15 Economic Security Metrics

Rainer Böhme\textsuperscript{1} and Thomas Nowey\textsuperscript{2}

\textsuperscript{1} Technische Universität Dresden
\textsuperscript{2} University of Regensburg

This chapter surveys economic approaches for security metrics, among which we could identify two main areas of research. One has its roots in investment and decision theory and is mainly pursued in the field of information technology-oriented business administration. It has yielded a number of quantitative metrics that can be applied as guidelines in investment decisions as well as for the evaluation of existing security measures. The second area of research has ancestors in micro-economics. It deals with market concepts to gather security-relevant information and extract quantitative indicators on information security properties.

15.1 Metrics for Security Investments

The previous chapter has demonstrated that it is essential to measure organisations’ security at different levels of detail. This also applies to the investment perspective. In the recent years, organisations see an increasing demand for determining the cost and benefit of IT security investments. Possible reasons include compliance with regulatory requirements, emerging information security threats, or increased dependence of business processes on information technology. Apart from definitions for metrics, this section will show the motivations behind metrics as well as challenges in quantifying the value of IT security investments.

Basics

When assessing investments one can basically take two different perspectives. First, the ex ante perspective tries to assess the costs and benefits of possible future investments and helps to decide whether an investment project is profitable or not. Second there is the ex post perspective for the retrospective judgement of past investments. The first perspective can help to decide whether to invest in a certain security measure or not, or to choose the best alternative out of different possible security measures (“What measures should we implement?”). The second perspective should provide a target-performance comparison and answer the question if the firm’s resources were spent effectively (“Did we do the right things?”).

The overall goal of the investment perspective on IT security is to measure the influence of investments in IT security on a firm’s success and to determine the cost and benefits of different security solutions. Thus metrics for IT security investments should support both of the perspectives explained above. And they should also fulfill some additional requirements, such as allowing for comparisons between firms. It is reasonable to assume that the law of diminishing marginal returns holds true for IT security investments as well (see [189]). Thus from a cost-benefit-perspective there can be a “too
much” of IT security. So as Soo Hoo [456] put it the question to answer could also be “How much is enough?”.

One could assume that it is easy to adapt the metrics of classical investment theory to IT security. However there are some major differences between investments in IT security and ordinary investments. The first main difference between usual investment considerations and investments in IT security is, that it is hard to determine the economic utility of those investments. This lies in the nature of IT security measures. Investing in IT security processes or products usually will not provide direct returns in the sense of a measurable positive cash flow. Their main utility rather lies in reducing potential risks. Second, determing the cost of IT security can also be quite hard. Besides direct costs (e.g. installation, maintenance, training) there are also indirect costs (e.g. through changes in employee motivation or changed workflows).

It is widely accepted to regard IT security risks as operational risks. According to the Basel Committee, operational risk can be defined as “the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events” [40]. Thus, many recent standards and other publications apply risk management theory and techniques to IT security (see for example [460], [3], [173]). To understand the metrics presented below it is useful to know some basic taxonomies and concepts of IT security risk management. Nevertheless a broad introduction is beyond the scope of this book and can be found in literature (see above).

An important determinant in risk management is the so called risk exposure, which is formally the product of expected likelihood vs. expected severity of an unwanted event. Investments in IT security aim either at reducing the probability of occurrence or on reducing the potential loss from an unwanted event or both. Gordon and Loeb [190] have shown that information security managers regard those parameters as critical determinants in budgeting for information security. Hence most metrics for security investments survey how efficiently a certain security measure can change those parameters.

Metrics

The concept of annual loss expectancy (ALE) represents one of the building blocks of quantitative metrics for IT security. It has been used in risk management since the 1970s and was adapted for IT security risks in the FIPS publication #65 in 1979 by the National Bureau of Standards [367]. The ALE for a single type of security event can be computed as the product of single loss expectancy (SLE) and the annual rate of occurrence (ARO). SLE represents the expected financial consequences of an unwanted event, while ARO is equivalent to the number of occurrences of that type of event per year.

\[
ALE = SLE \times ARO
\]

(1)

ALE can also be an aggregation of the annual loss expectancies of several undesirable events (see [456]).

\[
ALE = \sum_{i=1}^{n} S(O_i) F_i
\]

(2)

where \(O_i\) is the harmful outcome \(i\), \(S(O_i)\) is the severity of outcome \(i\) (in monetary units) and \(F_i\) is frequency of occurrence of outcome \(i\).