

Chapter 16

Project Commitment in the Context of Information Security

Ioannis Koskosas

University of Western Macedonia, Greece

Nikolaos Sariannidis

Technological Education Institute of Western Macedonia, Greece

ABSTRACT

This research investigates the role of project commitment in the context of information systems security. In doing so, the research adopts a psychological point of view by exploring and discussing the concept of project commitment in setting information security goals. Information security can be viewed as the efficient control of uncertainty arising from malicious acts intended to exploit valuable assets, and in the context of information systems the valuable assets under consideration are data. Data were collected by using an interpretive approach through in-depth interviews and observation within a single case study in Greece. The contribution of this research to interpretive information-systems consists of the study of project commitment and goal theory in an information security-management context, and its grounding within an interpretive epistemology. Ultimately, this research promotes an interdisciplinary and interorganizational theory that fosters a dialogue transcending industry-specific contexts and explores different management practices that can improve security project commitment and management in its real life context.

INTRODUCTION

As the society and its economic patterns have evolved from the heavy-industrial era to that of information, in terms of providing new products and services to satisfy people's needs, organizational strategies have changed too. In effect, corporations have altered their organizational and managerial structures as well as work patterns in order to leverage technology to its greatest advantage. Economic and technology phenomena such as downsizing, outsourcing, distributed architecture, client/server and e-banking, all include the goal of making organizations leaner and more efficient. However, information systems are deeply exposed to security threats as organizations push their technological resources to the limit in order to meet organizational needs (Dhillon, 2001; Dhillon & Torkzadeh, 2006).

A number of major studies conducted, including the Ernst and Young survey (2008), the Quocirca survey (2009), and the Computer Weekly survey (2009), indicated that security threats continue to rise. While security attacks are either internal or external, 66% of computer attacks in Greece come from employees within organizations (Souris et al., 2004). To this end, the success of information security appears to depend, in part, upon the effective behavior and understanding of the individuals involved in its use. Constructive behavior by employees and system administrators can improve the effectiveness of information security.

The present research takes a psychological-behavioral point of view by focusing on organizational commitment to information systems security projects in the context of goal setting within a financial institution in Greece. In doing so, this research examines the extent and impact to which specific information security behaviors are related to security project commitment through goal setting. The main research assumption is that information security project commitment would

relate positively to the enactment of information security behaviors such as understanding security project goals as well as communicating information security messages that ultimately have an effect on the organizations' overall business objectives. Hence, information security should support the mission of the organizations, it must be cost effective and must be in sync with employees' information security understanding seamlessly, that is integrate technology, processes and people through efficient project commitment.

In the next section, a brief organizational security background is given. Then, the theoretical framework of goal setting theory and project commitment is presented and the research methodology used for the purpose of this research is introduced. An analysis of the results is presented and the research findings and some conclusions are discussed.

BRIEF ORGANIZATIONAL INFORMATION SECURITY BACKGROUND

Although a number of IS security approaches have been developed over the years that reactively minimize security threats such as checklists, risk analysis and evaluation methods, there is a need to establish mechanisms to proactively manage IS security. That said, academics' and practitioners' interest has turned on social and organizational factors that may have an influence on IS security development and management. For example, Orlikowski and Gash (1994) have emphasized the importance of understanding the assumptions and values of different stakeholders to successful IS implementation. Such values have also been considered important in organizational change (Simpson & Wilson, 1999), in security planning (Straub & Welke, 1998) and in identifying the values of internet commerce to customers (Keeney, 1999).

12 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/project-commitment-context-information-security/73238

Related Content

Information Modeling in the Internet Age - Challenges, Issues and Research Directions

Keng Siau and Matti Rossi (2001). *Information Modeling in the New Millennium* (pp. 1-8).

www.irma-international.org/chapter/information-modeling-internet-age-challenges/22979

A Technology Commitment Model of Post-Adoption Behavior

Y. Ken Wang and Pratim Datta (2009). *Information Resources Management Journal* (pp. 1-22).

www.irma-international.org/article/technology-commitment-model-post-adoption/37206

The Auxiliary Function and Realization Mechanism of Artificial Intelligence in Cross-Cultural Traditional Music Education

Ningjing Li and Di Wu (2025). *Journal of Cases on Information Technology* (pp. 1-18).

www.irma-international.org/article/the-auxiliary-function-and-realization-mechanism-of-artificial-intelligence-in-cross-cultural-traditional-music-education/388947

Integrating Requirements Engineering Techniques and Formal Methods

María Virginia Mauco and Daniel Riesco (2005). *Encyclopedia of Information Science and Technology, First Edition* (pp. 1555-1559).

www.irma-international.org/chapter/integrating-requirements-engineering-techniques-formal/14473

Best Practices for Effective Virtual Teams

D. Sandy Staples, Ian K. Wong and Ann Frances Cameron (2005). *Encyclopedia of Information Science and Technology, First Edition* (pp. 260-265).

www.irma-international.org/chapter/best-practices-effective-virtual-teams/14247