Expert Systems with Applications 36 (2009) 10447–10460

Contents lists available at ScienceDirect

Expert Systems with Applications

journal homepage: www.elsevier.com/locate/eswa

Fuzzy cognitive map based on structural equation modeling for the design of controls in business-to-consumer e-commerce web-based systems

Sangjae Lee[a,1], Hyunchul Ahn[b,*]

[a] Department of E-business, College of Business Administration, Sejong University, 98 Kunja-dong, Kwangjin-gu, 143-747 Seoul, Republic of Korea
[b] School of Business IT, Kookmin University, 861-1, Jeongneung-dong, Seongbuk-gu, 136-702 Seoul, Republic of Korea

ARTICLE INFO

Keywords:
Fuzzy cognitive map
ECWS controls
Causal relationships
Structural equations modeling

ABSTRACT

Security and integrity of business-to-consumer e-commerce web-based systems (ECWS) is becoming a concern among ECWS adopters. The controls for ECWS are classified into controls for system continuity, access controls, communication controls, and informal controls. The control design for ECWS is not well structured and demands understanding of the complex causal relationships among environmental factors (infrastructure, organizational requirements for security), controls, implementation, and performance. In order to aid the design of ECWS controls, the application of a fuzzy cognitive map, ECFCM (EC-control design using a fuzzy cognitive map), was developed. Structural equation modeling was used to identify relevant relationships among the components and indicate their direction and strength. A standardized causal coefficient from structural equation modeling was then used to create a fuzzy cognitive map, through which the state or movement of one control component was shown to have an influence on the state or movement of others. Thus ECFCM provides a practical insight to IS auditors by addressing the applicability of soft approaches in capturing and illustrating the use of FCM in the design of ECWS controls.

1. Introduction

As the Internet becomes a part of daily lives, and business-to-consumer e-commerce web-based systems (hereafter ECWS) become widely available, security and controls issue in the use of electronic commerce (EC) have received critical importance in the workplace and home. The Computer Security Institute/Federal Bureau of Investigation (CSI/FBI) (2006) found that total losses from security damages for 2006 amount to $52, 494, 290 for the 313 respondents that were willing and able to estimate losses. The CSI study indicated that 48% of companies had experienced one to five security incidents in the previous year and the 39% of respondents attributed a percentage of their organization's losses greater than 20% to insiders.

IS auditors have relied upon their experience and know-how to make decisions on the degree to which a system maintains integrity and security. It is difficult to accurately describe the tasks of evaluating and designing ECWS controls, as conducted by managers and internal auditors. Designing ECWS controls is hardly simple, as it demands understanding of the complex interrelationships among various components (Lee & Lee, 2007).

A traditional technique for evaluating control systems is a checklist. The interactions among components, however, are such complex to be assessed using only a checklist method. ECWS auditors or managers can not easily quantify the strength and direction of the interrelationships among environmental factors, controls, implementation, and performance. A rigorous method is needed to integrate information from a number of data in order to assist ECWS auditors to fully understand the interrelationships among various components in controls design. This article proposes the use of an fuzzy cognitive map (FCM) approach in designing ECWS controls. This study suggests a causal structure of ECWS controls model where environmental factors, controls, implementation, and performance are causally interrelated. Sets of items to measure variables of environmental factors (infrastructure, organizational requirements for security), controls, implementation, and performance are assessed. The structural model is tested using data collected from firms adopting ECWS using a questionnaire survey method and associated measurements. This study adopts what-if simulation analysis using a FCM approach where input is operational performance and output is strategic performance to investigate interrelationships among the factors.

* Corresponding author. Tel.: +82 2 910 4560; fax: +82 2 910 4519.
E-mail addresses: sangjae@sejong.ac.kr (S. Lee), hyunchul.ahn@gmail.com (H. Ahn).
[1] Tel.: +82 2 3408 3980; fax: +82 2 3408 4310.

0957-4174/$ - see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.eswa.2009.01.070

2. Theoretical background

2.1. Types of ECWS controls

ECWS controls can be described as the process through which an organization accomplishes its goals when implementing ECWS. The controls can safeguard IS resources, thereby accomplishing the system objectives of timeliness and accuracy. ECWS controls are classified into management and application controls, which is the most common classification scheme suggested in the literature of IS controls (Weber, 1999). Management controls are fundamental controls in that they encompass general IS management, security management, IS development and maintenance, and operations management. Application controls seek to ensure that an individual application system achieves integrity and security requirements. The ones of most important management controls of ECWS controls are controls for system continuity. This study suggests controls for system continuity as management controls.

