Socially Optimal IT Investment for Cybersecurity

Abstract

This paper uses the concept of social cost - comprised of private and externality costs - to examine the optimal balance between prevention and detection & containment safeguards under three sources of uncertainty. We propose a robust optimization model with the help of distribution-free ellipsoidal uncertainty sets to ease the challenge of providing exact estimates for uncertain input. Tested on a case study, results from twenty-five deterministic test scenarios first reveal strong resource allocation preference toward prevention safeguard and then it shifts to containment & detection safeguard when budget constraint is relaxed. Results from fifty four robust test instances indicate that, among the three sources of uncertainty, adjusted effectiveness of prevention safeguard has the greatest impact on both the social cost and optimal makeup of the safeguards. Our analysis points out some serious pitfalls in the existing cybersecurity framework that mainly relies on prevention safeguard and provides urgently needed guidelines on cybersecurity to decision makers.