

# Quantifying the Value of IT Security Mechanisms and Setting Up an Effective Security Architecture

Huseyin Cavusoglu Srinivasan Raghunathan Birendra Mishra  
huseyin@utdallas.edu sraghu@utdallas.edu bmishra@utdallas.edu

School of Management  
The University of Texas at Dallas  
Richardson, TX 75083

## Abstract

Information technology (IT) security has emerged as an important issue in the last decade. Firms typically employ multiple security technologies, for example, firewalls as a preventive control and Intrusion Detection Systems (IDSs) as a detective control, to secure their IT systems. While security technologies have advanced rapidly, economic assessment of the Return on Security Investments (ROSI) has proven to be challenging. Assessing the value of these technologies is crucial to firms before they make investment decisions. Such assessments are also useful to security technology developers in focusing their design efforts on features that maximize their products' value. This paper describes an economic model for IT security management. Specifically, we consider a firm that can deploy a firewall and/or an IDS in addition to manual monitoring in its security architecture to minimize organizational loss. We (i) derive the value of a firewall and an IDS within a security architecture (ii) analyze the complementary and/or substitution effects between these technologies, and (iii) provide guidelines to firms on how to design an effective security architecture based on their risk environment and quality of available technologies. We analyze the problem from a strategic perspective using game theory. Our analysis reveals that the value of a firewall to a firm is positive if the cost of dropping authorized external users is smaller than a threshold value. The value of an IDS is positive only if it is a deterrent to hackers, i.e., it reduces hacking probability. Whether firewalls and IDSs complement or substitute each other depends critically on their qualities and the risk environment. For some firms, use of both these technologies is worse than using only of them. We supplement our analytical results with extensive numerical analysis. The results of the numerical analysis provide insights into whether a firm should use both firewall and IDS and the types of firewall and/or IDS it should use.