Decision Support Model for Cybersecurity Risk Planning: A Two-stage Stochastic Programming Framework Featuring Firms, Government and Attacker

March 11, 2019

Abstract

We study the decision making problem in cybersecurity risk planning with regards to resource allocation strategies by government towards intelligence and firms' investments in detection and containment safeguards. Aiming to minimize the social costs incurred due to data breaches, we consider not only the monetary investment costs, but also the deprivation costs due to delayed detection and containment. We accomplish this via a two-stage stochastic programming model that formulates the investment actions of government and firms to minimize losses from cyber-attacks. In the first stage, the firms decide on the prevention and detection investments aided by intelligence investments by the government that improve detection effectiveness. In the second stage, once the attacker actions are realized, the firms decide on containment investments after evaluating the cyberattacks. Our models optimize the overall social cost, which includes the deprivation cost capturing the losses to firms due to delayed detection and containment. We also consider the effect of positive externalities of the overall cybersecurity investment on an individual firm's resource allocation attitude. The optimal decision guides the firms on the cybersecurity countermeasure portfolio mix (detection vs. prevention vs. containment) and government intelligence investments while accounting for actions of a strategic attacker and limitations such as firm budgetary resources. We demonstrate the applicability of our model via a case study. Our findings indicate that externality can reduce government's intelligence investment and that the firms' detection investment receives priority over the containment investment as it pertains to the firm's budget allocation. Further, we also note that while the

prevention effectiveness has a decreasing impact on intelligence, the intelligence effectiveness has an increasing impact on intelligence.

Keywords: cybersecurity; stochastic programming; intelligence investment; social cost; safeguards; externality