Abstract

Business instabilities due to cybersecurity attacks and data breaches make cyber risk strategic decision making a critical part of a company’s business operation. Co-operation and competition among interacting businesses make it increasingly challenging to quantify the risks and understanding the organization’s socially optimal level of investment in cybersecurity. This paper investigates the role of social preferences in decision making under cyber risks and uncertainties created by incorporated externalities.

Keywords: cybersecurity risks, behavioral economics, social preferences

Objective

Humans play a vital role in cybersecurity strategic decision making, and at the same time, they are often considered the weakest links in this ecosystem [1]. However, deterrence and prevention of new and increasing forms of cyber attacks require the design of IT systems from a cybersecurity organizational perspective rather than a human-computer interaction perspective. The area of cybersecurity in organizations has three essential properties. First, it consists of heterogeneous interacting stakeholders and actors characterized by distinct local cultures, structure, machines, and methods [2]. Stakeholders act upon the basis of their own local states at any given time. Second, cybersecurity problems stem from dynamic systems and are driven by the interaction among various stakeholders. These interactions affect future local states and, therefore, create systemic complexity. Third, there are strategic decision makers whose decision processes take into account past actions, potential future actions, and outcomes of other actors. They have heterogeneous motivations, preferences, and benefits. Since these properties are based on the organizations’ unique sets of objectives, processes, and resources, it is difficult to see how a one-size-fits-all cybersecurity strategy can be optimal.

The trend toward more globalized production has increased inter-organizational dependencies. Particularly, businesses are forming multi-layered supply chains, as illustrated in Figure 1. As an externality, security and insecurity can be distributed disproportionately in a supply chain. The co-opetition (i.e. organizations may both compete and cooperate at the same time [3]) and interdependent preferences among the organizations face them with a challenge of understanding and measuring the risks that are propagating from them.

Research Method

Different economics models have been employed to address the challenges in the field of cybersecurity in both technical and social aspects [4, 5, 6]. In these models, agents are rational, selfish, and have complete information about other agents. However, in real-world scenarios, agents might be irrational, reciprocal, and have incomplete information about their environment. This paper shows by empirical examples that these standard models fail to properly model cybersecurity economics when social preferences are ignored.
In our study, the key research question is how to model heterogeneous incentives and preferences at the organizational level. The major aim is to better understand under which conditions the social preferences have significant effects on cybersecurity. To achieve this, we are aiming at developing an understanding of the important determinants of the socially optimal level of cybersecurity to prevent market failures.

Moreover, the paper investigates which type of social preferences (Reciprocal Fairness, Inequity Aversion, Pure Altruism and Spiteful or Envious [7]) is stronger and quantitatively a core motive in the domain of cybersecurity. We employed the Delphi Survey technique [8] to address these questions. The respondents of this survey are cybersecurity team members (Chief Information Security Officers, Information Security Analysts, Security operations center staff, etc.) and decision makers in organizations (Chief Executive Officers, Board Members, etc.). The selected organizations are among the clients of cybersecurity consultancy companies.

Finally – assuming that cybersecurity is a public good – we investigate the issue of free riders and externalities of weak cyberdefenses [9]. This study describes and attempts to measure organizations and the individual’s cooperation preferences in the cybersecurity domain by using a public goods game designed for that purpose. We use Public Goods Games (PGG) as a paradigm for explaining collective action and cooperation among the cyber agents [10]. The prototype of this game is an extension of CyberAIMS (Cyber Agents’ Interactive Modeling and Simulation) [11], a simulation tool for training System and Adversarial Thinking and strategic decision making.

**Conclusion**

Cybersecurity is no longer an isolated technical problem. Positive and negative security payoffs resulting from interactions among businesses require new modeling approaches by including social preferences. Using the Delphi Survey technique we indicated the relevant types of social preferences in the domain of cybersecurity. Moreover, this study identified the effects of coopetition on market failures and investigated the role of social preferences in managing the interaction with free riders by carrying out a public goods game experiment.
References


