CISA: A Policy Analysis Review

CJ McDonald

Department of Cybersecurity, Old Dominion University

CYSE 425W: Cybersecurity Strategy and Policy

Professor Bora Aslan

September 29, 2024

\

The Cybersecurity Information Sharing Act, CISA, is a key piece of legislation designed to improve cybersecurity in the United States. As the world becomes increasingly digital, cyberattacks have grown into a significant threat to both public and private sectors, highlighting the need for better collaboration to address these risks. To meet this need, CISA facilitates the voluntary sharing of cybersecurity threat information between the federal government and private companies, aiming to enhance the nation's ability to prevent, detect, and respond to cyber threats. By promoting information sharing, CISA helps individuals and organizations implement preventative measures and manage cyber risks more effectively.

The passage of CISA was driven by the growing threat of cyberattacks, which were increasing in both frequency and sophistication. Before CISA, high-profile cyber incidents such as the breaches of Target in 2013 and Anthem in 2015 exposed vulnerabilities in both the private and public sectors, compromising the sensitive personal information of over 150 million individuals, highlighting the need for improved communication and collaboration across industries and government entities. As explained by Renaud and Stolfo (2015), the legislative response was shaped by the growing consensus that cybersecurity needed to be a national priority, not just a corporate or agency issue.

However, before CISA, there were significant barriers to information sharing between the private sector and government agencies. Companies were often reluctant to disclose cyber threat data due to concerns over legal consequences or competitive disadvantages (New America Foundation, 2016). As a result, cyber threats were often addressed in isolation, limiting the collective ability to respond effectively. Consequently, CISA was developed to break down these barriers by providing legal protections for companies that voluntarily share cyber threat indicators with the government, fostering a more unified and proactive approach to cybersecurity.

CISA has been especially effective in public-private partnerships, particularly within the health sector, which is increasingly vulnerable to cyber threats. The healthcare industry faces a growing number of cyberattacks, with ransomware incidents in hospitals disrupting patient care and access to medical records. According to Tanwar et al. (2020), CISA facilitates information sharing between healthcare organizations and government agencies like the Department of Homeland Security without legal repercussions, promoting collaboration that enhances cybersecurity measures in this critical sector.

For instance, ransomware attacks on hospitals have led to patient diversions and hindered access to essential data, showcasing the urgent need for timely information sharing. During these incidents, healthcare providers utilized CISA's framework to rapidly exchange intelligence, enabling coordinated responses and mitigation strategies. Furthermore, CISA supports the establishment of Information Sharing and Analysis Centers, such as the Health Sector Cybersecurity Coordination Center, or HC3 for short, which fosters collaboration and provides resources tailored to healthcare providers. Initiatives like the HHS 405(d) program focus on aligning security approaches across the healthcare sector, helping organizations adopt best practices to combat current threats, including ransomware. These collective efforts under CISA have strengthened the cybersecurity posture of healthcare providers, ensuring uninterrupted care delivery and the safety of patient data.

Beyond the healthcare sector, CISA plays a vital role within the United States' broader national cybersecurity strategy by fostering public-private partnerships and enhancing collaboration to protect critical infrastructure. The act aligns with key policies like the Federal

Information Security Modernization Act, FISMA, and the National Institute of Standards and Technology Cybersecurity Framework, or NIST, promoting real-time information sharing, which improves security both domestically and internationally. Renaud and Stolfo (2015) emphasize that this alignment helps integrate CISA into a larger effort to safeguard national cybersecurity.

Moreover, CISA encourages international cooperation, recognizing that cyber threats often transcend national borders. By promoting the sharing of threat intelligence, CISA supports global responses to cybersecurity challenges. Furthermore, CISA helps cultivate a culture of cybersecurity awareness across public and private sectors by encouraging the disclosure of vulnerabilities and threats. This proactive stance is vital to building resilience against cyberattacks and enhances the nation's ability to defend against emerging risks.

In conclusion, CISA is critical in enhancing the nation's cybersecurity by facilitating collaboration between public and private sectors. Its framework for sharing threat intelligence without legal repercussions has strengthened the security of vulnerable sectors like healthcare while fostering a culture of preparedness. CISA's alignment with national and international cybersecurity policies further underscores its importance in addressing evolving cyber threats. As cyber risks continue to grow, CISA remains a vital tool in safeguarding critical infrastructure and ensuring coordinated, effective responses to emerging challenges.

References

CISA. (2023). *Cybersecurity Best Practices | Cybersecurity and Infrastructure Security Agency CISA*. Www.cisa.gov. https://www.cisa.gov/topics/cybersecurity-best-practices

Cybersecurity and Infrastructure Security Agency. (n.d.). *Healthcare and Public Health Sector | CISA*. Www.cisa.gov. https://www.cisa.gov/stopransomware/healthcare-and-public-health-sector

ENISA. (2017). *Information Sharing and Analysis Centers (ISACs)*. Europa.eu. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing

Greene, R. (2015). *Cybersecurity Information Sharing Act of 2015 Is CyberSurveillance, Not Cybersecurity*. https://static.newamerica.org/attachments/2741-cybersecurity-information-sharing-act-of-2015-is-cyber-surveillance-not-cybersecurity/CISA_Cyber-Surveillance.488b3a9d2da64a27a9f6f53b38beb575.pdf

HHS 405(d). (n.d.). 405d.hhs.gov. https://405d.hhs.gov/

Plachkinova, M., & Maurer, C. (2018). Teaching Case: Security Breach at Target. *Journal of Information Systems Education*, *29*(1), 11–20. https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1006&context=jise

Steinberg, S., Adam, Stepan, K., Rattray, G., & Healey, J. (2021). *Target Cyber Attack: A Columbia University Case Study*. https://www.sipa.columbia.edu/sites/default/files/2022-11/Target%20Final.pdf

Young, K. (2021, September 27). *Cyber Case Study: Anthem Data Breach*. CoverLink Insurance - Ohio Insurance Agency. https://coverlink.com/case-study/anthem-data-breach/