3 Part I: The Inhibiting Role of Unrealistic Optimism in Providers’ IT Security Risk Management

In this chapter, we present our empirical analysis of the role of the decision makers’ subjective ITSR perceptions in the Cloud providers’ IT security risk management. In particular, we demonstrate the inhibiting effects of unrealistic optimism (UO) in the ITSR perceptions of Cloud providers’ decision makers on the outcome of the providers’ IT security risk management. Therefore, we first show the theoretical background and the hypotheses development of this part (Section 3.1). In this section, we also show the development of the proposed theoretical model of Cloud providers’ IT security risk management. Afterwards, we show the research methodology of the empirical study (Section 3.2), including the proposed approaches to measure UO in the ITSR perceptions of providers’ decision makers. Then, we present the analyses of the collected data along with the results (Section 3.3). The findings of this part are summarized and discussed (Section 3.4).

3.1 Theoretical Background and Hypotheses Development

In this section, we describe the theoretical backgrounds and the development of the comprehensive framework of Cloud providers’ IT security risk management processes, which is based on an infusion of four distinct but related streams of literature and explicates the effects of the subjective risk and coping perceptions of the providers’ decision makers. First, we draw on organizational IT security risk management research (Subsection 3.1.1) and technology threat avoidance theory (Subsection 3.1.2) to theorize in which ways, and to what degree, the outcome of the providers’ IT security risk management processes are predicted by subjective perceptions of their decision makers. Second, based on institutional theory (Subsection 3.1.3), we hypothesize how the actions and demands of the providers’ stakeholders influence the IT security risk management decisions of the providers’ decision makers. Third, drawing on psychological risk perception research (Subsection 3.1.4), we postulate that there are two important perspectives on decision makers’ ITSR perceptions (i.e., absolute and comparative ITSR perceptions), which eventually determine the outcome of the organizational IT security risk management processes. Fourth, based on psychological literature, we introduce the phenomenon of unrealistic optimism (UO) (Subsection 3.1.5) and derive our main hypothesis regarding the existence and consequences of systematic errors in the decision makers’ ITSR assessments (see interlocking of theoretical underpinnings of the proposed theoretical model of Cloud providers’ IT security risk management in Figure 3-1).
3. Part I: The Inhibiting Role of Unrealistic Optimism in Providers’ IT Security Risk Management

3.1.1 Organizational IT Security Risk Management

In order to be able to relate to all processes of the providers’ IT security risk management and how they are determined by the decision makers’ perceptions, we built on Straub and Welke (1998)’s well-established model, that explicates the entire organizational IT security risk management process (see also IT security risk management in Subsection 2.3).

As shown in Figure 2-1, the normative model suggested by the authors, which is grounded in previous management science research and derives its structure from Simon (1960)’s model of decision-making, separates the organization IT security risk management process into five distinct stages and their outcomes: the identification of IT security threats, the ITSR analysis, the solution analysis, the decision, and the implementation phase. The IT security risk management process generally starts with the identification and formulation of threats concerning the risk of IT security breaches by the providers’ decision makers (e.g., a security loophole in the providers’ authentication systems was discovered). The central risk analysis phase is situated as a bridge between identified IT security threats and the assessment of available solutions, and preceding the decision phase. The analysis of the ITSR is inherent in the identified threat areas and includes the threat identification and prioritization of the risks resulting from