Available online at www.sciencedirect.com
ScienceDirect
ELSEVIER Journal of Accounting and Public Policy 25 (2006) 629–665
Journal of Accounting and Public Policy
www.elsevier.com/locate/jaccpubpol

Income, interdependence, and substitution effects affecting incentives for security investment

Kjell Hausken *

Faculty of Social Sciences, University of Stavanger, N-4036 Stavanger, Norway

Abstract

Firms in cyber war compete with external intruders such as hackers over their assets. Each firm invests in security technology when the required rate of return from security investment exceeds the average attack level, or when the formal control requirements dictate investment. Each firm invests maximally in security when the average attack level is 25% of the firm's required rate of return. The income effect eliminates or "freezes" parts of the agent's resource, attack tools, and competence. The security investment decreases in the income reduction parameter when the agent's resource is low, is inverse U shaped when the resource is intermediate, and drops to zero when the external threat is overwhelming. A sufficiently strong income effect eliminates the external threat. When two firms are interdependent, security investments and attacks impact both firms. With increasing interdependence, each firm free rides by investing less, suffers lower profit, while the agent enjoys higher profit. The substitution effect causes the agent to allocate his attack optimally between the firms. The attack distribution is endogenized. Each firm's security investment increases in its asset and investment efficiency. The attack against each firm increases in the product of the firm's asset and

* Tel.: +47 51 831632/831500; fax: +47 51 831550.
E-mail address: kjell.hausken@uis.no

0278-4254/$ - see front matter
doi:10.1016/j.jaccpubpol.2006.09.001

investment inefficiency. Specific analyses are made of how the substitution effect impacts security investment for differently sized firms.

Keywords: Cyber war; Conflict; Contest success function; Security technology investment; Security breaches; Income; Interdependence; Substitution

1. Introduction

The intensity of cyber war has increased through the Internet revolution. Firms are bombarded with attacks of all kinds, and invest increasingly in security technology. A variety of principles are applied to determine the size of the investment. The common approach in today's literature is to assume that the external threat is fixed and immutable. This means that the nature of cyber war is not fully appreciated. This article develops a model that accounts for the cyber war between firms as strategic players on the one hand and the external threat phrased as a strategic player on the other hand. None of the warring sides are fixed and immutable. They adapt to each other. Available resources by all players, and strategic choices, depend on all strategic choices and the nature of cyber war. As developed in the conflict and rent seeking literature, the firms and the external agents wage war over the firms' assets. This approach has not been made earlier in this literature, and generates new and interesting insights.

Three effects which with a few exceptions are ignored in today's literature are discussed. The income effect eliminates parts of the external agent's resource, or weakens the agent's ability to convert resources into an attack, which reduces the attacker's overall ability or willingness to conduct cyber war. The interdependence effect means that two firms in varying degrees are intertwined, dependent, and influenced by each other, so that one firm's security investment benefits both firms, and the attack on one firm also affects the other firm. The substitution effect causes the external agent to consider the firms' strategies and substitute into the most optimal and least costly attack allocation across the two firms. The three effects cause quite different optimal strategies regarding security investment and information sharing for firms.

The article describes the external agent as hackers or perpetrators intending to break through the security of firms to get access to assets. The model is phrased as cyber war, but applies for all kinds of external agents with hostile intentions directed towards appropriating firms' assets. Examples are terrorists, crime syndicates, thieves, proletarians, and various agencies, firms, or other actors engaged in asset appropriation. Firms in cyber war are well advised to apply competitor analysis (Porter, 1980), adopted to information security by Gordon and Loeb (2001), and which may be adopted further to the competition or war between firms and external attackers. We consider