# Chapter 86
# Corporate Information Security Investment Decisions:
## A Qualitative Data Analysis Approach

**Daniel Schatz**
*University of East London, London, UK*

**Rabih Bashroush**
*University of East London, London, UK*

## ABSTRACT

*This article describes how with information security steadily moving up on board room agendas, security programs are found to be under increasing scrutiny by practitioners. This level of attention by senior business leaders is new to many security professionals as their field has been of limited interest to non-executive directors so far. Currently, they have to regularly report on efficiency and value of their security capabilities whilst being measured against business priorities. Based on the Grounded Theory approach, the authors analysed the data gathered in a series of interviews with senior professionals in order to identify key factors in the context of information security investment decisions. The authors present detailed findings in context of a simplified framework that security practitioners can utilise for critical review or improvements of investment decisions in their own environments. Extensive details for each category as extracted through a qualitative data analysis are provided along with a category network analysis that highlights strong relationships within the framework.*

## 1. INTRODUCTION

Information asset security has been a subject of extensive research over the past years, largely focusing on technological risks. While there was early research on the economic impact of information security risks (Ekenberg, Oberoi, & Orci, 1995; Finne, 1997; Francke & Blind, 1996), academic research had been limited until the turn of the millennium when papers by Hoo (2000), Anderson (2001), as well as Gordon and Loeb (2002) raised levels of interest regarding this topic. However, studies remain fo-

DOI: 10.4018/978-1-7998-7705-9.ch086

cussed on the fast-moving area of information security risks in general. Much of the security economics research, particularly earlier approaches, is firmly footed in theoretical model space, leaving key challenges unmentioned or unsolved. Although such models are contributing towards a better approach for information security investments, they often suffer from their overly theoretical methodology and, as such, are not properly well suited for real-world application. The aim of this study is to identify current practices of information security investment prioritisation and evaluation in organisations. Based on a series of semi-structured interviews, a qualitative data analysis approach is followed so as to understand key factors, core challenges, and common practices as experienced by information security practitioners. In particular, this paper investigates the following research questions:

- How are information security investments in organisations currently approached by practitioners?
- What are the key factors and challenges considered by practitioners in relation to information security investments?
- How do information security management systems and information security governance models support practitioners in this regard?
- How are traditional accounting metrics (net present value (NPV), return on investment (ROI), etc.) used?

The remainder of the paper is structured as follows: in the next section, related work is presented. Section 3 discusses the research methodology and design, as well as the interview framework including sample strategy, data collection procedures, coding approach and analysis. Section 4 presents the results of the data analysis process including details on the responses of participants. And finally, in Sections 5 and 6, the limitations of the approach presented in this study are thoroughly reviewed and conclusive thoughts are provided.

## 2. RELATED WORK

At this point in time, there can be little doubt that cybercrime-related loss is a serious issue threatening the economic well-being of most organisations (Anderson et al., 2013; Armin, Thompson, & Kijewski, 2016; Hyman, 2013). As such, it is not surprising that organisations are either actively discussing how to deal with this situation or are already well underway taking action in form of information security risk management programs and aligned investments. In this context, Hoo (2000) quite rightly asked the difficult question as to how much is enough. As expected, there is no single right answer to this. Rather, Hoo stresses the need for quantitative computer security risk management to become more acute. Inevitably, the follow-up question will be how to sensibly allocate funds in order to maximise risk management benefits. Although this is still a relatively new field of research, there has been notable activity over the last two decades describing a wide range of options of how to approach the problem (Eisenga, Jones, & Rodriguez, 2012; Kesswani & Kumar, 2015; Neubauer & Hartl, 2009; Sawik, 2013; Schatz & Bashroush, 2016). Some solution approaches are more popular among researchers than others; Cavusoglu, Raghunathan, and Yue (2008) argue that investments in IT security should be managed differently from other investments which organisations conduct. Their research proposes a game theoretic approach that is illustrated to outperform an alternative decision-theory based approach. In their research, Bistarelli, Dall'Aglio, and Peretti (2007) discuss the use of defence trees to assess the effectiveness and economic