Inf Technol Manag (2010) 11:43–59
DOI 10.1007/s10799-010-0065-2

The relationship among formal EDI controls, knowledge of EDI controls, and EDI performance

Sangjae Lee · Kun Chang Lee

Published online: 29 January 2010

Abstract As new technologies and software applications are supplanting traditional electronic data interchange (EDI) applications, new fraud concerns due to the ubiquitous connectivity of the Internet have increased the interest in EDI controls. Traditional outcome (or process)-oriented views of (formal) control should be supplemented by knowledge management considerations, and user knowledge of contents control and its importance should be enhanced in order to maximize performance. This research addresses the indirect effect of EDI control usage levels on EDI performance through knowledge enhancement. EDI controls were categorized as internal and third-party in order to highlight their internal and external aspects in inter-organizational systems. Knowledge of controls has two parts: knowledge of control content and an understanding of control importance. The research model was empirically tested using a structural equation modeling approach with data collected from Korean companies that have adopted EDI. The results indicate that knowledge plays an important role in mediating the effect of controls on performance. That is, EDI adopters can achieve operational and competitive benefits from high levels of knowledge in relation to control content and its importance.

Keywords EDI · EDI controls · EDI performance · Knowledge of controls · EDI adopters

S. Lee
College of Business Administration, Sejong University, Seoul 143-747, Korea
e-mail: sangjae@sejong.ac.kr

K. C. Lee (✉)
SKK Business School and Department of Interaction Science, Sungkyunkwan University, Seoul 110-745, Korea
e-mail: kunchanglee@gmail.com; leekc@skku.edu

1 Introduction

Electronic Data Interchange (EDI) is a type of inter-organizational electronic commerce (EC) that allows organizations to exchange business documents electronically in a structured, machine-readable format. The rapid growth of EC in the global scope is propelling developing countries to adopt EDI to conduct international electronic business-to-business trades [39]. The Internet offers a number of new communication possibilities, and its few geographical constraints and large-scale connectivity make it the most feasible channel for EDI [55]. The rationale for participating in EC (defined by the U.S. National Institute of Standards and Technology as electronic data interchange) is that there is a new opportunity to create a product, provide a service and increase market share. It is relatively easy to adopt EC; the problem with the Internet, however, is how to maintain the security of internal business systems and computer networks. The 2008 Computer Security Institute/Federal Bureau of Investigation (CSI/FBI) [12] found that respondents' estimate of the losses caused by various types of computer security incidents averaged $288,618 for the 522 respondents. The CSI study indicated that almost half of the companies had experienced one to five security incidents in the previous year. The survey indicated that considerably more respondents believed that their losses from security incidents were due to attacks from outside, jumping from 36% last year. The vast majority of respondents said their organizations either had (68%) or were developing (18%) a formal information security policy.

Although EDI provides many benefits, it has drawbacks such as channel conflict [44] or increased vulnerability due to the sharing of operational information with trading partners [24]. Increased EDI use results in security risks

that increase according to the extent of user integration and reliance on the system [36, 37]. A factor that affects the successful implementation of EDI is EDI control over the security and integrity of the system [57]. The security and integrity of applications and networks is increasingly critical as transaction processing becomes more automated and more closely linked to operational decision making. With the growing dependence on IS to increase organizational effectiveness and productivity, the demand for reliability and integrity of information has become even greater.

Unless the appropriate controls are in place, the increased transaction speeds and reduced human intervention of EDI pose a much greater risk of data errors, lost transactions and uncontrolled processes. EDIs automated, real-time nature requires that systematic and computerized safeguards be put into place to isolate and track individual transactions from origin to destination. The boundaries of the system include networks and other third parties, as well as trading partners and the computer applications involved in the transmission. Direct access by unwanted hackers through an external network connection is not the only security concern, as numerous other remote points of network access exist. Particular attention should be directed at accounting cycles and functions [9], as the value of traditional paper-based accounting reports has been significantly challenged. The business cycle has been reduced to a computer-to-computer exchange, effectively eliminating the need for paper invoices, purchase orders or checks. As dependence on automated controls to monitor accounting functions increases, user skills and training must be adjusted to new processes and new control procedures. Organizations should create the controls necessary to both reduce risk and enhance system performance.

