1-1-2017

Partly Cloudy, Scattered Clients: Cloud Implementation in the Federal Government

Elston Steele
Trident University International

Indira Guzman
Trident University International

James Gaskin
Brigham Young University

Monica Adya
Marquette University, monica.adya@marquette.edu

Partly Cloudy, Scattered Clients: Cloud Implementation in the Federal Government

Emergent Research Forum

Elston H. Steele
Trident University
elston.steele@my.trident.edu

Indira R. Guzman
Trident University
Indira.guzman@trident.edu

James Gaskin
Brigham Young University
james.gaskin@byu.edu

Monica Adya
Marquette University
monica.adya@marquette.edu

Abstract

While cloud computing adoption is on the rise, barriers continue to play a critical role in delaying the progress of some cloud computing adoption efforts. In 2010 the United States federal government launched the 'Cloud First' policy which requires government agencies to consider the adoption of cloud computing when the solution is secure, reliable and cost effective (Kundra, 2010). Unfortunately, cloud computing adoption among federal agencies has been sluggish. This study investigates pressures asserted to facilitate cloud computing adoption. Although a vast amount of literature exists, very few studies empirically investigate cloud computing adoption from an institutional perspective in concert with top management support. This study aims to fill the gap where the literature is lacking concerning the adoption of cloud computing by federal agencies.

Keywords

Information Security Awareness; Top Management; Institutional Theory

Introduction

Since issuance of a federal mandate in 2010 requiring federal government agencies to immediately shift to a "Cloud First" policy, agencies have struggled to adopt cloud computing. The emergence of cloud computing as a new paradigm for achieving operational efficiencies has been obfuscated by several problems inhibiting rapid adoption of cloud computing. The Department of Homeland Security (DHS) is one those federal organizations having difficulty with cloud computing adoption. Previous research has examined hindrances to cloud computing adoption across industries in the private sector (Raza et al., 2015, and Park and Ryoo, 2012). While this research provides important insights on cloud computing adoption in the private sector, it devotes scant attention to challenges of cloud computing adoption in the federal government. This study seeks to fill this gap by examining the roles of Top Management Support and Information Security Awareness on cloud computing implementation success in the federal government. This research will provide a distinctive theoretical contribution to institutional theory by advancing our understanding of the process by which moderating factors impacts cloud implementation success. In addition to contributing to the Top Management literature, this research advances knowledge in the cloud computing literature by being the first to provide empirical evidence in examining federal organizations. Finally, this research contributes to future research on why agencies choose specific cloud service implementations.

Theoretical Framework

Institutional theory forms the foundation for this research. It has been applied in the field of information systems by several researchers (Zheng et al., 2013, Basaglia et al., 2008, and Liang et al., 2007). Scott (1987) suggests that the beginning of wisdom is to recognize that institutional theory has evolved over time and its concepts of institution and institutionalization have been defined in a variety of ways. Lawrence and Shadnam (2008) defines institutional theory as a theoretical framework for analyzing social phenomena which views the social world as significantly comprised of institutions – rules, practices, and structures that set conditions on action. A new concept of institutional theory, neo-institutional theory, emerged with the seminal works of Meyer and Rowan (1977) and DiMaggio and Powell (1983). Meyer and Rowan (1977) argued that formal structures (institutional myths) in organizations were ceremoniously accepted by actors as a means of attaining legitimacy in the institutional environment. Although formal structures secured legitimacy, stability, and survival, they reduced organizational efficiency in the technical environment, which led to decoupling the formal structures from the technical activities. DiMaggio and Powell (1983) argued that organizations become homogenous through isomorphic processes. A central tenet of neo-institutional theory asserts that organizations and organizational actors seek to gain legitimacy through the process of homogeneity to ensure their survivability (DiMaggio and Powell, 1983). Homogeneity in organizational fields occurs as the result of institutional isomorphic changes within organizational environments. DiMaggio and Powell (1983) introduce isomorphism mechanisms as a compelling means to influence an organizational actor to resemble another organizational actor subjected to the same environmental circumstances. Thus, the following hypotheses are presented:

H1: Coercive pressures will have a positive association with cloud implementation success.

