Chapter 9

Cost-Effectiveness of Security Measures: A Model-Based Framework

Wolter Pieters  
Delft University of Technology, The Netherlands & University of Twente, The Netherlands

Christian W. Probst  
Technical University of Denmark, Denmark

Zofia Lukszo  
Delft University of Technology, The Netherlands

Lorena Montoya  
University of Twente, The Netherlands

ABSTRACT

Recently, cyber security has become an important topic on the agenda of many organisations. It is already widely acknowledged that attacks do happen, and decision makers face the problem of how to respond. As it is almost impossible to secure a complex system completely, it is important to have an adequate estimate of the effectiveness of security measures when making investment decisions. Risk concepts are known in principle, but estimating the effectiveness of countermeasure proves to be difficult and cannot be achieved by qualitative approaches only. In this chapter, the authors consider the question of how to guarantee cost-effectiveness of security measures. They investigate the possibility of using existing frameworks and tools, the challenges in a security context as opposed to a safety context, and directions for future research.

DOI: 10.4018/978-1-4666-4983-5.ch009
INTRODUCTION

In the context of safety, it is well understood how to evaluate the effectiveness of measures that aim at reducing risk. For example, we can estimate how often a certain area will flood when we build a dike of a certain height. The estimation is based on our knowledge of the physical rules underlying the flooding (threat) and the dike (countermeasure) and their interactions. Especially for physical threats, there is abundant historical data that enables predicting their expected frequency and impact with good degrees of reliability.

In the context of security, the situation is far less clear. In this setting, attackers intentionally disrupt systems. This intention is hard to measure; attackers do not follow physical laws but have their own goals. Also, attackers may intentionally execute multiple interdependent steps to achieve their goal (Nunes Leal Franqueira, Lopes, & van Eck, 2009), increasing the likelihood of simultaneous failures of components or systems. While there is good knowledge of some of the threats and countermeasures, neither the underlying rules nor their interactions are as well understood as in the case of safety. As a result, even though organisations and society are increasingly concerned about the effects of malicious threats against critical infrastructures, it is unclear how to counter these threats in a cost-effective way.

Especially cyber threats are difficult to address, due to the increased connectivity of systems (Van Cleeft & Wieringa, 2009). In this area, several complex attacks have been observed recently. Examples include StuxNet, using infected USB sticks to sabotage nuclear plants (Langner, 2011), and the DigiNotar attack, using fake digital certificates to spy on website traffic (Leavitt, 2011). By now, organisations should be aware of the risk of being attacked in this way, and should ideally have access to adequate decision support to mitigate the associated risks. This requires a better understanding of the adequacy and cost-effectiveness of measures against cyber threats.

To illustrate the situation of decision makers, consider an organisation that has a set budget available to invest in security measures against malicious attacks. Investments are possible in fences, in firewalls, and in employee education. Which investment (or combination of investments) would be the most cost-effective one? In this chapter, we provide the basic concepts and open research questions that would provide the components needed for an answer.

The rest of this chapter is structured as follows. After introducing the relevant background in the next section, we discuss the proposed framework for cost-effectiveness of security measures in Section 3. This is followed by an outline of a future research agenda in Section 4, and conclusions in Section 5.

BACKGROUND

In this section we cover some of the background needed for performing the necessary analyses to evaluate the cost-effectiveness of security measures.

Safety Metrics

In principle, the risk concepts needed to evaluate the cost-effectiveness of security measures are readily available, e.g., in the risk taxonomy by The Open Group (2009). For both situations ‘with’ and ‘without’ a particular countermeasure in place, we can calculate the faced risk with respect to a certain threat by multiplying the Threat Event Frequency, the Vulnerability, and the Probable Loss Magnitude. The threat event frequency represents the number of occurrences of external events. The vulnerability represents the likelihood of a particular type of loss in the system due to a threat event. The probable loss magnitude represents the damage if such a threat event results in a loss. By multiplying the three