Generally, IS (and EDI) controls for security and integrity are concerned only with the formal or technical aspects of information management (e.g., formal administrative and procedural controls, access control software); however, any formal or technical system characterized by bureaucracy is supported by the informal system of an organization [15]. Formal or technical systems reside in a larger informal environment where beliefs, responsibilities and commitments are made and discharged, meanings are established and altered, and intentions are understood. Companies tend to concentrate their security efforts on tangible concerns, such as data files and software and on guarding entrances and communication networks. In many cases, corporate IS security administrators are not fully aware of the security risks resulting from lack of employee knowledge, commitment, responsibility, and awareness of controls. Informal factors such as these constitute an "invisible" security force that safeguards businesses by implementing procedural controls that ensure their smooth and effective operation.

There is a growing awareness among today's businesses that a more systematic approach to knowledge-sharing is necessary for success [14]. Knowledge management, as an area of academic research, has only recently begun to receive attention. The overall purpose of knowledge management is "to understand, focus on, and manage systematic, explicit, and deliberate knowledge building, renewal, and application" [64]. Competitive knowledge assets and their effective utilization are critical for organizational success. For instance, the success of Japanese firms is thought to be based on their skill and expertise at "organizational knowledge creation," that is, their ability to create new knowledge and disseminate it throughout the organization: "Japanese companies have used knowledge management to cope with something new—a new marketing approach, a new technology, a new product design" [46]. Japanese companies have initiated corporation-wide efforts to manage knowledge in such internal functions as research and development, marketing and quality management.

Knowledge management is also important within the context of IS security and controls. Securing an information system from potential intruders demands a high level of technical knowledge, as hackers are constantly improving their techniques. Security policies, therefore, must begin with a solid foundation in technical expertise and management, and security administrators and IS staff members must be fully trained in the special implications and operations of IS as they relate to the security of their business as a whole. They should understand the place of IS in the business process and its impact on the job, and should work closely with the internal auditor, perhaps forming a corporate security team that involves other groups as required. This team may perform an ongoing IS review that ensures close monitoring of the system. The best control design and implementation depends on the expertise of the team, who must consider organizational circumstances, others' experiences and practices and the cost-effectiveness of the controls they put into place. Obviously, sufficient specifications, manuals and training materials are a part of an acceptable control system [47].

Some researchers and practitioners have questioned whether significant cost savings and other durable benefits can be gained from using EDI. EDI literature has examined the factors affecting EDI performance, which include organizational support (such as user involvement and training), implementation success, and implementation capability (such as planning, evaluation and championing) (e.g., [49]). This study attempts to extend this stream of research by exploring the knowledge of EDI controls and its impact on the relationship between formal EDI controls and performance. The causal model attempts to explain how knowledge of control content and the importance of controls contribute to system performance. A research

model for EDI controls is proposed, based on EDI implementation and control literature. This model was empirically tested with data collected from Korean companies that have adopted EDI. A summary of the empirical findings, their practical implications, and future research issues is also included.

2 Theoretical framework

2.1 Electronic data interchange (EDI)

A great deal of research has linked the Intranet and/or extranet and other technologies to inter-organizational information systems such as EDI [45], focusing on analyses of telecommunications-based systems that can play a role in supporting business strategies. EDI is changing rapidly to an Internet-based format due to the rapid development of Internet-based information technologies [42]. Internet-based EDI systems result in increased transactional precision between/among businesses, increased information transfer speed through simplified work processes, and greater productivity and work efficiency. Many researchers have suggested that the intermediary functions of Internet-based EDI systems, such as networking technology that enhances the efficiency of organization and managerial performance, also provide many advantages [10].

Based on organizational innovation and IS implementation theory, the adoption and implementation of Internet-based information intermediary system was explored with the purpose of identifying factors that explain or predict the successful implementation of an Internet-based information intermediary system and to evaluate the impact of such a system on an organization's competitive advantage. Researchers have previously attempted to identify the major factors affecting the successful implementation of IOIS and EDI systems [11]. These success factors include organizational support, the implementation process, control procedures, compatibility, organizational size, functional differentiation, training, MIS support, vendor support, customer influence and the level of system integration in a particular firm. The level of success also depended upon the level of imposition of the systems by partners.

