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

October 14, 2023

Introduction

As technology evolves, cybersecurity is one of the main concerns for governments, organizations, and individuals. Developing robust cybersecurity strategies is important to safeguarding national security, critical infrastructure, and personal data. The CISA National Cybersecurity Strategic Plan (FY2024-2026) is playing a specialized role in carrying out national cybersecurity policies in the United States. While it is crucial to enhance cybersecurity, it is equally important to consider the ethical implications that arise from this strategy. There comes a balance between security measures and individual rights, the potential costs and benefits of these measures, and the broader societal implications. The research paper dives into the ethical landscape of the CISA National Cybersecurity Strategic Plan (FY2024-2026).

Ethical Implications and Privacy

The CISA Cybersecurity Strategic Plan (FY2024–2026) has come with a new focus to prioritize resources that achieve the greatest impact for the American people. One of the primary ethical considerations in the new CISA Cybersecurity Strategy is the protection of individuals' privacy. The strategy aligns with the fundamental principles of human rights, ensuring that individuals' rights are not compromised in the pursuit of cybersecurity. Any measures that might restrict freedom of expression, association, or access to information are carefully evaluated. When cybersecurity measures are put into place, it puts a higher risk towards PII since it could involve collecting vast amounts of data. The CISA Cybersecurity Strategy may involve retaining user data for security purposes. The ethical implication is how long this data is retained, who has access to it, and for what purposes. The strategy will ensure transparency about the data being collected, how it's being used, and who has access to it. Additionally, mechanisms for accountability should be in place to address any mishandling or unauthorized use of data.

Balancing security needs with the protection of personal information is critical. Currently, there are no rights or laws that will limit the strategy as they are attempting to avoid concerns and upgrade critical cyber infrastructure.

Cost and Benefits from Three Scholarly Articles

The costs and benefits are important when it comes to implementing cybersecurity measures. Ethical implications may arise if the costs, such as financial investments or potential limitations on certain technological advancements, outweigh the benefits in terms of increased security and protection from cyber threats. It is essential to ensure that all parts of society have access to the necessary resources and protection. Maintaining and managing cybersecurity systems can result in ongoing operational costs. Regular updates, maintenance, and training of personnel all contribute to the operational overhead of the strategy. Putting money into a strong cybersecurity strategy can safeguard critical infrastructure, government systems, and sensitive information, enhancing national security and protecting against cyber threats.

Conclusion

While the CISA National Cybersecurity Strategic Plan (FY2024-2026) policy aims to fortify the nation's cybersecurity infrastructure, it is important to emphasize the ethical implications that arise from its implementation. To ensure the effectiveness and ethical soundness of the CISA National Cybersecurity Strategic Plan, it is essential for policymakers to prioritize the principles of transparency, user empowerment, and technological neutrality. There must be a striking balance between security imperatives and individual rights when building public trust and maintaining the integrity of the digital ecosystem.

References

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/