**Career Paper: The Social Science of Cybersecurity Administration**

Evan Jenkins

Old Dominion University

Professor Diwakar Yalpi

11/24/2024

**Career Paper: The Social Science of Cybersecurity Administration**

**Career Overview**

 The role of a cybersecurity administrator is a mid-level role that requires strong technical skills and a well-rounded understanding of the social sciences to succeed. It involves overseeing cybersecurity operations in an organization day-to-day. This could include guiding cyber incident response, policy development, deployment, and compliance, training new and current staff members, and answering to the Chief Information Security Officer, or other upper management superiors depending on organizational hierarchy.

 While any role in cybersecurity requires a mix of soft and hard skills this is especially true for a cybersecurity admin. This career requires problem-solving, effective communication both up and down the chain of command, leadership, and managerial skills, in addition to technical cybersecurity and computer science knowledge (Yalpi, n.d.-a, p. 23). The disciplines of the field of social science also provide skills that can relate to the career of a cybersecurity administration such as psychology, economics, and criminology.

**Social Science Principles**

The basic principles of social science can also be the guiding philosophy for the day-to-day life of a cybersecurity admin. First, there is parsimony, which states to keep explanations simple (Yalpi, n.d.-c, p. 8). The job may require you to work with departments outside of the cybersecurity team and you need to be able to explain security matters in a way that does not overwhelm them. A cybersecurity admin is also expected to uphold ethical neutrality. They have the power of the system that protects the critical information of employees and customers alike. Determinism explains that people act because of previous occurrences (Yalpi, n.d.-c, p. 12). It is not enough for your cyber team to stop an attack; you need to understand why and how the organization was attacked. Objectivity is the practice of removing bias from your work. The cyber landscape evolves quickly so a cyber admin cannot hold only to old notions, but instead be open to alternative solutions.

**Social Science Research in Cybersecurity**

The social sciences utilize several research methods that could be useful for a cybersecurity administrator. One such method is that of surveys, which is obtaining responses through a questionnaire. Considering that a cybersecurity administrator will oversee a team of cybersecurity experts it is important to gauge their insight into current policies and procedures. Their direct experience with the needs of the organization could be invaluable. Another research method is archival research, which is gleaning saved records for insights. In cybersecurity, incident reports and work order tickets could be the source of archival research. Perhaps by examining them as a whole one might notice a trend of recent password attacks on employee accounts. This could lead to stronger password requirements for employees in the workplace or the implementation of two-factor authentication. Then there is the “gold standard” of social science research which is experimentation (Yalpi, n.d.-b, p. 12). A cyber admin could run an experiment to evaluate the effectiveness of their training. They could send out an intentionally suspicious email to see whether the staff will recognize the warning signs or not. Even field studies could be useful to a cybersecurity team in the form of honeypots, which allow one to watch a hacker operate in real-time in a controlled environment (Yalpi, n.d.-e, p. 18). Seeing how they try to breach your organization could change policy planning.

**Cybersecurity Training and Psychology**

The human side of cybersecurity is an often overlooked variable in the equation. It is not always a sophisticated hack that leads to a cybersecurity breach but often a simple phishing email that preys on people’s trusting nature. Psychology can help to explain how people can be so trusting and easily lured in. A key task of a cybersecurity administrator’s job description is overseeing the training and education of cyber topics to the workforce of an organization which is a process steeped in the study of the human mind. Psychology has been so deeply tied to cybersecurity and how people use technology that it has led to the subfield that is cyberpsychology. Cyberpsychology is defined as the “discipline of understanding the psychological processes related to, and underlying, all aspects and features of technologically interconnected human behavior” (Ancis, 2020, p. 1). Training must begin with the understanding that not everyone in the organization is going to have a deep knowledge of cybersecurity, so applying psychology could aid the administrator in teaching other departments to develop a secure mindset (Yalpi, n.d.-d, p. 14). Training must challenge the notion that cyberspace is safe. People often feel safe in their office environment, which makes them vulnerable to overlooking potential security risks. Employees must be trained to ask themselves questions before proceeding. If Susan from accounting receives a random email from someone claiming to be Jim from Human Resources asking for her work account and password, will she comply without a second thought or stop and ask herself some questions? Does she know a Jim from HR? Does someone from HR have permission to ask for such information? If she has been properly trained and developed a safety-focused cognitive process, she should find this suspicious and reach out to the cybersecurity administrator.

**The Economics of Security**

Being in a mid-level position means you are confined to the limitations set by higher management. This means that cybersecurity admin must be able to effectively leverage the limited resources at their disposal, which is the central topic of economics (Yalpi, n.d.-f, p. 4). Sometimes it is not feasible to have every tool available, so choices must be made. This is where risk assessment and costs/benefits analysis come into play (Yalpi, n.d.-f, p. 9-10). Risk assessment can help an admin prioritize areas of their policy to dedicate the most resources towards, while costs/benefits analysis can help see the pros and cons of assorted options.

 While economics impacts cybersecurity, the same is true in reverse. The impacts of a cybersecurity incident can be devastating to an organization. There is a financial cost for downtime to recover from an attack, fines, and payment settlements. There is a reputational cost from consumers, the stock market, and financial institutions (Cashell et al., 2004, p. 14). Many organizations can struggle to recover from such heavy repercussions, often leading to bankruptcy and layoffs. All this in turn shows how a cybersecurity admin, and their team, can have an impact on the economy.