The growing familiarity and practicality of the Internet make it a strong alternative to implementation on business-to-business (B2B) communications, thus capturing market share from EDI. EDI, company websites, B2B hubs, e-procurement systems, and Web services are the mainline EC architectures [1]. The adoption of IT-based interorganizational linkages has become the center of attention due to the increased focus on B2B EC over the Internet [33, 54, 58, 60].

With the emergence of the Web-based platform, EDI can continue to be the most vibrant IOS technology for B2B electronic transactions [17, 25]. A large portion of B2B electronic transactions continue to be exchanged via EDI over a third-party value-added network or the Internet [43, 59, 61, 65]. While EDI systems have been replaced with online B2B exchanges or a more open infrastructure such as XML (extensible markup language), which is touted as a more flexible and less expensive successor to ED, it remains for firms to migrate EDI to XML due to the considerable costs incurred from implementing and maintaining the technology and from redefining processes on each side of the relationship [31]. Further, EDI is considered to be secure and a means to avoid risk. Enterprise application integration (EAI) helps extend the batch orientation of traditional EDI to perform real-time transactions over the Internet [32].

2.2 IS controls and security knowledge management

In this study, IS controls are defined, behaviorally, as the activities or processes that ensure system security and integrity. IS controls broadly incorporate management controls, which in turn deal with the development, implementation, operation and maintenance of IS, and application controls, which manage the input, process and output of each application. Control is generally recognized as a fundamental management activity, but control issues such as security and integrity have received only cursory attention among IS researchers. IS controls are designed to affect individual action and, consequently, performance, ensuring that an error or failure in the system does not propagate into other applications or organizations. IS may not reduce cycle time or administrative costs unless their controls are well designed.

Human behavior is always an active component of controls (even those that are automated), and persons who are constrained or monitored by controls should tolerate and "respect" them [47]. Many people do not like to enforce controls and will neutralize them or otherwise shut them off if given the chance. Others may consider them attractive challenges. Dedicated and ingenious programmers can bypass any control system, no matter how sophisticated. Manual procedures and safeguards are often unenforceable and ineffective in practice. Given that people may not have patience with controls if their importance is not frequently stressed and reinforced, it is important to obtain support from users, especially knowledgeable users, when providing the reasons for constraints and principles. Management should willingly set an example and provide incentives (e.g., rewards or job promotion) for employees who conform to controls. However, enforcement of controls should not be required beyond a reasonable and

acceptable level. Controls should not force employees to challenge the unauthorized activities of their colleagues, for example, as such behavior would make many of them feel uncomfortable.

Organizations should be clear about what constitutes improper behavior. Possible ways of doing this include professional ethics statements, computer security awareness sessions, distributed system guidelines, reports on discovered violations and informal discussion. Security administrators can deal with such topics as system authorization, conditions for use, penalties for security breaches and methods for changing passwords.

While research continues on more sophisticated formal or automated control mechanisms (e.g., encryption, firewall techniques), relatively few studies have been conducted on the *management* of controls. The presence, and especially the mechanism, of control should be kept secret except when deterrence is achieved by its visible presence [47]. Despite the development of highly advanced security techniques, lax security practices often diminish the effectiveness of controls. For instance, despite the widespread use of sophisticated passwords systems, system users' awareness of the consequences of the passwords they choose is generally low [66]. User-selected passwords are easy to remember and simple in structure, composed of personal details meaningful to the user, and are frequently written down and rarely changed. An authentication control system utilizing user passwords is more effective if users first establish a positive, unique identification of each person or entity to which access is to be granted. Development of authentication technology should be commensurate with sophistication in the management of access authentication.

A control should function effectively and have a lifetime appropriate to the activities with which it is associated. Once a safeguard has been implemented, its use may sometimes demand extensive modification to cope with developing circumstances [47]. For instance, in order to reduce exposure to systematic guessing trials and enhance security in a password system, user authentication strategies ("three strikes and you're out") can be employed. Other values, such as time limits, authorization limits or passwords, can be applied to make controls more effective. To protect them from being compromised, segregation of duties or dual controls may also be necessary. Compensating controls must be prepared for use during deactivation periods when controls are shut down to replace and repair systems, or when changes must be made to the conditions or functions of applications. Moreover, controls should be imposed uniformly and consistently on every person and object that they constrain, as exceptions to rules and procedures may result in deterioration of the value of control and increase vulnerabilities.

