The Social Implications of Information Systems Security Policies

Samantha Riggs

Old Dominion University

CYSE 425W: Cyber Strategy and Policy

Dr. Shideh Yavary Mehr

July 14th, 2025

When analyzing policies in the cybersecurity field, it is important to recognize the social factors that were involved in that policy's creation. The technical aspect, while important, is only one portion of the policy development process. Human behavior, and more importantly human error, is known as one of the weakest points of entries for cyber-attacks. Therefore, policy developmental decisions and effectiveness post-implementation, and in order to evaluate this factor, social implications must be examined.

Today's modern state of technological advancement has allowed for increased collaboration and innovation worldwide. As much as a positive impact these developments have made on society as whole, new potential threats, motivations and methodologies emerge as well. This includes an increase of attempted social engineering attacks known as phishing, which saw a 58 percent increase globally from 2022 to 2023 (Barros, 2025). These attacks work to directly target and subsequently exploit the human factor in cybersecurity. This change in the social sphere impacts the way security policies must be developed, as policies require adherence and compliance by employees to be fully effective.

This compliance can be difficult for cybersecurity policy developers to achieve and maintain. Policy makers must examine the current workplace culture and employee attitudes towards cybersecurity measures and try to integrate this social factor within the new policy. Policy adherence is heavily reliant on the presence of an active, cyber aware culture in the organization. Positive attitudes can be "influence by factors such as awareness of security risks, training, and organizational support" (N & Mathew, 2024).

A large consequence of policies surrounding information security is the potential for a negative impact on employee trust towards the organization. If a policy seems too overbearing or causes a feeling of constantly being monitored it can result in a degradation in policy adherence,

greatly affecting policy effectiveness. In order to prevent this negative outcome, there should be a feeling of transparency concerning what the policy does, if and how data collected pertaining to the policy is used, and what measures are being taken to protect the privacy rights of employees. This can also include making policy development a more involved process by allowing “time for frequent peer discussions on the interpretation and implementation of rules” (Gyllensten & Torner, 2021).

In conclusion, the social impact and its implications play a large role in information security systems policy development. This factor can sometimes be overlooked by technological or ethical factors, which can hinder a policy’s effectiveness. Policies that either incorrectly assume the state of social factors within the workplace or completely ignore the factor all together are missing a core component to success. By correctly examining and identifying social factors, policies have the potential to become more efficient and effective in the long term.

References

Barros, M. (2025, January 27). *The Rise in Phishing Scams* . Cyber Defense Magazine. https://www.cyberdefensemagazine.com/the-rise-in-phishing-scams/

Gyllensten, K., & Torner, M. (2021). The role of organizational and social factors for information security in a nuclear power industry. *Organizational Cybersecurity Journal: Practice, Process and People*, *2*(1), 3–20. https://doi.org/10.1108/ocj-04-2021-0012

N, B., & Mathew, S. K. (2024). Exploring the factors influencing information security policy compliance and violations: A systematic literature review. *Computers & Security*, *147*, 104062. https://doi.org/10.1016/j.cose.2024.104062