Contributing Factors of Information Security Investments in South East Asia SMBs: A Technology-Organisational-Environment Approach

Mathews Z. Nkhoma, Department of Business IT & Logistics, RMIT University Vietnam, Ho Chi Minh City, Vietnam
Duy P. T. Dang, Department of Business IT & Logistics, RMIT University Vietnam, Ho Chi Minh City, Vietnam

ABSTRACT

This research aims to determine the contributing factors of information security investment by developing a theory-based conceptual model using Partial Least Square techniques to analyze the data collected from 500 IT decision-makers in Vietnamese small and medium sized businesses. The findings from the conceptual model, which is based on Technology-Organization-Environment framework, suggests that the drivers of organizational intention to invest in information security include the organization’s internal information, size, perceived IT benefits and manager’s knowledge about information security. By understanding more about the contributing factors of information security investment, practitioners could focus on such factors to make rational investment decision and improve their defense against the emerging cyber-crimes. On the other hand, the authors also hope to fill in the existing gap of information security management research area in which there are few studies investigating the drivers of information security investments.

Keywords: Drivers, Information Security, Investment, Partial Least Square, Small and Medium Business, South East Asia

INTRODUCTION

During the recent years, we have been experiencing the rapid adoption of electronic commerce (eCommerce) that connects businesses and customers around the world. On one hand, prior and ongoing researches have been focusing on improving the effectiveness and efficiency of conducting transnational businesses with new strategies and devices. On the other hand, the important role of Information Security (InfoSec) in securing online transactions and digital assets is essential due to the increase of cybercrimes. Indeed, the latest surveys by Symantec and...
Computer Security Institute (CSI) reveal the increasing number of cyber-threats that aim at organisations of all sizes and industries. The sophisticated attacks have damaged businesses profits directly as shown by the global average loss of $3.44 million in 2009 (Ponemon, 2010) and $5.5 million by data breach in U.S. alone in 2011 (Symantec, 2012). In addition, Canalys announces that global enterprises security investment is expected to reach a market value of $22.9 billion worldwide in 2012 (Alto, 2012). While it is outside of the scope to discuss the effectiveness of such huge investments, these figures raise questions about how small and medium businesses (SMBs) – with their limited budget and lack of experience in InfoSec management – can ensure adequate protection for their information assets while spending efficiently?

Prior and ongoing studies have been dedicated to evaluate optimum strategies to justify InfoSec investments through the development of InfoSec investment model and theories. Nonetheless, little effort was spent to investigate the drivers that influence managerial intention to invest in InfoSec initiatives. Managers may estimate how much budget they should allocate for InfoSec development using the well-known Gordon-Loeb model or prioritise budget for InfoSec options with ROSI formula; but the question of when it is necessary, and why, to spend on data protection remains unverified. By determining the drivers that encourage managers to invest in InfoSec initiatives, such factors can be used as metrics to indicate when is the best time to make precise strategic investments as well as how to make sound proposals of InfoSec initiatives that align well with business goals.

This research investigates the drivers of InfoSec investments in the perspectives of SMBs’ InfoSec decision-makers working in Vietnam, an emerging market in South East Asia. The aforementioned works have briefly summarised the purposes and main content of this work, the rest of the paper is in the following order. Firstly, the second section provides our literature review including the position of (1) InfoSec investment in SMBs and (2) this research with respect to prior studies forming the body of knowledge. The third section presents the conceptual and theoretical backgrounds that justify our conceptual model and methodology. The fourth section provides the details of our data analyses. The fifth section elaborates and discusses the research findings. The sixth section discloses the research project with its limitations and suggests future research directions.

BACKGROUND

Information Security’s Essential Roles in Today’s Business

It has been widely discussed that the essential role of Information Security (InfoSec) is continuously growing with the increasing cyber-threats, especially when businesses tend to be more dependent on the rapid changing technologies. Traditionally, organisations need to react fast to technological changes and constantly develop business models to meet customers’ new demands and gain market shares. Nevertheless, InfoSec has always been posing as a major concern of businesses’ intention to adopt new technologies. The latest IBM Tech Trend report reveals that today’s organisations are most concerned about InfoSec as the main barrier preventing them to implement the emerging technologies (IBM Center for Applied Insights, 2012). Similarly, Ernst and Young’s report (2012) also warns about the security gaps caused by the rapid technological developments. We elaborate the barrier role of InfoSec by examining one of the latest technologies introduced in early 2007 i.e. cloud computing. Indeed, a large amount of literature about cloud adoption’s barriers share common view on the central issues of data’s confidentiality, availability and integrity of firms when they have to entrust their data to the 3rd parties (Motta, Sfondrini, & Sacco, 2012; Sengupta, Kaulgud, & Sharma, 2011). While it appears that cloud vendors take much responsibility in securing their clients’ data, adopters also have to provide adequate training and policy to ensure InfoSec behaviour among their employees. Without
Digital Rights Management for E-Content and E-Technologies
[www.igi-global.com/chapter/digital-rights-management-content-technologies/23114?camid=4v1a](www.igi-global.com/chapter/digital-rights-management-content-technologies/23114?camid=4v1a)

Three Models to Measure Information Security Compliance
[www.igi-global.com/article/three-models-measure-information-security/40360?camid=4v1a](www.igi-global.com/article/three-models-measure-information-security/40360?camid=4v1a)