A central premise of this article is that the traditional outcome (or process)-oriented point of view of controls limits their influence on system performance and hence that the traditional perspective should be supplemented by knowledge management considerations. User knowledge and understanding of the need for security should be enhanced in order to ensure the effectiveness of formal policies and the security-related behavior of users [19]. This is consistent with the organizational controls literature, which asserts the necessity of multiple modes of control. If formal controls are necessary, some informal controls (e.g., knowledge, experience, commitment) should also be "managed" to ensure high morale, job performance and group cohesiveness [28]. Educational efforts are needed, for example, to raise the security consciousness of system users. Project managers' individual characteristics, such as their personal skills and levels of experience, affect their capability and performance in managing software risks and system development [53].

The need for knowledge can be discussed in terms of general innovation-diffusion theory. Knowledge of and expertise in the use of control mechanisms is generally related to *complexity*, one of the characteristics of innovation. Rogers [51] has defined complexity in innovation as "the degree to which an innovation is perceived as difficult to understand and use." Complexity inhibits the adoption and diffusion of innovation and possibly reduces satisfaction and success from the implementation of technology. Firms should possess knowledge commensurate with the levels of control they apply to managing the linkage of different hardware/software, network protocols and complex network infrastructure. Organizational learning is an important theme in innovation literature, as it provides high competitiveness and productive environments that are protected from technological change or redesigned business practices [16]. Learning occurs internally through such mechanisms as technological/R&D development [21] and reflection on past experiences, and externally through boundary scanning and customer and technology analysis for new developments and opportunities. Successful business process change depends on learning capacity that is represented by the capability of several factors, including the following: "learning from others" (benchmarking), "learning by doing" as a means of improving learning efficiency, developing a cumulative knowledge base, using external information along with "higher" level learning which reflects on past experiences and adapts change strategies [20]. This helps companies to set goals continuously, measure achievement and understand problems within current processes.

IT innovation is usually accompanied by business process changes. In particular, organizational structure and operational processes may change greatly and undergo

"business reengineering" when use of information technology strongly affects the way firms do business [22]. The implementation of control procedures in a redesigned business process is a critical change management issue, as it poses new challenges to organizational controls through compression of responsibilities, empowerment of employees, and a reduction of supervisory controls [56]. The effectiveness of a redesigned business process depends on a corresponding realignment of organizational controls. Traditional controls based on independent checks, and manual approval procedures using paper source documents are less useful due to the broader span of managerial control and the automated and real-time nature of the process. Control themes that appear to be appropriate include the automation of many manual controls. For instance, independent checks for completeness and accuracy are replaced by edit checks at the input stage; approval authority is applied according to programmed predetermined standards. The segmentation of controls, i.e., the application of different control mechanisms to transaction segments that have different sensitivities and vulnerabilities, is another emerging control theme that promises to enhance the contribution of controls on performance by focusing on controls that "add value" to business. Thus, rules and procedures based on transaction value, the reasonableness of segregation criteria for transaction streams, and an appropriate control design become critical.

The capacity for learning necessary for successful business process change should encompass the control and security issues raised by the implementation of new technology. An effective IS control system demands a high level of knowledge about physical, operational, and technical safeguards [47]; accordingly, trained employees must be assigned responsibility for managing IS security. Responsibility should also be assigned for educating users about the risks, effects, impact of threats, and the proper procedures to follow in assessing the design or operational effectiveness of specific controls [30]. Automated controls should be performed by technically competent non-management personnel whose work might include installing appropriate software safeguards, regularly reviewing computer logs, developing computer operational and recovery procedures, and procuring the necessary testing and backup software or hardware components.

The importance of knowledge and responsibility in IS security and controls can be understood in terms of general deterrence theory. General deterrence theory asserts that illegal behavior in the general population is negatively related to the certainty and severity of punishment for abusers [8, 48]. Organizational guidelines for acceptable system use should be distributed to dissuade potential offenders and to give IS controls a deterrent effect. It is the perceived risk of punishment and penalties for violations, rather than the controls themselves that are important, and this is commensurate with efforts to inform users that unethical behavior produces a negative rather than a positive result. At the same time, if people are unaware of the gains to be made from unauthorized acts, the desire for unauthorized gains is reduced. As a deterrent to computer abuse, the presence of controls can be made widely known by such methods as training, rewards for good performance, communicating positive experiences, and imparting responsibility for results.

