Organizational Characteristics and Their Influence on Information Security in Trinidad and Tobago

Kyle Papin-Ramcharan
University of the West Indies, Trinidad and Tobago

Simon Fraser
University of the West Indies, Trinidad and Tobago

INTRODUCTION

This study explores the issue of information security in the developing world using the experiences of Trinidad and Tobago. The digital divide is closing with regards to access to technology and reliance on information systems is now commonplace (Pasternack, 2010). However, developed and developing countries differ significantly in technological prowess and education. These differences may be responsible for different attitudes towards the protection of information assets.

Information security is regarded as a major contributing factor to business survivability (Sung, 2006; Torres et al., 2006). A study by Kim and Lee (2005) highlighted that organizations which adequately invested in information security enjoy benefits such as added profitability, enhanced decision making, and enhanced relationships with suppliers and customers.

Although the importance of information security is clear, there are still organizations which underperform in information security management. Research has shown that poor information security management practices exist within many organizations. For example, recent research by Symantec reveals that only 27 per cent of IT professionals surveyed reported that their organizations have security procedures and policies for the burgeoning field of cloud computing (Lau, 2010).

BACKGROUND

According to the United Nations (2011), Trinidad and Tobago is classified as a "Small Island Developing State." Nevertheless, the country has built a reputation of being the industrial capital of the Caribbean based on its energy, banking, insurance and retail sectors.

Information security is critical to local organizations. Supervisory Control and Data Acquisition (SCADA) systems are used extensively by firms in the energy and utilities sectors. However, the increasing interconnectivity of SCADA systems has exposed them to a wide range of security exploits (Dumont, 2010; Sovacool, 2011). The Stuxnet worm attacks on Iran in late 2010 exemplified the weaknesses of SCADA. (Dareini, 2011).

Other sectors are also reliant on information systems. Local financial players and retailers are all highly automated and the government is also increasing its reliance on IT.

Apart from studies done by Xu and Bowrin (2005), Thorpe (2005) and Duncan and Duggan (2008) information security remains a relatively under-researched field in the Caribbean context. These studies have also highlighted the unique information security challenges of organizations in small developing countries such as resource challenges in the case of banks which struggle "to provide information security at a level commensurate with the other banks" (Xu & Bowrin, 2005), to deploy a robust security architecture (Thorpe, 2005) and also to combat cybercrime (Duncan & Duggan, 2008). This study aims to add to the reservoir of local knowledge and in this endeavour we will use the information security model developed by Chang and Wang (2010).

DOI: 10.4018/978-1-4666-5888-2.ch428

LITERATURE REVIEW

Peltier (2005) states that information security "encompasses the use of physical and logical data access controls to ensure the proper use of data and to prohibit unauthorized or accidental modification, destruction, disclosure, or loss of access."

Information security rests on the concepts of confidentiality, integrity and availability. Wang (2005) posits that confidentiality, integrity, and availability are "the most important properties for information systems in terms of security" and Bishop (2003) stated that "computer security rests on confidentiality, integrity and availability."

Protecting confidentiality is based mainly on defining and enforcing appropriate access levels and permissions for information, i.e. ensuring that those who are supposed to have access to information do, and those who are not supposed to have access, do not. Confidentiality is essentially protecting information from unauthorized access (Schultz et al., 2001).

The goal of information integrity is to protect information from unauthorized modification. According to Lee et al. (2004), information integrity refers to the "extent that information remains consistent and compatible with its original state after being stored and/or transmitted." Schou (1996) defines integrity as the "condition that exists when data is unchanged from its source and has not been accidentally or maliciously modified, altered or destroyed."

Availability is the "timely, reliable access to data and information services for authorized users" (Schou, 1996). The objective of availability is to "enable access to authorized information or resources" (CEC, 1991).

Organization Size and Information Security

According to Blakely (2002), SMEs typically suffer from small IT staff with no security training, a lack of formal security policies, minimal investments in security technologies and a lack of either business continuity or disaster plans. Kardel (2004) also cites a belief among SMEs' management that they will not be targets of hackers or cyber terrorists.

Research by Heikkila (2009) shows that larger organizations performed vulnerability assessments more regularly, typically have more written information security policies and revise these policies more often.

These considerations lead to the following hypotheses:

H1: Organization size positively affects the extent of organizational information confidentiality.
H2: Organization size positively affects the extent of organizational information integrity.
H3: Organization size positively affects the extent of organizational information availability.

Organization Type

The use of information systems tends to vary across industries (King, 1994; Reich & Benbasat, 1990). According to Jarvenpaa and Ives (1990), information systems play a "more strategic and critical role" in financial institutions.

Consequently, information security needs vary by industry. The basis of this variance is the concept of data criticality and degree of dependence on information systems. A study by Kankanhalli et al. (2006) shows that financial organizations utilize more resources towards deterrents than organizations in other sectors. Kearns and Lederer (2004) also found significant differences between industry types and business dependence on IT, resulting in a different intensity of information security practices.

These considerations lead to the following hypotheses:

H4: Organization type positively affects the extent of organizational information confidentiality.
H5: Organization type positively affects the extent of organizational information integrity.
H6: Organization type positively affects the extent of organizational information availability.

Relationship Resources

Relationship resources refer to the "spirit of partnership" that the IT department of the firm has developed and maintained with its internal and external clients (Ross et al., 1996; Byrd & Turner, 2000). Internal and external relationship resources build mutual trust, foster collaboration and information exchange on information security within the organization's departments and