/top-10-password-policies-and-best-practices-for-system-administrators