Chapter 17
The Development of a Model for Information Systems Security Success

Kimberley D. Dunkerley
Nova Southeastern University, USA

Gurvirender Tejay
Nova Southeastern University, USA

ABSTRACT
Information security has received a great deal of attention from a number of researchers. However, there has been little research aimed at understanding the dimensions critical for the success of organizational information security programs. This chapter considers a large body of information security literature and organizes the research based on their findings. This taxonomy is used to develop a parsimonious model for information security success within organizations. Also, the utility of the proposed model within the contexts of government and healthcare is considered.

INTRODUCTION
Modern society has become reliant on information systems (IS) and the information assets they process and store. This reliance is quite impressive when presented with the facts: IS power much of the modern infrastructure, including such vital assets as telecommunications, power production and distribution, oil and gas distribution, and water purification and distribution. While the IS assets are themselves valuable, the value of the information assets they process and store must also be considered. Research has shown the greatest damage often offered by a breach of IS security to be the loss of information resources and their resultant strategic advantages (CSIS, 2009; Pisello, 2004).

Even while organizations are beginning to fully realize the value of their IS and information assets, IS security incidents do occur, and with
potentially significant losses. These losses are of both a monetary nature, as well as compromises to information assets. While it can be difficult to determine the full extent of losses suffered through IS security exploits (Cavusoglu, Mishra, & Raghunathan, 2004; CSIS, 2008; Gaudin, 2007), threats certainly have been realized at the corporate, state, and federal levels. The 2008 CSI Computer Crime and Security Survey found an average annual loss to corporate entities reported at $300,000 USD, with the potential to rise sharply depending on the type and scope of the incident (CSI, 2008). The sheer losses borne by organizations fundamentally underline the problems that face corporate entities and nation-states as their infrastructures become increasingly technological and enemies become increasingly sophisticated in their attack techniques.

To combat threats to their IS and information assets, a number of prescriptive IS security programs with varying content (e.g., U.S. department of defense information assurance certification and accreditation process (DIACAP), international organization for standardization (ISO)/international electrotechnical commission (IEC) 27000 series, national institute of standards and technology (NIST) SP 800-53) have been developed. These programs differ widely in their content and context, but they have one common aim: securing IS and their concomitant information assets. However, even after the implementation of one or more IS security programs, there is no assurance that IS and information assets are secure. Arguably, in order to properly address the known and unknown threats towards an organization, a thorough understanding of the factors constituting a successful IS security program is essential. Without this understanding, it could prove difficult for organizations to accurately state the benefits the IS security program provides (DeLone & McLean, 2003; Gable, Sedera, & Chan, 2008) as well as ensure optimal resource utilization for future efforts (Zviran & Haga, 1999).

In order to effectively contribute towards this greater understanding, this chapter will detail the seminal works within IS success and discuss how they can be extended towards the IS security domain to create a model for IS security success within organizations. For this purpose, the key research themes within the IS security domain will be presented within the context of those theoretical foundations. Because we have chosen to adopt the model development approach used to develop seminal IS success models, our strategy differs from the approach used to develop alternative models of IS security success such as Kankanhalii, Teo, Tan, and Wei (2003). The review of IS security literature was conducted as outlined by Webster and Watson (2002). Selected papers (no time period constraint) from the IS field were discovered using keywords. Those reference lists were then also examined to expand the reviewed research.

IS SUCCESS MODELS

The following section introduces three models influential to the development of the IS security success model: Shannon and Weaver (1949), Mason (1978), and DeLone and McLean (1992). DeLone and McLean (1992) is a seminal work in IS success (Elleithy, 2008), and itself builds upon the works of Shannon and Weaver (1949) and Mason (1978). Understanding the evolution of these models and the lessons learned along the way is important for the development of an effective and efficient IS security success model.

Shannon and Weaver (1949)

Shannon and Weaver (1949) developed a model that identified three constructs involved in effective communications. The Shannon and Weaver model is considered a seminal model for understanding communication and a seed for communication studies (Fiske, 1982) as well as