A strong "outcome orientation" is necessary for the effectiveness of controls in the highly interdependent business processes that result from business reengineering (which might be accompanied by successful EDI implementation). Reliance on outcome controls stresses accountability with clear performance targets, stresses the reward-performance linkage, and stresses core values and culture [56]. Enhanced monitoring of individuals, work status and a reward structure to provide incentives for individual accountability are important to deal with the "higher" risks resulting from greater interdependence of business processes and employee empowerment. Active promotion of core values such as integrity and fairness is necessary as a guideline for acceptable behavior and should be communicated among employees, as this will mitigate the risks of potential compromise behaviors that may be detrimental to system performance. This "outcome orientation" requires employees to have comprehensive knowledge of control content and importance, as it is intended to provide a sense of the organization's overall direction and to elicit commitment from employees; it is positively reinforced though core value awards for employees who faithfully conform to organizational procedures.

2.3 Modes of EDI controls

Many different controls can be applied to enhance IS security and integrity. IS controls can be classified in terms of data processing activities such as operations, application programming, system programming, and system planning and standards; computer applications requiring security such as those related to production, accounting, and marketing; priority of security functions such as preventive, detective, and corrective controls; and the objectives of security processes such as authentication, accuracy, audit trails, completeness and privacy controls [63].

Among the three modes of controls suggested by Lee et al. [38], this study deals with formal controls and knowledge of controls, which are one component of informal controls. There has been little research that has applied a conceptualization of formal and informal controls in the context of IS security, despite the fact that it is based on a long tradition in organizational behavior studies.

Theory building can also be facilitated by a large body of existing control literature, and tasks related to IS security are good candidates for structuring formal and informal control mechanisms, as they are unstructured and complex.

This study classifies formal EDI controls as internal controls and third-party controls as external controls. Internal and external controls exist in response to the internal and external aspects of inter-organizational systems. Internal EDI controls cope with security threats within an organization that result from human behavior or erroneous business processes. They include operational procedures, process changes and standards. Internal controls also encompass internal applications (e.g., accounting or sales connected to the network) and the communication interface. External controls, on the other hand, include controls provided by third-party network services and trading partners. External controls deal with security threats from the external environment, such as telecommunications networks and trading partners. They involve formal contracts, such as technical and operation procedures of trading partners and Value-Added Networks (VANs).

Internal formal controls can be sub-classified into application and communication controls. These differ according to whether they deal with internal EDI systems (such as an application system interface) or external EDI systems (such as the interface with a VAN, or a network linked to trading partners). External controls are primarily implemented by third-party VAN service providers and are therefore classified as third-party controls for the purposes of this study.

There are two types of third-party controls: third-party communication controls and network service controls. Third-party communication controls involve temporary procedures for short-term outages and contingency planning for reinstatement of processing. Third-party network service controls center on the provision of compatible network infrastructure and functions (e.g., standards, protocols) in order to facilitate the development of EDI systems. These controls are specified in the agreements that must be reached between trading partners regarding transmission and message standards, and communication protocols.

2.4 Knowledge of controls

As stated above, knowledge of controls can be regarded as one aspect of the informal controls of Lee et al. [38] and Lee and Han [35]. Informal controls are initiated through communication among organization members who rely on members' values and judgments. Knowledge of controls has two parts: *knowledge of control content* and *knowledge of control importance*. The former indicates the degree to which employees are aware of the details of control procedures and have the capability to design and operate controls. Control activities and procedures should be understood in terms of "process" characteristics in implementation and operation of controls. The knowledge of control content allows employees to cope with various routine and non-routine situations, and this is enhanced by work experience and education. Through education and training provided by management or external third parties, expertise with respect to various assets, threats, and exposures may be learned for use in implementing controls. Experience in the operation of controls enables a more flexible application of controls that can incorporate organizational considerations regarding, for instance, allowances for errors, mischievous behavior, the scope of assets to be protected, and security privileges rather than strict adherence to control procedures.