H2: Normative pressures will have a positive association with cloud implementation success.

H3: Mimetic pressures will have a positive association with cloud implementation success.

Top Management Support

Institutional theory has been supplemented with other theories to complement institutional theory by compensating for its scarcity in specifically explaining how subordinate organizations decide which actions to take to respond to external pressures (Zheng et al., 2013 and Jensen et al., 2009). This study uses Top Management Support to compliment institutional theory as it explains how key leaders use its resources in response to institutional pressures. Drawing on the work of Lin (2010) this study operationalizes top management support as the degree to which top management understands the importance of cloud computing adoption and the extent to which top management is involved in cloud computing adoption. The involvement and participation of top management, such as the CEO and CIO, in managing IT and committing resources to cloud services illustrates the degree of importance placed on cloud computing (Jarvenpaa and Ives, 1991). Zheng et al. (2013) found that top management had positive and significant ($p < 0.001$) influence on the allocation of IT human resources and financial resources which lead to the intention to adopt technology. Top management participation has been found to have significant influence on assimilation of technology within an organization. Liang et al. (2007) confirmed top management participation to positively affect the degree of technology usage ($p < 0.05$). Not only must top management champion support for cloud computing, but they must ensure training and education is available for deploying cloud strategies and manage expectations for cloud adoption.

H4a: Top management support will positively influence the relationship between coercive pressures and cloud implementation success.

H4b: Top management support will positively influence the relationship between normative pressures and cloud implementation success.

H4c: Top management support will positively influence the relationship between mimetic pressures and cloud implementation success.

Information Security Awareness

Concerns for security in the cloud environment have been discussed thoroughly in the literature (Modi et al., 2013, Ogigau-Neamtiu, 2012, and Cebula and Young, 2010). Rubóczki and Rajnai (2015) suggest the complex issue of cloud security requires a solid understanding of cloud solutions for various security domains and expert understanding of compliance and risk management. Securing the cloud computing environment is a complex and challenging endeavor due to a lack of understanding of the source of security risks associated with the cloud environment. Modi et al. (2013) survey security issues in the cloud at various levels and propose that since cloud computing is a merger of several known technologies; inherent in those existing technologies are vulnerabilities, which facilitate risks in the cloud computing environment. Since each level of the cloud computing environment has security vulnerabilities, understanding responsibilities of actors involved in securing the environment is necessary. Ogigau-Neamtiu, (2012) assesses the cloud computing environment and divides responsibility between the cloud provider and the client based on the service deployment model. Understanding the cloud provider/client responsibilities for each service deployment creates information security awareness. IS awareness has been found to modify the behavior of individuals thereby fostering a secure environment. In their investigation of antecedents of information security policy compliance, Bulgurcu and Cavusoglu (2010) found that information security awareness (ISA) significantly influenced employees' compliance with security policies. Information security awareness has been found to significantly influence compliance behavior among employees of information security policies (Humaidi and Balakrishnan, 2015). Humaidi and Balakrishnan (2015) found that severity awareness and benefit of security-countermeasure effectively influenced compliance behavior.

H5a: Information security awareness will positively influence the relationship between coercive pressures and cloud implementation success.

H5b: Information security awareness will positively influence the relationship between normative pressures and cloud implementation success.

H5c: Information security awareness will positively influence the relationship between mimetic pressures and cloud implementation success.

Conceptual Model

Drawing on DiMaggio and Powell (1983) Neo-Institutional Theory, the conceptual model for this study explores the effects of Top Management and Information Security Awareness on cloud implementation success from a federal government perspective.

