.The Cybersecurity Information Sharing Act, enacted in 2015 in the United States, aims to enhance national cybersecurity by facilitating the sharing of cyber threat information between the government and private companies. While its goal is to improve security, CISA brings with it a number of social implications, particularly regarding privacy and the broader societal impacts of information sharing. In this paper I will be exploring the social consequences of CISA, focusing on the factors that led to its creation, its impact on society, and the ways in which cultural and subcultural influences have shaped the policy.

A key factor that influenced the development of CISA was the growing recognition that cybersecurity is a shared responsibility between the private sector and the government. The increasing frequency of cyberattacks on U.S. businesses and government entities highlighted the need for more effective collaboration in combating cyber threats. According to Hitchens and Goren (2017), international cybersecurity agreements, including those focused on information sharing, have become vital in tackling global cyber threats. These agreements laid the foundation for domestic policies like CISA, which focuses on encouraging the sharing of threat data to improve collective defense mechanisms. However, as this information sharing increased, so too did concerns about the privacy of individuals and the potential for governmental overreach. Critics of CISA pointed to the lack of robust privacy protections in the bill, questioning whether the benefits of increased cybersecurity could justify the risks to personal privacy (Mussington & MacLellan, 2018).

One significant social implication of CISA is the potential erosion of trust between the public and both private corporations and government entities. CISA allows for the sharing of large volumes of data between companies and federal agencies, including sensitive cybersecurity

information. While the intention is to strengthen defenses against cyber threats, many individuals are concerned that their personal data could be caught up in these exchanges. Although the law requires that certain information be anonymized to protect privacy, there are still valid concerns about the transparency and accountability of this process. Solansky and Beck (2021) emphasize that trust is a crucial factor in successful interorganizational collaboration during cybersecurity threats. If the public believes their data could be shared without sufficient safeguards, this could lead to a loss of trust in both private organizations and the government, undermining the very goal of securing sensitive information.

Cultural and subcultural influences also play a significant role in shaping the way CISA is viewed by different segments of society. While individuals in tech savvy communities may be more inclined to support the policy due to its potential for enhancing security, those in privacy focused subcultures may view it as an invasion of their rights. According to Mussington and MacLellan (2018), countries like the U.S. often struggle with balancing the competing demands of national security and personal privacy, a conflict that is especially pronounced in the context of policies like CISA. This division in values highlights how cultural perspectives on privacy and security can shape the way a policy is implemented and received.

In conclusion, CISA carries significant social implications. While its intent to enhance national security by encouraging information sharing is clear, it also raises concerns about privacy, trust, and the cultural divide between different societal groups. The social factors behind CISA's development show that cybersecurity cannot be tackled in isolation, it requires careful balancing of national security needs with the protection of individual rights. As the policy continues to evolve, it will be essential to ensure that the societal implications of such laws are carefully considered, and that privacy concerns are adequately addressed. The discussions

surrounding CISA illustrate the complexities of modern cybersecurity policy and highlight the need for ongoing debate about the social responsibilities of both the government and private organizations.

Citations

- Hitchens, Theresa, and Nilsu Goren. *International Cybersecurity Information Sharing Agreements*. Center for International & Security Studies, U. Maryland, 2017. *JSTOR*, http://www.jstor.org/stable/resrep20426. Accessed 6 Apr. 2025.
- Mussington, David, and Stephanie MacLellan. "US Cyber Policy: Sources of and Impediments to Rapid Progress." *Governing Cyber Security in Canada, Australia and the United States*, edited by Christian Leuprecht, Centre for International Governance Innovation, 2018, pp. 9–12. *JSTOR*, http://www.jstor.org/stable/resrep17311.7. Accessed 6 Apr. 2025.
- Solansky, Stephanie T., and Tammy Beck. "Interorganizational Information Sharing: Collaboration during Cybersecurity Threats." *Public Administration Quarterly*, vol. 45, no. 1, 2021, pp. 105–22. *JSTOR*, https://www.jstor.org/stable/27204175. Accessed 6 Apr. 2025.