Knowledge of control importance represents the degree to which employees feel a sense of responsibility for organizational performance and the importance of controls. The "ends" or "outcome" aspects of controls should be completely understood by employees with regard to the potential impact of deficient control on organizational performance. This enhances the commitment to controls and the deterrent effect of controls, as it prevents intent from reaching the degree necessary to carry out a violation of trust, which may lead to unacceptable or disagreeable outcomes [47].

3 Research model

Based on the theoretical framework discussed above, a research model concerning relationships among EDI controls, knowledge of controls, and EDI performance was developed. It is presented in Fig. 1. The research model addresses the indirect effect of the usage level of EDI controls on EDI performance through knowledge enhancement. The usage level of internal formal and third-party controls is positively associated with the knowledge of control content and the importance of controls that individuals in the company possess. System performance is

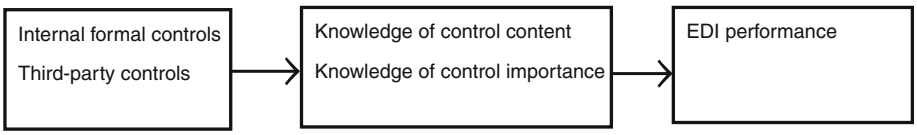

Fig. 1 Research model

indirectly affected by the usage level of controls through knowledge of controls. This study mainly deals with the mediating role of knowledge of controls in EDI performance, as studies concerning knowledge of management issues within the context of IS controls and security are rare.

The ultimate goal of EDI controls is to derive EDI benefits. The techno-centric view is that more controls lead to a more secure system, but it is not clear whether tighter control of EDI translates into greater organizational benefits. The key issue is hypothesized to enhance the knowledge of controls such that the effects of controls on performance are the greatest.

3.1 Internal formal controls, knowledge of controls, and performance

The successful implementation of a complex technological innovation such as EDI depends on the ability to modify and master the technology and to adjust internal organizational practices and procedures. The flow of technical know-how from suppliers of complex technologies to user organizations is not always complete [3], and acquisition of knowledge and expertise is necessary to take on the technical challenges of EDI, as it helps lower "knowledge barriers" [41]. The knowledge necessary to deal with the technical aspects of implementing EDI and its controls may lead to system success: companies with a high level of technical expertise may be better able to cope with the technical issues of EDI implementation, but EDI staff members should nonetheless be trained on issues specific to the new technology. From the point of view of security and integrity, organizations with wider experience in internal formal controls can improve management practices, vis-à-vis security risks, by sharing experiences and building a culture of risk awareness that will subsequently apply more effective risk management methods. More experienced EDI staff members can better estimate the risk levels of new applications and the potential for threats to occur. Managerial attention, commitment, and a disciplined process for developing applications and communication interfaces, rather than specific risk management techniques, can improve risk management performance in these systems.

The full effectiveness of internal formal EDI controls can be realized only if they can monitor transaction processes across integrated systems in a timely manner. The subsequent application of control procedures across departments is more complex and problematic, as it may require changes to organizational work practices and significant commitment to ensure success. Process change in traditional audit procedures is needed, as paper or electronic source documents often no longer exist as such [6]. The existence of proper controls and audit trails around the EDI function is necessary to isolate and track individual EDI transactions from origin to destination. Perceived EDI performance is dependent on the ability to operate and maintain the controls, i.e., on the knowledge of control content. EDI transactions are generated by program logic or an indirect series of events in which the maintenance of adequate traceability of transactions can become very complex. Business processes should therefore be designed jointly with trading partners and the underlying "implied transactions" and application logic should be regularly reviewed and adjusted. A shipping notice of an order for replenishment of a safety stock or a report of sales order information applied against inventory levels should be logged and checked to determine whether they have the desired result. Reconciliation of resulting transactions should be performed, for example, by reconciling a shipping notice against the generation of a payment authorization for that shipment. A complex chain of interrelated external and programmatic events usually entails several points of possible exposure; consequently, formal monitoring procedures and human intervention must be combined with application logic [7]. The effectiveness of these systems depends, then, on the expertise and perceived sense of control importance that EDI staff members possess regarding the measures underlying the EDI transaction process.

