Social Implications of Information Sharing in Cybersecurity

Michael A Gurule

Old Dominion University

CYSE425W: Cyber Strategy and Policy

Bora Aslan

April 14, 2024

Social Implications of Information Sharing in Cybersecurity

As technology becomes more entwined into everyday life, all forms of social considerations must be taken when discussing the sharing of information. “Information society” has become a commonplace expression and this virtual space closes the gap between people allowing the expansion of social areas (Canongia, C. & Mandarino, R., 2012). Information sharing is the control of breach and threat information and its dissemination to other organizations outside of the originally affected. It has been discussed on whether legal implications should be set to force organizations to share information about breaches, or potential breaches, but less of a focus on what that means from a societal standpoint. This paper will focus on what it means to society to allow information sharing amongst all organizations in the cyber landscape.

The Importance of Information Sharing In Society

Society has moved forward to the information age, and everything is at arms-reach. Society expects organizations to safeguard them and their information, even if they are unable to do it themselves. Just like with the military complex, protection is expected and society views this as a right. Many guidelines and policies have been implemented to create a more secure future for all users of that cyberspace. Even Microsoft has set out to create an international organization, Digital Geneva Convention, to promote and streamline information sharing guidelines and policies. Microsoft’s focus is on the connection between corporations and the citizens and its tenants in this approach are based on social ques. Three out of four of the main objectives are societal based: trust building, balance of responsibility, and socio-political influence (Fairbank, N., 2019). The strive of a private organization in the social landscape of information is a testament to the importance of it succeeding.

Security information sharing (SIS) is of vital importance and will lead to a more secure future for all of society but one must take into consideration the possible shortfalls in information sharing. Only then can we move forward and solve the issues at hand. Though information sharing comes with direct implications, such as data loss during sharing, this will focus on a more abstract idea, human behavior. According to Mermoud, A., et al. (2019), instead of trading financial means for information, SIS should be characterized by "…continued social interaction among many individuals who mutually exchange information assets." The problem is that this is a perfect world scenario where human factors are not taken into consideration. Interests may not be aligned between action taken and organizational standards as agents may not always be indifferent. A single passage from the article sums up the problem with human behavior in information sharing, "In contrast, it showed that human beings have bounded instead of perfect rationality. They often violate social expectations, have limited information-processing capacity, use heuristics when making decisions, are affected by emotion while doing so, and retaliate even if the cost of retaliation exceeds its benefits." (Mermoud, A., et al., 2019)

A change in attitude and overall way of doing things must be implemented for any kind of information sharing to properly utilized. Education and proper training and professional development is one way to start implementing changes at a slow pace. Liu, D., Ji, Y., & Mookerjee, V. (2011) propose the use of a "Social Planner" in organizations to combat the adversarial mindset organizations have with other organizations. This social planner would be more aligned with an advisor than an employee of the company. They would encourage proper sharing and tactics to do so for organizations to ease themselves in making the proper choice to share. Not only would this aid the cyber society as a whole, but respect from users will be given to organizations for taking the initiative to try and combat social related issues. "The proposed

coordination schemes [social planner], with some modifications, achieve the socially optimal outcome even when the firms are risk-averse.” (Liu, D., Ji, Y., & Mookerjee, V., 2011)

Conclusion

In conclusion, the social implications of information sharing in cybersecurity underscore the intricate balance between technical protocols and human behavior. While society expects organizations to protect data as a fundamental right, challenges arise from human factors like bounded rationality and self-interest, hindering effective collaboration. Initiatives such as the Digital Geneva Convention highlight the importance of international cooperation and trust-building in cybersecurity frameworks. Addressing these challenges requires a cultural shift within organizations, emphasizing education and the establishment of roles like the proposed "Social Planner" to promote collaboration and mitigate adversarial mindsets. By aligning incentives with societal goals, coordination mechanisms can lead to socially optimal outcomes, fostering responsible information sharing and building trust between organizations and users, ultimately contributing to a safer digital landscape for all.

References

Canongia, C. & Mandarino, R. (2012). Cybersecurity: The New Challenge of the Information Society. In M. Cruz-Cunha, P. Gonçalves, N. Lopes, E. Miranda, & G. Putnik (Eds.), *Handbook of Research on Business Social Networking: Organizational, Managerial, and Technological Dimensions* (pp. 165-184). IGI Global. https://doi.org/10.4018/978-1-61350-168-9.ch009

Fairbank, N. (2019) The state of Microsoft?: the role of corporations in international norm creation, *Journal of Cyber Policy*, 4:3, 380-403, DOI: 10.1080/23738871.2019.1696852

Liu, D., Ji, Y., & Mookerjee, V. (2011). Knowledge sharing and investment decisions in information security. *Decision Support Systems*, *52*(1), 95-107. https://doi.org/https://doi.org/10.1016/j.dss.2011.05.007

Mermoud, A., et al. (2019). To share or not to share: a behavioral perspective on human participation in security information sharing. *Journal of Cybersecurity*, *5*(1). https://doi.org/10.1093/cybsec/tyz006