Chapter 14
IT Security Investment Decision by New Zealand Owner-Managers

Radiah Othman
https://orcid.org/0000-0002-9772-0439
School of Accountancy, Massey University, New Zealand

Sydney Kanda
7 Eyes Cyber Security Consultants, New Zealand

ABSTRACT

Small businesses employ 29% of New Zealand's private sector workforce and account for more than a quarter of its gross domestic product. Thus, a large-scale attack on small businesses could prove to be catastrophic to the economy. This chapter, which is framed by the protection motivation theory, explores 80 small business owners' IT security decision-making via an online survey. The findings revealed that 21% of small businesses were affected by ransomware. Fifty-one percent of the respondents did not have any anti-malware and none of the respondents used data classification, which means all information was regarded as the same. Since they managed to recover their backup information, they did not perceive the threat of ransomware as imminent. In terms of coping appraisal, it is assumed that if the business owner-managers believe that the capability of IT security investment averts threats in their organizations, they will be more inclined to develop an intention to invest in it.

INTRODUCTION

There is an abundance of studies on investment decision-making practices focusing on management accounting (MA) techniques and tools. In terms of investment decision-making behavior, previous research has largely focused on shareholders (e.g., Agyemang, 2019) rather than business owners, especially small-medium enterprises (SME). Lucas, Prowle, and Lowth (2013) surveyed SME business owners and indicated that less successful SMEs often did not use MA tecnhiques adequately. Research

DOI: 10.4018/978-1-7998-3149-5.ch014

has yet to cover New Zealand SME in this regard. With the exception of sustainability practices (Collins, Lawrence, Pavlovich, & Ryan 2007), MA research on SME in New Zealand is limited. In fact, little is known of the risk tolerance and uncertainty management behaviors associated with New Zealand (NZ) SME business decision-making and activities (Islam, Tedford, & Haemmerle, 2017).

Small businesses make the bulk of the business community in New Zealand. Currently, 97% of enterprises in New Zealand have fewer than 20 employees and are regarded as small enterprises (MBIE, 2015). Smaller businesses have higher failure costs, both at firm and personal levels (Islam et al., 2017). However, SMEs in New Zealand growth and development are influenced by attitudes of owner-managers (Islam et al., 2017; Lewis, 2008). Since they are constantly exposed to threats imposed by using information technology (IT) in their operation, the IT security investment they make could be critical to their survival. Collectively, they employ 29% of New Zealand's private sector workforce and account for more than a quarter of gross domestic product (NZentrepreneur, 2017). Thus, an attack on small business on a large scale could also be catastrophic to the economy. In addition, previous research on MA and IT security was conducted in isolation, focusing on ransomware threats. Thus, this study intends to address the knowledge gap by exploring New Zealand's small business owners' consideration of MA information in their IT security decision-making.

The main contribution of this chapter is twofold. First, the chapter extends studies on small businesses into MA decision-making studies and IT security literature framed by Protection Motivation Theory (PMT) (Menard, Bott, & Crossler, 2017; Rogers, 1983) from psychology. Second, it provides relevant insights on the current state of management accounting consideration in owner-managers' investment decisions. In terms of practical managerial significance, this study provides insight on the challenges and dilemmas faced by owner-managers in balancing the cost of investment required and the need to protect their businesses against security threats. Intuitively, it encourages managers to view IT security as a strategic resource rather than an outflow expenditure from their budget.

The conceptual framework proposed in this chapter aims to assist managers in redesigning IT strategy based on their assessment of vulnerability-threat analysis and realign them with required cyber essentials. This includes the flexibility to modify IT security policies, schedule periodic employee training, and to have an ongoing security audit. It will make managers more prepared to deal with constant and ever-evolving IT security threats and challenges.

The next section focuses on the background of ransomware threats and their impacts on New Zealand small businesses. The theoretical background is explained and then followed by research method and research findings. Then a conceptual framework of MA-driven IT security decision is proposed before the chapter concludes.

RELATED LITERATURE

Most businesses rely on computers and IT to the extent that it would be impossible to manage without them. Increasing investment in technological advances is necessary to increase presence, speed in responding to customers' needs, and leverage on competition in the targeted market. Information has become so prolific that companies have had to change their business models and processes to become more open by introducing multiple touch points for stakeholders and customers wanting to interact with them (Kwok, 2015). This also presents abundant opportunities for unauthorized access and data breaches (Watad, Washah, & Perez, 2018).