The Ethical Implications of Financial Incentives for Investing in Cybersecurity Policies

Eric Mung'aũ Preston

Old Dominion University

CYSE 425W: Cybersecurity Strategy and Policy

Dr. Bora Aslan

March 30, 2025

Introduction

The implementation of financial incentives for companies to invest in cybersecurity policies has been shown to be effective and cause positive political change. However, to support both companies and smaller organizations of people, an ethical analysis is required to ensure the effectiveness of the most ethical policies. This paper will cover the ethical implications of financial incentives to invest in future cybersecurity policies, the costs and benefits for societal groups, and the potential effects on people's rights.

Ethical Implications

Several ethical dilemmas appear when financial incentives for cybersecurity policies are at play. For example, different types of financial incentives lead companies to postpone cybersecurity investments rather than increase them. According to Wells-Dietel & Erkan-Barlow (2023), when companies are presented with short-term financial incentives like stock, they are more likely to delay cybersecurity investments to maintain the relationship with shareholders and generate profit because of the intangibility of cybersecurity risk. Furthermore, even with an incentive like cyber insurance, it can lead to the same behavior of allocating resources into the breach instead of over time due to the insurance taking partial control away from the company, leading to riskier decisions.

Costs and Benefits for Societal Groups

Companies utilize cyber insurance to transfer the financial risk in case of a cyber attack, and it has been considered effective in mitigating financial losses to the benefit of stockholders or investors. Additionally, transferring risk to cyber insurance has the potential to improve the reputation of the company after a cyber-attack. However, while the investors, stockholders, and insurance companies benefit from this arrangement, the users of the technology whose

information is compromised lose the most from a cyber-attack, ranging from exposed private information, cyber-scams, and a sense of insecurity with the information on their technology. (Erkan-Barlow & Wells-Dietel, 2023).

Does the Policy Address People's Rights?

Cyber insurance as a requirement for mitigating damage and losses caused by cyber-attacks has shown to be ineffective in addressing people's rights. As mentioned earlier, users' rights are the least protected from cyber-attacks and further damage. Hiller et al. (2024) recommend a more robust strategy that includes policy makers incentivizing cybersecurity companies financially that demonstrate a commitment to significant investment towards cybersecurity structures. Additionally, the proposal for a Federal Cybersecurity Investment Tax (FCIT) credit to these companies shows promise of a more secure global ecosystem.

How Does the Policy Affect People's Rights?

While cyber insurance is lacking in its ability to address rights, financial incentives can affect people's rights in different ways. Vagle (2023) argues that because organizations experience a term called "moral hazard," where they feel less incentive to be safer because of insurance, this affects other decisions, such as manufacturers not making secure products for their consumers, endangering their privacy. Alternatively, a study on corporate social responsibility for cybersecurity showed that when organizations effectively balance their incentives for profit with maintaining a productive environment for employees, it improves cybersecurity awareness and, in turn, improves the protection of customers (Kim & Lee, 2025)

Conclusion

In conclusion, there is a present ethical dilemma that can occur with the implementation of financial incentives for companies. The dilemma of how financial incentives influence

companies is apparent regarding financial incentives like stock or cyber insurance that instill short-term economic behavior. While there can be some protection for companies, stockholders, and investors by having cyber insurance, security breaches are still significant and most detrimental to users due to short-term enforced behavior. Financial incentives also have the potential to be ineffective in addressing rights effectively, like cyber insurance, or lead to negative consequences, like the compromised privacy of customers. However, there are positive outcomes for financial incentives to improve both the security operations of a company and, in turn, benefit the customers associated with them.

References

Hiller, J., Kisska-Schulze, K., & Shackelford, S. (2024). Cybersecurity carrots and sticks. *American Business Law Journal*, *61*(1). https://doi.org/10.1111/ablj.12238

Kim, B.-J., & Lee, J. (2025). The impact of corporate social responsibility on cybersecurity behavior: The crucial role of organizationally-prescribed perfectionism. *Humanities and Social Sciences Communications*, *12*(1). https://doi.org/10.1057/s41599-025-04511-w

Vagle, J. L. (2020). Cybersecurity and Moral Hazard. *SSRN Electronic Journal*, *23*(1), 71–113. https://doi.org/10.2139/ssrn.3055231

Wells-Dietel, B., & Erkan-Barlow, A. (2023). The current state of cyber insurance and regulation in the context of investment efficiency and moral hazard: A literature review. *Journal of Insurance Regulation*, *42*, 1–27. https://doi.org/10.52227/26579.2023