A Structural Model Approach for Assessing Information Security Value in Organizations

Daniel Schatz, University of East London, London, UK
Rabih Bashroush, University of East London, London, UK

ABSTRACT

Data is rapidly becoming one of the most important assets in global markets, and criminals are spotting opportunities to exploit new potential income sources. In response to this, organizations are dedicating increasing resources to information security programs. However, faced with unrelenting breach reports and rising costs, decision makers inevitably wonder which type of security investment is economically viable. In this article, the authors present an empirically tested model describing the underlying key constructs for assessing information security value in an organization. Based on identified latent variables previously put forward in the literature, the authors use a partial least squares structural equation modeling approach to verify the model’s soundness. They identify five crucial variables for value-focused information security investment. The relationships among these latent variables are then investigated and contributions of the structural model assessed. The key findings are finally presented to highlight opportunities for security practitioners to apply the proposed model.

INTRODUCTION

Data is rapidly becoming an important asset in global markets. It is no longer just a byproduct, but rather a driver of new and improved business models that generate high value. Hence, interest in this area is increasing rapidly—and not just for legitimate businesses (The Economist, 2017). Criminals are quick to spot opportunities and are adapting to these new value streams. Indeed, organized crime is embracing and exploiting billions of dollars of digital opportunities (Dethlefs, 2015; Hyman, 2013; Ponemon Institute, 2017). With losses at this magnitude and still rising, governments and regulators are playing an active role in encouraging businesses to protect their information assets (Pawlak & Wendling, 2013). This is not lost on senior executives and leads to security of organizations information assets being a common agenda point in most board rooms. As a result, security professionals are tasked with ensuring organizations are secure by addressing which assets should be protected, how they should be protected and how such protection adds value. However, although a substantial research body on information security risk management examines which assets to protect and how to protect them, research on the value of information security is scarce albeit rising (Anderson, 2001; Gordon, Loeb, & Zhou, 2016; Rue & Pfeffer, 2009) and the adoption of research findings by practitioners in the real world remains lacking. To improve the practical implementation of information security, we extend the body of knowledge by proposing an evidence-based model combining theoretical work with real-world experience. Recognizing that information security is an interdisciplinary field with requirements along several corporate dimensions (managerial, organizational, cultural, technical, financial), we follow an exploratory convergent mixed method research approach (Creswell, 2013) to
examine information security investment in this context. The background to this study is the research by Schatz and Bashroush (2017), who analyze interview data obtained from senior practitioners and identify a range of key aspects they consider when investing in information security. In the present work, we combine those findings and the results of a systematic literature review of the methods proposed in academic journals to create a new conceptual model. To verify the proposed model, we then analyze quantitative data gathered through a survey instrument designed using the structural equation modeling (SEM) method. This approach allows us to investigate several key questions such as is there an underlying structural model for information security investment, what are the significant components and relationships in the model and what are the indicators of the components and how are they measured?

RELATED WORK AND THEORETICAL FOUNDATION

Early discussion on information security was mostly driven by technical aspects (Hitchings, 1995; von Solms, 1996), but it quickly moved onto governance topics (Dhillon & Backhouse, 2000; Dutta & McCrohan, 2002; Shuchih Ernest & Chienta Bruce, 2006) as well as focusing on value (Bojanc & Jerman-Blažič, 2008; Dhillon & Torkzadeh, 2006). Work on the economic aspects of information security (Anderson, 2001; Gordon & Loeb, 2002a; Hoo, 2000) was rapidly extended upon by research investigating the allocation and optimization of security investment. For example, by taking into account the vulnerability of information and potential loss from a security breach, Gordon and Loeb (2002a) approach the topic as an optimal stopping problem and present a model to calculate optimal investment levels. Their model has been critically reviewed and extended by several researchers, including the original authors (Baryshnikov, 2012; Gordon et al., 2016; Matsuura, 2009; Willemson, 2010). Similarly, a return on investment (ROI) approach aligned with commonly used accounting principles was popular in the early days of research in this field (Al-Humaigani & Dunn, 2003; A. Davis, 2005; Mizzi, 2010; Sonnenreich, Albanese, & Stout, 2006). However, it also attracted criticism because of the ambiguity in the underlying data as well as general applicability of the metric to information security (Gordon & Loeb, 2002b; Wood & Parker, 2004). Indeed, the publication of research on this approach and other related accounting metrics such as net present value (NPV) has declined over time, as shown by the systematic literature review on this topic by Schatz and Bashroush (2016).

Cremonini (2005) improves on earlier approaches by introducing the concept of attacker returns. The author proposes coupling the ROI index with a corresponding return on attack (ROA) index that aims to measure attackers’ convenience (or inconvenience). The notion of ROA is also a key component of game theory-based models. Bistarelli, Dall’Aglio, and Peretti (2007) use the concept of defense trees as an extension of attack trees with countermeasures and economic quantitative indexes such as ROI and ROA to evaluate the effectiveness of investment. Cavusoglu, Raghunathan, and Yue (2008) argue that a game theoretic approach is suitable as attackers modify their strategy in response to security investment by the defender. They show that sequential as well as simultaneous games in some circumstances lead to a higher payoff for the defender compared with a decision theory-based approach. Fielder, Panousis, Malacaria, Hankin, and Smeraldi (2015) apply a hybrid game theoretic–optimization approach in the context of security spending, particularly by small and medium-sized enterprises. While they conclude that their approach works well in that context, they also highlight issues with optimal budget allocation caused by indirect costs. Carin, Cybenko, and Hughes (2008) combine several methods in their approach, using a Partially Observable Markov Decision Process for attack modeling. They find their methodology primarily suitable for approximating investment levels related to the protection of critical intellectual property in complex systems. H.-K. Kong, Kim, and Kim (2012) state that the financial focus on information security investment is inadequate and argue that any assessment should consider the multidimensionally of performance measures in an organization. In particular, their modeling approach shows that technological and human aspects in the context of
Group Verbal Decision Analysis
www.igi-global.com/chapter/group-verbal-decision-analysis/11281?camid=4v1a

Managing a Firm's Cash Flow Recovery Strategy
Aditya Vikram Rajkumar and Jeffrey Williams (2012). International Journal of Strategic Decision Sciences (pp. 60-80).
www.igi-global.com/article/managing-firm-cash-flow-recovery/63656?camid=4v1a