Chapter 104
Socio-Technical Determinants of Information Security Perceptions in US Local Governments

Eunjung Shin
Science and Technology Policy Institute, South Korea

Eric W. Welch
Arizona State University, USA

ABSTRACT

Concerns about electronic information security in government have increased alongside increased use of online media. However, to date, few studies have examined the social mechanisms influencing electronic information security. This article applies a socio-technical framework to model how technical, organizational and environmental complexities limit electronic information security perceived by local government managers. Furthermore, it examines to what extent organizational design buffers security risks. Using data from a 2010 national survey of local government managers, this article empirically tests the proposed model in the context of U.S. local government's online media use. Findings show that, in addition to technical complexity, organizational and environmental complexities are negatively associated with local managers' awareness of and confidence in electronic information security. On the other hand, internal security policy and decentralized decision-making appear to buffer security risks and enhance perceived information security.

INTRODUCTION

Governments at all levels have sought to consistently improve online resources for citizens and other stakeholders. As the quantity and quality of information stored and disseminated have increased, so too have concerns that government information security safeguards have failed to keep pace (Dawes, 2008; Moyle & Kelley, 2012). The need to address these concerns intensifies as new technologies such

DOI: 10.4018/978-1-5225-9860-2.ch104

as interactive social media and cloud computing become more widely used for government services (Paquette, Jaeger, & Wilson, 2010). Although new information and communication technologies are being implemented by government, it is unclear whether governments are ready to deal with emerging electronic information security issues that accompany this new technology (White, 2012).

Just as government's power and authority enables it to collect and store private information, government is also accountable to the public for ensuring citizen privacy. Breakdown of this social contract is likely to further reduce levels of public trust in government (Blanchard, Hinnant, & Wong, 1998). Even in a practical sense, information security is essential for improving the performance of electronic government (Reddick, 2009; Shea, 2014). Several articles have called for an improved understanding of electronic information security in the public sector, particularly in local and state governments (Hof & Reichstädter, 2004; Kaliontzoglou, Sklavos, Karantjias, & Polemi, 2005; White, 2012; Williams, Hardy, & Holgate, 2013; Zhao & Zhao, 2010).

In response, this paper investigates electronic information security of US local governments. Information security, in general, refers to the status of information and information systems protected from unauthorized access, use, misuse and disclosure (Hof, 2003; McCumber, 1991; Smith & Jamieson, 2006). Provision of information security comprises two tasks: (1) protecting information from unauthorized users, and (2) making information trust-worthy and readily available for authorized users. When local governments use online media for public services, they are required not only to protect government information from unauthorized access but also to provide timely, trust-worthy information to citizens and stakeholders through an appropriate authorization process. Inevitably, there exist managerial tensions between the practices of data protection and data provision. Information security entails vigilant decision-making on when and how to provide data and to the extent to which online systems are open to the public. Hence, information security is a contextual and organizational outcome rather than the result of a static technical system (Dhillon & Backhouse, 2001; Huang, Rau, & Salvendy, 2010).

This paper examines electronic information security using subjective measures of perceived security. That is because subjective aspects of information security, such as security awareness, security compliance, and confidence in information security, effectively describe malleable nature of organizational information security and predict user-related security outcomes (Chan, Woon, & Kankanhalli, 2005; Huang, et al., 2010; Siponen, 2000). Chang and Ho (2006) point out that employees' negligence is a major challenge to electronic information security, despite the fact that external threats to electronic information security, such as cyber-crime, are more widely recognized to threaten information security. Organizational members' unawareness and ignorance of security issues may fundamentally diminish the preventive and deterrent effects of security systems. At the same time, employees' confidence in information security can influence their security practices (Rhee, Kim, & Ryu, 2009). Rhee et al. (2009) show that those who are confident in handling security threats tend to make self-regulatory efforts. On the other hand, when local government managers are not confident in organizational electronic information security, they may be reluctant to release government information through an organizational online platform. Therefore, subjective indicators, such as employees' awareness of security risks and confidence in information security, can inform us to what extent local governments keep information secure in practice. Recognizing that security perceptions play a key role in electronic information security, this paper specifically focuses on two subjective measures of perceived security: manager awareness of accidental electronic information disclosure and manager confidence in electronic information security.

This paper asks: What underlying factors might influence perceived electronic information security of an organization? Previous literature identifies that perceived information security and internal vulner-