Ethical Implications of Information Sharing in Cybersecurity

Michael A Gurule

Old Dominion University

CYSE425W: Cyber Strategy and Policy

Bora Aslan

March 31, 2024

Ethical Implications of Information Sharing in Cybersecurity

In the realm of cybersecurity, the exchanging of information plays a vital role in defending against malicious activities and protecting sensitive data (Bullock, Johnson, & Williams, 2019). This sharing of information raises ethical concerns in regard to privacy, transparency, and the balance between security and users' rights. This paper explores the ethical implications of information sharing in cybersecurity and is a brief overview of ethical considerations, focusing on privacy rights.

Benefits vs. Ethical Implications

Information sharing in cybersecurity helps organizations to get threat information out faster and more streamlined. This will help not just the organization sharing, but all organizations that may be affected by the threat. This is quite needed in the ever-changing landscape of the cyber world. Bullock et al. (2019) agree that a collaborative effort is needed among industry peers, government agencies, and cybersecurity professionals to enhance collective defense mechanisms, thereby bolstering overall security posture (Bullock et al., 2019). By sharing insights into cyber threats as they occur, organizations can proactively implement countermeasures and mitigate potential breaches. This will ultimately lead to the safeguarding of critical infrastructures and sensitive information (Hassan, & Seidl, 2019). Transparency also adds a level of overall trust to the organization amongst all of its users and partners, even if that is to announce a breach that will temporarily damage that trust.

Information sharing in cybersecurity also raises a variety of ethical dilemmas including those dealing with privacy infringement and data misuse. The exchange of sensitive information, including personal and organization's proprietary data, needs to have strict safeguards in place to protect individual/organizational privacy rights (Arachchilage & Love, 2017). Unauthorized disclosure or mishandling of shared information can lead to privacy breaches, damaged reputations, and legal repercussions for all involved parties. That is in addition to the possible privacy breach that was brought about by the original threat about which the information is now being shared. Also, the unequal allocation of resources and subject matter expertise may further increase the gap in power. This leads to smaller organizations or less-developed regions in the world being at a disadvantage in the ability to access critical threat intelligence (Dhillon & Moores, 2001). The key to solving the separation in power lies in the ethical frameworks that must address the equal distribution of benefits and responsibilities associated with information sharing initiatives in guidelines, policy, and law.

Achieving and maintaining a balance between cybersecurity objectives and individual privacy rights is paramount in ethical decision-making. Organizations must utilize a risk-based approach to information sharing which prioritizes security measures that minimize harm to everyone involved while maximizing the collective benefit (Bullock et al., 2019). Transparency and informed consent are essential principles in ethical information exchange. This is to ensure that individuals understand the implications of sharing their data and have control over its usage (Hassan & Seidl, 2019). Regulatory frameworks, such as the General Data Protection Regulation (GDPR), impose obligations on entities handling personal data, reinforcing ethical standards and accountability in cybersecurity practices. More frameworks that create an atmosphere of incentive and repercussion may be able to change the landscape into one that information can be shared on, yet remain safe and private.

Conclusion

Information sharing is essential in combating cyber threats and enhancing overall cybersecurity resilience. However, ethical considerations regarding privacy, transparency, and equality must guide the implementation of information sharing initiatives. By adhering to ethical principles, everyone can utilize the benefits of collaborative cybersecurity efforts while mitigating potential risks to individual rights and societal values.

References

Arachchilage, N. A. G., & Love, S. (2017). Ethical considerations in cybersecurity research. *2017 16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom).*

Bullock, J. B., Johnson, D., & Williams, T. (2019). Ethical considerations of cybersecurity. In *Cybersecurity Readiness*. Springer, Cham.

Dhillon, G., & Moores, T. (2001). Case studies of corporate information security cultures. *Information & Management*, 39(5), 467-476.

Hassan, Q., & Seidl, D. (2019). Ethical considerations in cybersecurity. *2019 3rd Cyber Security in Networking Conference (CSNet)*.