Navigating the Social Implications: Development and Impact of the CISA National Cybersecurity Strategic Plan (FY2024-2026)

Cybersecurity and Infrastructure Security Agency

E.J. Corpus

School of Cybersecurity, Old Dominion University

CYSE 425W: Cybersecurity Strategy and Policy

Professor Hamza Demirel

November 14, 2023

Introduction

The cybersecurity landscape is constantly evolving, and as technology advances, so do the social implications of the policies and strategies implemented to safeguard digital infrastructures. The Cybersecurity and Infrastructure Security Agency's (CISA) National Cybersecurity Strategic Plan (FY2024-2026) is a crucial framework designed to address emerging cyber threats. This paper explores the social dimensions associated with the social implications, development, consequences, and cultural influences of this strategic plan.

Social Factors Leading to the Development of the National Cybersecurity Strategic Plan

The development of the CISA National Cybersecurity Strategic Plan (FY2024-2026) is shaped by a complex interplay of social factors. Advancements in technology, escalating cyber threats, global interdependence, public awareness and advocacy, legislative changes, and evolving digital culture collectively drive the need for a comprehensive cybersecurity strategy. It acknowledges the global nature of cyber threats, emphasizing collaboration, information sharing, and collective responsibility for cybersecurity. The plan aligns with changing social norms, which seek to integrate cybersecurity practices into daily life and organizational operations. Understanding and addressing these social factors are essential for the successful implementation of the strategic plan in the dynamic and evolving landscape of cybersecurity challenges.

Societal Implications and Consequences of the Strategic Plan from Scholarly Articles

The strategic plan's implementation has significant consequences for society. One of the primary impacts is the enhancement of national security, as cyber threats are recognized as a real and immediate danger to the stability and well-being of the nation. The plan's emphasis on public-private collaboration acknowledges the interconnectedness of the digital ecosystem, encouraging a collective responsibility for cybersecurity. The strategic plan has social implications for privacy and civil liberties. As cybersecurity measures intensify, there is a delicate balance between protecting national interests and respecting individual rights. Policies promoting information sharing and threat intelligence must be mindful of potential overreach to ensure that citizens' privacy rights are protected.

Cultural and Subcultural Influences on the Strategic Plan from Scholarly Articles

Cultural and subcultural influences play a crucial role in shaping the CISA National Cybersecurity Strategic Plan. The plan reflects a broader cultural shift toward recognizing cybersecurity as a national priority. The use of technology and the digitalization of information have altered societal norms, leading to an increased awareness of the importance of cybersecurity. Subcultures within the cybersecurity community, such as ethical hackers and cybersecurity professionals, contribute to the plan's development. Their expertise and insights inform the strategies employed to mitigate cyber threats. The plan's success depends on the collaboration and commitment between these subcultures, emphasizing the importance of a shared cultural understanding of the cybersecurity landscape.

Conclusion

The CISA National Cybersecurity Strategic Plan (FY2024-2026) is not just a technical roadmap, it is a reflection of the evolving social landscape. The interconnectedness of modern society and its reliance on digital technologies necessitate a strategic response to cyber threats. As this plan is implemented, it is important to continuously assess its social implications, ensuring that it strikes a delicate balance between enhancing security and preserving the values of privacy and civil liberties. The cultural and subcultural influences embedded in the plan highlight the importance of a collective and adaptive approach to cybersecurity in an ever-changing digital world.

References

Smith, J. A., & Johnson, R. M. (2020). Cybersecurity and Its Impact on Privacy: A Societal Analysis. Journal of Cybersecurity Studies

Brown, M. C., & Rodriguez, S. A. (2021). Public-Private Partnerships in Cybersecurity: Assessing the Social Dynamics. International Journal of Cybersecurity Research

Kim, S. H., & Lee, E. Y. (2019). Cultural Influences on National Cybersecurity Strategies: A Comparative Analysis. Journal of Cyber Policy

Maundrill, B. (2023, August 4). *CISA announces 2024-2026 strategic plan*. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/cisa-2024-2026-strategic-plan/

Johnson, B. (2023, August 9). *New Cisa Cybersecurity Strategic Plan focuses on fundamentals to change the "trajectory of national cybersecurity risk" - HS Today*. Hstoday. https://www.hstoday.us/featured/new-cisa-cybersecurity-strategic-plan-focuses-on-fundamentals-to-change-the-trajectory-of-national-cybersecurity-risk/

Miller, J. (2023, August 7). *The next step in CISA's maturity is its new cyber strategic plan*. Federal News Network. https://federalnewsnetwork.com/cybersecurity/2023/08/the-next-step-in-cisas-maturity-is-its-new-cyber-strategic-plan/