**The Legal Landscape and Cybercrime**

By understanding how cybercriminals act and think a cybersecurity administrator can better tailor the policies they make for their team and organization to counter such criminal acts. One must be aware of what they are up against. Cybercriminals are those working to tear down everything that has been built in your career as a cybersecurity administrator. It is important to understand criminal motivations, attack vectors, how they select targets, and how they are scoping out processes. It is also important to understand the legal code that can be to your advantage. If the organization of a cybersecurity administrator suffers from a breach on a criminal level, they could be assisted by the vast resources of federal agencies such as the FBI. In cybersecurity, it is also important to understand the state and federal laws you are obligated to abide by. The policies developed by a cybersecurity administrator must be compliant with the legal rights of both employees and customers. While it depends on the specifics of the organization, one could be expected to abide by the European GDPR, HIPAA in healthcare, PCI DSS for e-commerce settings, and several others.

**Diversity Issue in the Cybersecurity Industry**

Cybersecurity is a field that is constantly evolving and presenting new challenges. Finding solutions to these challenges requires innovative mindsets. Innovation can come from anywhere in the world which highlights a severe issue in the field of cybersecurity, which is the lack of diversity. The industry has low levels of representation among women, African Americans, as well as Latinos. U.S. Department of Labor statistics show that “women and minorities represent only 11% of the cybersecurity workforce” (Lyon, 2020, p. 3). Having different viewpoints, cultural backgrounds, values, and beliefs could allow someone to see different solutions that others might miss. Additionally, it is a field that is rapidly growing and will need to appeal to broader demographics to fill the growing number of cybersecurity positions demanded by the job market (Mountrouidou et al., 2019, p. 158). There are various challenges faced by these underrepresented groups that discourage their participation in the field of cybersecurity. These challenges include a lack of role models in the industry they can look up to, a lack of opportunities, and the perception that it is a male-only environment (Lyon, 2020, p. 53). While it can be difficult to bring sweeping changes to an entire industry or to address the deeper issue leading to the lack the diversity, a cybersecurity administrator can at least improve the situation at their organization. This could be done by offering internship opportunities for these marginalized groups, offering cross-training pathways for other departments of the organization, and community outreach to local schools and universities. The internships would allow for immediate representation and career development in the field, which would create a future will role models for the next generation of women and minority groups. Cross-training would allow people in other parts of the organization to explore cybersecurity when they might not have previously been given the chance. Once the workforce becomes more diverse the perception of the industry being an “old boys’ network” can be broken (Lyon, 2020, p. 53).

**Societal Importance of Cybersecurity**

There is not a sector of society that cannot be touched by a cyberattack. Where there is data and technology there is a potential for a cyber threat, and thus a need for cybersecurity. Individuals, nations, government agencies, military organizations, non-profits, corporations, hospitals, banks, universities, and critical infrastructure, can, have been, and will continue to be targeted by cyberattacks. The reasons behind cyberattacks are just as diverse, such as financial gain, activism, cyber warfare, recreation, espionage, and cyberterrorism (Bay, 2016, p. 21). Every system of society is built upon cyber technology, and it is the field of cybersecurity that keeps it protected. The job of a cybersecurity administrator is to lead a team in the fight to protect their organization from the onslaught of cyberattacks.

**Conclusion**

 The career path of cybersecurity administrator is one of immense importance in a society that has grown so dependent on digital technologies. It is a career that requires a diversified skillset that often overlaps with those of the social sciences, such as economics, psychology, criminology, and law. It is a position that can, in many ways, have an impact on society as a whole.

**References**

Ancis, J. R. (2020). The age of cyberpsychology: An overview. *Technology Mind and Behavior*, *1*(1). https://doi.org/10.1037/tmb0000009

Bay, M. (2016). WHAT IS CYBERSECURITY?: In search of an encompassing definition for the post-Snowden era. *French Journal for Media Research*, *6*, 2264–4733.

Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). The Economic Impact of Cyber-Attacks. In *CRS Report for Congress* (No. RL32331). Government and Finance Division. https://archive.nyu.edu/bitstream/2451/14999/2/Infosec\_ISR\_Congress.pdf

Lyon, V. (2020). *Exploring strategies for recruiting and retaining diverse cybersecurity professionals* [Doctoral Study, Walden University]. https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=9579&context=dissertations

Mountrouidou, X., Vosen, D., Kari, C., Azhar, M. Q., Bhatia, S., Gagne, G., Maguire, J., Tudor, L., & Yuen, T. T. (2019). Securing the Human: A Review of Literature on Broadening Diversity in Cybersecurity Education. In *ITiCSE-WGR*. Working Group Report.

Yalpi, D. (n.d.-a). *Applying Psychological Principles of Cyber Offending, Victimization, and Professionals* [Slide show]. Old Dominion University.

Yalpi, D. (n.d.-b). *Introduction to Course Introduction to the Social Sciences* [Slide show]. Old Dominion University.

Yalpi, D. (n.d.-c). *Principles of Social Sciences and Cybersecurity Diversity and Cybersecurity* [Slide show]. Old Dominion University.

Yalpi, D. (n.d.-d). *Psychology Research, Human Factors, and Cybersecurity* [Slide show]. Old Dominion University.

Yalpi, D. (n.d.-e). *Strategies to Study Cybersecurity through an Interdisciplinary Social Sciences Lens* [Slide show]. Old Dominion University.

Yalpi, D. (n.d.-f). *The Economics of Cybersecurity* [Slide show]. Old Dominion University.