Social Implications of CISA

CJ McDonald

Department of Cybersecurity, Old Dominion University

CYSE 425W: Cybersecurity Strategy and Policy

Professor Bora Aslan

November 24, 2024

The Cybersecurity Information Sharing Act of 2015 was developed to improve cybersecurity by fostering collaboration between private companies and the federal government. This policy facilitates the voluntary sharing of cybersecurity threat information, promoting a stronger defense against cyber threats. While CISA provides significant national security benefits, it also has profound social implications. These include its effects on privacy, individual autonomy, and the balance of power within society. This paper explores these social implications, paying particular attention to the social factors that led to CISA's development, the social consequences of its implementation, and the influence of cultural and subcultural norms on the policy.

The development of CISA was driven by the increasing frequency and sophistication of cyberattacks, which threatened both private and public sectors. High-profile breaches such as the Target breach in 2013 and the Anthem breach in 2015 exposed vulnerabilities in both sectors, compromising the sensitive personal information of millions of individuals (Renaud & Stolfo, 2015). These incidents created a sense of urgency, underscoring the need for improved communication and collaboration between private companies and government entities to prevent similar attacks. This urgency led to widespread recognition that cybersecurity is a collective responsibility, requiring coordinated efforts across industries and government levels to mitigate risks effectively.

Before CISA, legal and competitive concerns hindered information sharing between companies and the government. Thus, CISA was developed to break down these barriers by providing legal protections, thereby promoting a more unified approach to cybersecurity. This legal framework not only facilitated greater collaboration but also fostered a sense of shared

responsibility across sectors, encouraging companies to contribute to national security without fear of legal repercussions.

One of the major social implications of CISA is its impact on privacy and individual rights. CISA's broad language allows the federal government access to substantial amounts of shared data, which raises concerns about potential government overreach and surveillance (Sedenberg & Dempsey, 2018). The vague language of the policy can lead to the misuse of personal information without the consent of the individuals involved (Jaffar, 2016). This situation represents a significant trade-off: while CISA enhances national security by allowing faster responses to cyber threats, it does so at the potential cost of infringing upon individual privacy rights. The lack of explicit safeguards in the policy has led to ongoing debates about how to ensure accountability and transparency in the use of shared data. The risk of privacy violations has led to diminished public trust, particularly among communities that are already skeptical of government surveillance practices.

In addition to privacy concerns, CISA has also had economic and social consequences that affect the balance of power within society. The economic benefits of CISA have disproportionately favored larger cybersecurity firms, which have more resources to comply with and leverage the policy to their advantage (Yang et al., 2020). This has intensified competition within the industry, making it difficult for smaller companies to thrive and raising concerns about equitable access to cybersecurity advancements. This has led to concerns about fairness within the cybersecurity industry, as smaller companies struggle to compete. This disparity has broader social implications, as it exacerbates existing inequalities within the industry and limits the opportunities available to smaller firms, thereby reinforcing economic disparities.

The cultural context in which CISA was developed also played a significant role in shaping the policy. The heightened fear of cyber threats, amplified by media coverage of high-profile cyberattacks, created a cultural environment that prioritized security over privacy. This cultural emphasis on national security influenced the development of CISA, leading policymakers to prioritize rapid information sharing and collaboration between private companies and the government, even at the cost of privacy rights. This prioritization reflects a broader societal trend of valuing collective safety over individual freedoms, especially in times of heightened threat perception.

Furthermore, subcultural influences within the cybersecurity community have shaped CISA's implementation. The cybersecurity community, which values proactive threat management and collaboration, supported CISA as a necessary tool for improving national cybersecurity resilience. However, privacy advocates within this community have raised concerns about the implications for individual rights and government accountability, emphasizing the need for more robust checks and balances to prevent abuse of power. These advocates argue that without clear limitations and oversight mechanisms, the risk of privacy violations becomes a significant concern. This divide within the cybersecurity community illustrates the cultural and subcultural tensions that have influenced CISA, as different groups within society prioritize different values—security versus privacy.

CISA has had significant social implications, from affecting individual privacy rights to reinforcing economic disparities within the cybersecurity industry. The social factors that led to its development, including the increasing frequency of cyberattacks and the need for a coordinated response, highlight the urgency with which the policy was implemented. However, the cultural environment that prioritized security over privacy and the economic consequences of

favoring larger firms underscore the complex social trade-offs involved in CISA's implementation. As cyber threats continue to evolve, it is crucial to ensure that policies like CISA are implemented to balance security with the protection of individual rights and address the needs of all stakeholders within society. This balance can be achieved by integrating more stringent privacy safeguards, ensuring transparency in data handling, and involving diverse stakeholders in policy evaluation and decision-making processes.

References

Jaffar, J. N. (2016). *Carrots and Sticks in Cyberspace: Addressing Key Issues in the Cybersecurity Information Sharing Act of 2015*. Scholar Commons. https://scholarcommons.sc.edu/sclr/vol67/iss3/5/

Sedenberg, E., & Dempsey, J. (2018). *Cybersecurity Information Sharing Governance Structures: An Ecosystem of Diversity, Trust, and Tradeoffs*. https://arxiv.org/pdf/1805.12266.pdf

Yang, A., Kwon, Y. J., & Tom Lee, S.-Y. (2020). The adoption of RFID in fashion retailing: a business value‐added framework | Emerald Insight. *Industrial Management & Data Systems*. https://doi.org/10.1108//imds