Cybersecurity Education; Ethical Implications

Robert Timmons

School of Cybersecurity

CYSE 425w: Cybersecurity Strategy and Policy

Professor Bora Aslan

March 25th, 2025

The Ethical Implications of Cybersecurity Education

As more of the human experience digitizes, it is important to analyze and understand the ethical implications of this new daunting reality. Cybersecurity education is a facet of this new expansion, setting standards to these new questions. Ethics as a field has scrambled to answer many quandaries emerging technologies have brought through the fore. Cybersecurity education as a policy has been studied by ethicists, discussing the implications of ineffective and proper cyber training alike. This paper aims to highlight some of these implications, as well as the drawbacks, costs, and benefits of cybersecurity education. From training disparities to immoral training, there are various angles to look at cybersecurity education. There are proven benefits to the policy, displaying the ability to curb malevolent conduct online while also arming potential victims and students with knowledge to identify and better grapple with hackers. While the path forward is made chaotic by new threats and technologies, policies like cybersecurity education when infused with ethical consideration can make all the difference.

When looking into cybersecurity education, there are a few ethical implications to consider. The largest one is the distribution of proper, even training throughout communities. Computer systems have been an aspect of our society for almost fifty years. Gas stations, libraries, and private institutions all have some base-level of digitization. The same cannot be said for cybersecurity education. Countries have begun creating cyber security curriculum, but there seems to be divides in how the education is applied. In rich urban communities, there is a greater emphasis on this education. This is seen in a report discussing socioeconomic factors in secure code practice, where it was found that "...students belonging to rural areas not updating their programs thereby showing low security…" (Khan et al., 2023) The report further details richer areas and even those impoverished but living near more technologically advanced areas

had better cyber awareness. It's essential that when crafting cyber education policies, that fair and proper disbursement of training is considered. The second implication can in some cases be worse than the first, amoral training. Cybersecurity education not only aims to protect individuals but seeks to instill proper online conduct in those going through the training. These trainings are only as effective as the morals they're built upon, however. Education frameworks should be imbued with strong moral undertones. Discussed in the *Role of Cybersecurity Education in Promoting Ethical and Responsible Use of Technology for Sustainable Development,* "... the unchecked and unethical use of technology can pose significant risks and challenges to achieving these goals…" (AdeJuwon, 2023) Without a consideration of proper application of training and a moral framework for training, these implications can be devastating to cybersecurity education endeavors.

When discussing the benefits and costs of cybersecurity education, it's important to understand that the policy can be implemented in a myriad of ways. There is already a litany of materials to pull from, so costs can be relatively low for smaller organizations. Larger groups, however, may struggle. A conference report detailing cyber education costs explains that "... budget constrains have represented the main obstacle for more than 3600, in their attempt to prevent or correct cybersecurity issues." (Dumitru, 2019) Budget concerns are not just about collecting fiscal resources, but human resources and finding time to apply the former two. Another issue concerns legacy systems. Training could be outdated or too advanced, with many organizations having a combination of dated and current systems requiring specialized training. The issue compounds when security software is introduced into training, as compatibility of this software with older systems may arise. Despite this, there's still great benefits to be garnered from cyber education. Instead of being on the back foot and continually cleaning up messes,

trained employees can recognize and shutdown attacks before they even occur. The upfront cost of the training is peanuts compared to the costs of remediating, fixing, or going through the legal processes of dealing with a cyber breach. remediation of systems. This is built upon in the conference where they state "...including a training budget in the organization's financial planning can save a lot of money in terms of corrective actions, when an actual threat becomes an attack." (Dumitru, 2019) Though there is a high upfront cost of cybersecurity education, it can prepare organizations and individuals to deter devastating attacks.

As the semester has gone on, cybersecurity education has proven to be a complex and multifaceted policy. With the field handling PII such as credit cards, birth certificates, and sensitive health information, it's extremely important to understand the ethical and moral responsibilities of those working in or operating with cyberspace. Cybersecurity education helps protect information such as this and inadvertently protects the individual's rights. It does so by setting the standard of proper and ethical use of information, tools, and cyberspace. Cybersecurity education accentuates the right to privacy and decency online, as training can instill netiquette on proper use of technologies and the harms cybercrime, cyberbullying and cyber stalking. The policy doesn't come without certain implications, as improper training can create hackers that don't truly understand the ramifications of their actions. On top of this, inequitable training practices can leave some communities vulnerable to threats. Despite this, a strong cybersecurity curriculum has been shown to build a great understanding of threats, the ethical use cases of hacking and penetration testing tools, and arms potential victims with knowledge to avoid cyber pitfalls and scams.

References

AdeJuwon, F. (2023). Lead City University Postgraduate Multidisciplinary Serial. https://www.journals.lcu.edu.ng/index.php/LCUPGMCP/article/download/867/641

Hynninen, T. (2023, October 18). *Student Perceptions of Ethics in Cybersecurity Education*. ceur-ws.org. https://ceur-ws.org/Vol-3582/FP_07.pdf

Hamburg, I. (2017, October 25). *Ethical Aspects in Cyber Security* . SemanticScholar. https://pdfs.semanticscholar.org/ca4c/3e1bf0f7b6bfe38deccdb30fadff7c185b8f.pdf/1000

Khan, N. F., Ikram, N., & Saleem, S. (2023, April 22). *Effects of socioeconomic and digital inequalities on cybersecurity in a developing country*. Security Journal. https://pmc.ncbi.nlm.nih.gov/articles/PMC10122089/

Dumitru , D. (2019). New Trends in Sustainable Business and Consumption 2019. In *CYBERSECURITY EDUCATIONAL PROGRAMS: COSTS AND BENEFITS* (pp. 625–631). Bari; Carol I National Defense University .