Ethical Implications of IT Security Policies

Samantha Riggs

Old Dominion University

CYSE 425W: Cyber Strategy and Policy

Dr. Shideh Yavary Mehr

June 27th, 2025

When developing successful strategies and policies surrounding the cybersecurity industry, it is integral to consider the ethical implications that are presented. For example, the quick advancement of modern technology in today's era introduces new ethical dilemmas, particularly surrounding synthetic intelligence, quantum computing, and the Internet of Things (Navdeep et al., 2022). Fenech et. al stated that decisions to apply technical or policy solutions must consider how an individual's values and moral stance influence their responses to these implementations (2024).

Ethical concerns are such a large part of the cybersecurity field as a whole, in fact, that the Association for Computing Machinery (ACM) has created its own code of ethics and professional conduct, which is "designed to inspire and guide the ethical conduct of all computing professionals" (Association for Computing Machinery, 2018). The ACM is recognized as the world's largest computing society and works to address the challenges posed in the field as well as promote high standards and technical excellence. The code of ethics that they have created serves as a guide for decision-making and ethical reasoning in the computing industry in general. Similar to the "do no harm" statement in the Hippocratic Oath that medical professionals must take, the ACM's code of ethics also states that actions (which includes the creation of policies) should "avoid harm". Other core principles present in this code are that any actions should contribute to society and human well-being, honor confidentiality, be fair and not be discriminatory, respect the work required to produce new ideas, respect privacy, and be honest and trustworthy. Additionally, this code provides a number of professional responsibilities and leadership principles.

While different ethical concerns apply to various cybersecurity policies in different ways, information systems security strategies have main concerns pertaining to privacy and

transparency. Privacy has always been a large focus in the cybersecurity field, as strategies require a balance between the privacy needs of users and providing adequate cybersecurity measures. This balance can be difficult to not only initially obtain, but also subsequently maintain. Carefully considering ethical implications of information systems security policies (or any cybersecurity policy for that matter), can help balance the scales. The need to both protects user privacy and implement necessary measures also requires transparency. This requires organizations to be accountable for the cybersecurity policies they develop and make all employees or members aware of what these policies require of users. If an employee is aware of the policy in its entirety, they can both raise concerns and have explanations provided for a better understanding. As a result, a greater organizational sense of trust and overall understanding surrounding these policies can be achieved. This is beneficial to address the human factor of cybersecurity, in which many employees fail to adhere to cybersecurity policies either due to misunderstanding or perceived inconvenience of the policy itself. By addressing the ethical concerns that can be posed when developing cybersecurity policies, these policies can be more efficient and successful overall.

References

Association for Computing Machinery. (n.d.). https://www.acm.org/

Fenech, J., Richards, D., & Formosa, P. (2024). Ethical principles shaping values-based cybersecurity decision-making. *Computers & Security*, *140*. https://doi.org/10.1016/j.cose.2024.103795

Naveep, Garg, A., Muskan, & Sharma, V. (2023). The role of ethics in developing secure cyber-security policies. *Tuijin Jishu/Journal of Propulsion Technology*, *43*(4), 250–254. https://doi.org/10.52783/tjjpt.v43.i4.2346