Application controls are further divided into *internal application* and *external application* (or communication) controls. Internal application controls deal with internal components of ECWS systems such as the application system interface, while external controls are involved with external ECWS systems networks, and the communication interface with customers and the network service provider. Internal application controls are established to monitor the internal application systems, like a production system or a sales system, linked to an external network. In an integrated ECWS, minor failures or a short downtime of one system may adversely affect other systems. Adequate detective controls (controls that identify the occurrence of errors and failures) and contingency planning should be installed to prevent errors from affecting the whole system. In this study, access controls are described as controls to protect internal applications and communication controls protect external applications such as networks. Thus, this study suggests access controls and communication controls as (internal and external) application controls.

The controls for system continuity, access controls and communication controls are formal controls attributes in that they are “visible” and management-initiated procedures or mechanisms to ensure system security and integrity. This study includes informal controls as ECWS controls, which represent commitment of IS staff members in IS controls, experience of IS staff members in IS controls, and Cooperation of IS staff members for IS performance. These are established by the propagation of common beliefs and social norms within a group of individuals, which is the socialization process identifying “acceptable behaviors” (Dhillon & Backhouse, 2000). The trend toward decentralized computing resources leads to the gradual transfer of control over these resources from management and central authorities to employees. This decentralization increases employee autonomy as a way of enhancing the employee’s sense of responsibility, involvement, and motivation. The social control theories can be applied in the context of computer abuse: attachment, commitment, involvement, and norms help prevent insider computer abuse in organizations (Lee, Lee, & Yoo, 2004).

Table 1 presents three modes of controls adopted in this study.

2.2. Organizational contexts and ECWS controls

The security effectiveness depends on various organizational factors such as size, top management support, industry type, managerial attitudes toward security risks, IT resource posture, and executive management support (Kankanhalli, Teo, Tan, & Wei, 2003; Kotulic & Clark, 2004). An ECWS controls model ties together five factors representing organizational and IS related factors. The factors include top management support, system compatibility, IS infrastructure, IS expertise, and IS security concern. Other variables that have a second or lower order effect on ECWS controls are not included. The organizational and IS related factors included in the research model looks into issues being confronted in efforts to introduce ECWS controls. The causal model for ECWS controls is depicted in Fig. 1. The following subsections explain the relation in the model in detail:

2.2.1. IS infrastructure

Information systems executives consider the capability of IS infrastructure as one of the most important issues (Brancheau, Janz, & Wetherbe, 1996). A basic level of IS infrastructure is necessary to successfully implement a new technology (Cash, McFarlan, McKenney, & Applegate, 1992). The range-enabling complex transactions and boundary crossing services across multiple business units are possible through a rich set of infrastructure capabilities (Broadbent, Weil, & Clair, 1999). The extent of efforts to introduce an IT innovation depends on the existing practices and hardware/software currently adopted (Chau & Tam, 1997). Kotulic and Clark (2004) suggest that IT resource posture including all of the technologies, capabilities, data and information affects security program effectiveness. Organizations with appropriate level of cross-functional and cross-business applications and telecommunications infrastructure, firm-wide consistency in architecture and standards for system development and operation, and experience with integrated database applications are better prepared for ECWS controls. ECWS controls are likely to be better implemented on the sophisticated IS infrastructure composed of multiple platforms with different operating systems, applications, and connectivity arrangements.

2.2.2. Organizational requirement for security

Kotulic and Clark (2004) suggest that managerial attitudes toward risk influence management choices relative to the

Table 1
Modes of controls.

Control class	Controls	Objectives	Description
Management controls	Controls for system continuity	Availability	Procedures for the recovery of information systems department’s services following unanticipated interruptions and the backup of critical resources
Internal application controls	Access controls	Integrity, confidentiality	Procedures designed to ensure that access to data and programs is controlled and authenticated
External application controls	Communication controls	Integrity, confidentiality	Procedures used by company to ensure security in inbound and outbound transactions. Procedures designed to ensure that error are detected and corrected during input of data and the process of data is authorized and appropriate during communication
NA	Informal controls	NA	Commitment of IS staff members in IS controls, experience of IS staff members in IS controls, and cooperation of IS staff members for IS performance

NA, not applicable.