Knowledge of control content and its importance is necessary in order to establish effective internal formal controls. Risk analysis is a series of *judgment* decisions concerning asset identification and valuation, threat identification and analysis, vulnerability analysis, risk assessment, and controls identification. The threats are often a broad range of forces capable of producing adverse consequences. Vulnerability is a security deficiency that makes it possible for a threat to materialize. Risk is the possible loss incurred from the occurrence of a threat. The relationship among assets, threats, vulnerability, risk, and controls should be identified for risk management and control design.

IT assets should be analyzed first, then the threats to those assets, and finally the vulnerabilities of those assets should be examined. Following risk analysis, several alternative security measures that address a specific risk are suggested. The determination of allowable risks (i.e., the acceptance of great danger without controls) relies on prudent business judgment. Therefore, knowledge of control content and importance is essential in order to assess the risks concretely and enhance the effectiveness of EDI controls.

Hypothesis 1-1 The usage level of internal formal controls indirectly affects EDI performance through their effect on the level of knowledge of control contents.

Hypothesis 1-2 The usage level of internal formal controls indirectly affects EDI performance through their effect on the level of knowledge of control importance.

3.2 Third-party formal controls, knowledge of controls, and performance

Knowledge of the content and importance of controls is needed to establish new rules and procedures, set up interfaces with the telecommunication infrastructure provided by a third-party network service, and persuade reluctant users. The ability of EDI adopters to accumulate experience is very important to obtaining benefits from EDI implementation with the VAN supplier and trading partners. Knowledge of control development, control operation, and testing methods for controls is important; for instance, every control should be instrumented in such a way that it gives a timely, logged alarm or notice of activation and deactivation in any case of malfunction in the VAN or the internal systems of trading partners. Attendants of controls can provide some notice when significant deviations occur and should be trained to record all extraordinary circumstances and to check them for compliance at reasonable intervals. Separation of those responsible for controls from those subject to them is also necessary. The development of test methods and criteria must be accomplished during the design and specification stages of each control.

Implementing control systems with the VAN and trading partners is difficult and unstructured, as there is no normative model of EDI controls. Many alternative VAN services and forms of controls may exist, and many environmental factors can affect the design of controls. It is difficult to establish if–then rules explaining the choice of controls in some organizational contexts given that the benefits of controls are hard to measure quantitatively. Many organizational factors, such as the volume and complexity of transactions and the speed of processing, affect the effectiveness of third-party controls.

Staff members must analyze the organizational context and select third-party controls that are most appropriate for a given situation; they must then concentrate their limited IS resources to design and effectively implement these controls. However, determining and evaluating the required controls requires subjective, nondeterministic and context-sensitive judgments. EDI staff members often use analogies from their previous experience to design controls, but the effectiveness of this reasoning is moderated by its cognitive and situational limitations. As EDI staff members may directly or indirectly have encountered only a limited number of cases, their ability to retrieve analogous cases is also limited.

The introduction of IS controls must proceed in view of an organization's requirements for security and integrity. It is inefficient to implement expensive control subsystems if the sensitivity and vulnerability of the systems themselves are not high. Considering that available resources are limited, it is not possible for EDI managers to develop all of the necessary controls, and it is difficult to allocate resources for protection from a particular vulnerability, as it is also difficult to isolate and treat vulnerabilities separately [47]. Overemphasis on one subset of security functions or vulnerabilities in comparison with others may increase security deficiencies or lead to serious sub-optimization. Nevertheless, the effectiveness of IS controls depends on the quality of the control design process as performed by internal staff members or management.

Substantial knowledge of control content and importance is needed to provide guidance in the selection of third-party controls; the cost of their usage should be lower than the reduction in expected losses. It is not always clear to managers, however, how to assess the costs and benefits of system security and how to obtain a "reasonable assurance" of computer security. It is very difficult to know how much computer abuse and error is avoided or deterred by installing a third-party security system. The benefits of each EDI control vary across organizations, and the benefits of third-party EDI control systems are related to decreased occurrence of irregularities or errors. It is difficult to assess the benefits of third-party EDI controls accurately, as these benefits are different across organizations confronting different organizational environments; EDI staff members must determine which controls are necessary from the viewpoint of cost–benefit effectiveness. Knowledge of control content and importance are critical in determining an effective set of third-party controls in a particular organizational context related to EDI performance.

