Chapter 12
Competitive Cyber-Insurance and Internet Security

Nikhil Shetty, Galina Schwartz, Mark Felegyhazi, and Jean Walrand

Abstract This paper investigates how competitive cyber-insurers affect network security and welfare of the networked society. In our model, a user’s probability to incur damage (from being attacked) depends on both his security and the network security, with the latter taken by individual users as given. First, we consider cyber-insurers who cannot observe (and thus, affect) individual user security. This asymmetric information causes moral hazard. Then, for most parameters, no equilibrium exists: the insurance market is missing. Even if an equilibrium exists, the insurance contract covers only a minor fraction of the damage; network security worsens relative to the no-insurance equilibrium. Second, we consider insurers with perfect information about their users’ security. Here, user security is perfectly enforceable (zero cost); each insurance contract stipulates the required user security. The unique equilibrium contract covers the entire user damage. Still, for most parameters, network security worsens relative to the no-insurance equilibrium. Although cyber-insurance improves user welfare, in general, competitive cyber-insurers fail to improve network security.

Nikhil Shetty
UC Berkeley, Berkeley-94720, e-mail: nikhils@eecs.berkeley.edu

Galina Schwartz
UC Berkeley, Berkeley-94720, e-mail: schwartz@eecs.berkeley.edu

Mark Felegyhazi
ICSI, Berkeley-94704, e-mail: mark@icsi.berkeley.edu

Jean Walrand
UC Berkeley, Berkeley-94720, e-mail: wlr@eecs.berkeley.edu
12.1 Introduction

In this paper, we propose a model to study the effects of cyber insurance on user security and their welfare. Our model highlights how network externalities combined with information asymmetry lead to a missing market for cyber insurance.

The Internet serves as a ubiquitous communication platform for both individuals and businesses. Thus, an increasing amount of wealth is accessible online, and cyber-crime is becoming one of the most lucrative criminal activities. Cyber-crime is lucrative because network vulnerabilities are easy to exploit and persecution of cyber-criminals is plagued by enforcement problems. First, and importantly, criminals are relying on the anonymity of the Internet protocols to disguise their traces. Second, global Internet connectivity makes it difficult for law enforcement authorities to identify the origin of the attacks. Exploiting national differences in legal systems, criminals often operate safely from countries with the weakest legislations and enforcement. Third, criminals quickly adapt their attack strategies as new defenses are developed; thus, cyber-crime evolves to minimize the chance of persecution. Altogether, this situation results in formation of highly professional, mafia-style cyber-crime establishments, which are rapidly expanding, see [2].

Technology-based defense and enforcement solutions are available, but there is a consensus among security researchers [2] that the existing security problems cannot be solved by technological means alone. We concur that these security problems primarily result from misaligned incentives of the networked parties with respect to their security. Existing research [4, 7, 16, 18, 19] indicates that risk management in general and cyber-insurance in particular are potentially valuable tools for security management. Still, at present, risk management capabilities are virtually nonexistent in the network [2].

We model the effects of informational asymmetries in the presence of network externalities, and study their consequences for network security incentives. We believe that these features of the environment induce socially suboptimal network security, and complicate the management of security risks. We build on the seminal ideas of Akerlof [1], Rothschild and Stiglitz [17] and others, which we combine with the ideas of interdependent security originated by Heal-Kunreuther [14], Gordon-Loeb [8] and Hausken [11].

In our model, all users are identical, meaning that their wealth is identical and they suffer identical damage if successfully attacked. The user’s probability of being attacked depends on both the user security level and the network security level, which individual users take as given. Thus, we have an externality. Indeed, due to this externality, individually optimal user security level is lower than the socially optimal one.

1 This work was funded in part by the National Science Foundation under grant NSF-0433702. Any opinions, findings, conclusions, and recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funding source.
2 See [20] for the literature review.
3 See also [3, 5–7, 9, 10, 12, 13, 21]. This list is by no means exhaustive.