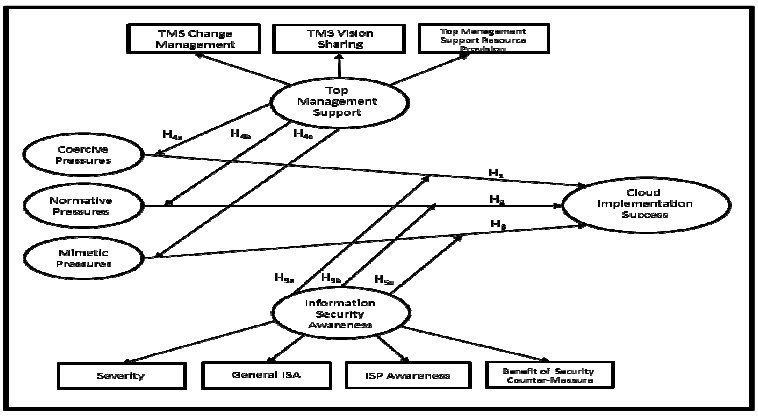

Figure 1. Conceptual Model

Methodology

The purpose of this survey research is to investigate the effects of institutional pressures on cloud implementation success and moderation imposed on that relationship by top management support and information security awareness. Survey research is appropriate for the proposed study due the investigation of expected relationships between independent and dependent variables and the effects of moderating variables (Pinsonneault and Kraemer, 1993). The proposed study will employ a quantitative, non-experimental, correlational design. A cross-sectional design will be used, as I will collect data at one point in time. The advantages of a cross-sectional design are that it is less time consuming, less expensive, and large amounts of data can be collected. An email-based survey method (questionnaire) will be used to collect data.

Population

The population for the proposed study is the more than 3,500 federal IT Specialists in DHS. The unit of analysis for this study will be conducted at the individual level. Information Technology Managers, Program Managers and Specialists will be included as participants in the proposed study. The sample for this study will be determined using the stratified sampling technique (Suresh et al., 2011). The third participant from each stratum of 10 will be selected into the sample. This study will use a sample size of at least 220 participants as required to use SEM.

Data Collection

The survey instrument proposed for data collection for this research is a questionnaire consisting of items measuring specific variables adapted from the literature reviewed for this study. Herath and Rao (2009) suggest adopting items from previously validated scales reduces problems with the reliability and validity of the questionnaire. Items on the survey will be measured using a 7-point Likert scale. The scales were adapted for the variables in Table 1 below:

Variable Name	Source	Items
IV1: Coercive Pressures	Liang et al., (2007)	3
IV2: Normative Pressures	Liang et al., (2007)	3
IV3: Mimetic Pressures	Liang et al., (2007)	3
Moderating Variable 1: Top Management Support	Lin, (2010)	7
Moderating Variable 2: Information Security Awareness	Bulgurcu et al. (2010)	6
Dependent Variable: Cloud Implementation Success	Wixom, 2001	3

Table 1. Variables and Research Questions

Statistical Analysis

This study will employ Structural Equation Modeling (SEM) using the Partial Least Squares (PLS) method to analyze data collected and test hypothesized relationships between the variables in this study. SEM provides a general and convenient framework for statistical analysis that includes traditional multivariate statistical analysis, which includes factor analysis, regression analysis, and discriminant analysis (Hox and Bechger, 1998). In a review of PLS-SEM articles, Ringle et al. (2012) found that a common argument for using PLS-SEM is that the technique excels at prediction and almost all model estimations use the coefficient of determination R^2 values to characterize the ability of the model to explain and predict the endogenous variables. Researchers have used SEM in several studies where non-experimental data was collected and analyzed and is thus appropriate for this research.

REFERENCES

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," *MIS Quarterly* (34:3), September, pp. 523-548.

Cebula, J.L., and Young, L.R. 2010. "A Taxonomy of Operational Cyber Security Risks," (No. CMU/SEI-2010-TN-028), *Software Engineering Inst., Carnegie-Mellon Univ, Pittsburgh, Pa.*, December, pp. 1-47.

DiMaggio, P., and Powell, W.W. 1983. "The Iron Cage Revisited: Institutional Isomorphism And Collective Rationality In Organizational Fields," *American Sociological Review* (48:2), April, pp. 147-160.

Herath, T. and Rao, H.R. 2009. "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations," *European Journal of Information Systems* (18), April, pp. 106-125.

Hox, J.J., and Bechger, T.M. 1998. "An Introduction to Structural Equation Modelling," *Family Science Review* (11:4), pp. November, 354-373.

Humaidi, N. and Balakrishnan, V. 2015. "Leadership Styles and Information Security Compliance Behavior: The Mediator Effect of Information Security Awareness," *International Journal of Information and Education Technology* (5:4), April, pp. 311-318.

Jarvenpaa, S.L., and Ives, B. 1991. "Executive Involvement and Participation in The Management of Information Technology," *MIS Quarterly* (15:2), June, pp. 205-227.

Jensen, T.B., Kjaergaard, A., and Svejvig, P. 2009. "Using Institutional Theory with Sensemaking Theory: A Case Study of Information System Implementation in Healthcare," *Journal of Information Technology* (24:4), December, pp. 343-353.

Kundra, V. 2011. "Federal Cloud Computing Strategy," *The White House,* Washington, D.C., Feb, pp. 1-39.

Lawrence, T.B., and Shadnam, M. 2008. "Institutional Theory," Oxford, UK, Blackwell Publishing, pp. 2288-2293.

Liang, H., Saraf, N., Hu, Q., and Xue, Y. 2007. "Assimilation of Enterprise Systems: The Effect of Institutional Pressures and The Mediating Role of Top Management," *MIS Quarterly* (31:1), March, pp. 59-87.

Lin, H-F. 2010. "An Investigation into The Effects of IS Quality and Top Management Support on ERP System Usage," *Total Quality Management* (21:3), April, pp. 335-349.

Meyer, J.W., and Rowan, B. 1977. "Institutionalized Organizations: Formal Structure as Myth and Ceremony," *American Journal of Sociology* (83:2), September, pp. 340-363.

Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A. and Rajarajan, M., 2013. "A Survey of Intrusion Detection Techniques in Cloud," *Journal of Network and Computer Applications* (36:1), January, pp.42-57.

Ogigau-Neamtiu, F. 2012. "Cloud Computing Security Issues," *Journal of Defense Resources Management* (3:2(5)), October, pp. 141-148.

Park, S.C. and Ryoo, S.Y. 2012. "An Impirical Investigation of End-Users' Switching Toward Cloud Computing: A Two Factor Theory Perspective," *Computers in Human Behavior* (29:1), January, pp. 160-170.

Pinsonneault, A. and Kraemer, K., 1993. "Survey Research Methodology in Management Information Systems: An Assessment," *Journal of Management Information Systems* (10:2), September, pp.75-105.

Ringle, C.M., Sarstedt, M., and Straub, D.W. 2012. "A Critical Look at The Use of PLS-SEM In MIS Quarterly," *MIS Quarterly* (36:1), March, pp. 3-14.

Rubóczki, E.S., and Rajnai, Z. 2015. "Moving Towards Cloud Security," *Interdisciplinary Description of Complex Systems* (13:1), January, pp. 9-14.

Scott, W.R. 1987. "The Adolescence of Institutional Theory," *Administrative Science Quarterly* (32:4), December, pp. 493-511.

Suresh, K., Thomas, S.V., and Suresh, G. 2011. "Design, Data Analysis and Sampling Techniques for Clinical Research," *Annals of Indian Academy of Neurology* (14:4), October, pp. 287.

Wixom, B. 2001. "An Empirical Investigation of the Factors Affecting Data Warehousing Success," *MIS Quarterly* (25:1), March, pp. 17-41.

Zheng, D., Chen, J., Huang, L., and Zhang, C. 2011. "E-government Adoption in Public Administration Organizations: Integrating Institutional Theory Perspective And Resource-Based View," *European Journal of Information Systems* (22:2), March, pp. 221-234.