Hypothesis 2-1 The usage level of third-party controls indirectly affects EDI performance through their effect on the level of knowledge of control contents.

Hypothesis 2-2 The usage level of third-party controls indirectly affects EDI performance through their effect on the level of knowledge of control importance.

4 Research method

4.1 Research design

A field survey was organized to test the significance of the relationships among variables using a statistically testable sample. The objective was to validate and enhance the isolated claims of past research so that they can be generalized to a larger population of companies. A mail survey was the primary method of data collection. Prior to completing the questionnaire, all participants were provided

with an information sheet describing the definitions of key terms such as EDI, EDI controls, standards, VAN, and trading partners. Confidentiality was assured to obtain reliable responses from the questionnaire, which addressed such sensitive and confidential issues as IS security and controls. On the other hand, personal contacts stimulated the trust and cooperation which are often required to provide sensitive information about control systems. Personal contacts tended to elicit relatively more full and frank responses. In addition, it was important to ensure that these questions could be answered by EDI practitioners.

4.2 Participants

The unit of analysis in this study was the individual EDI adopter organization. Among more than 7,000 Korean companies that have used KTNET, one of the major VAN service providers in Korea, and among those that have adopted EDI, respondent organizations were selected as follows. The industries which have used EDI heavily were first determined, and from publicly available company databases (through the Chollian Network by DACOM), approximately 2,000 Korean companies that had implemented EDI comprehensively were selected. The sample was not random, as questions about controls can be answered reliably only by the companies which have implemented EDI comprehensively. Questionnaires were mailed to 500 companies after they had been contacted to confirm their levels of EDI adoption.

Participation in the survey was solicited through direct calls to EDI managers in which the objectives of the study were explained. Responses were encouraged by one of the authors, who was at the time attending KTNET. In total, 157 completed and returned the survey, a response rate of 31.4%. The response rate was adequate given that the questionnaire was long and complex. 5 questionnaires were excluded from final sample because the replies on these contained omitted data, resulting in a final sample of 152 companies. Some companies refused to participate in the survey because they were afraid of exposing the vulnerabilities of their systems. A comparative analysis of industry membership and revenues was conducted in order to determine whether responding firms had characteristics significantly different from non-responding firms. No significant differences were found, supporting the conclusion that response bias was not a concern in this study. The industry distribution of the sample is shown in Table 1, which indicates that the responding firms were fairly well distributed across various industry types.

The average number of employees in the responding organizations was 1,396. The average annual sales amounted to 761.1 billion won (0.692 million USD). Larger firms are able to invest resources to integrate and control EDI more easily than small firms; therefore, EDI user firms would be expected to be larger firms. The mean utilization of EDI was 23.7% and the average number of trading partners was 84. EDI had been used for 2.9 years on average. The elapsed time since the first adoption of EDI was less than 5 years for 80% of the companies.

Table 1 Industry representation of responding companies

Name of industry	Number of firms	Percent (%)
Electronics industry	52	34.2
Textile manufacturing	39	25.7
Chemical product manufacturing	20	13.2
Food manufacturing	10	6.6
Paper manufacturing	9	5.9
Trade industry	8	5.3
Others	12	7.9
Total	152	100

4.3 Measures

EDI controls were measured by statements to which the respondent was asked either to agree or to disagree on a seven-point Likert-type scale. Table 2 describes the operationalization of each variable along with corresponding references. Each variable was measured wherever possible with multiple indicator items. The questions pertaining to EDI controls were refined from the work of based on Lee et al. [38], which had been adapted in turn from Chan et al. [9], Jamieson [27], Marcella and Chan [40], and the ISACA [26], who explained the concepts, objectives, characteristics and techniques of EDI controls and auditing. The measurement was based on the responding firm's expressed perception of the usage level of controls. The modes of controls and subparts in Table 2 comprise the latent variables and constructs.

The items for the constructs indicate the expressed perception of the usage level of controls. For instance, one item of internal formal application control is: "Systems are changed only through authorization from the responsible managers." If respondents strongly agree to the statement (score 6 or 7), they are claiming to perceive that the usage level of that control is high.

The measure for EDI performance was based on various EDI survey results [4] and EDI management and controls [9, 18, 27, 40]. The items for perceived EDI performance were formulated from the objectives of EDI usage. Reinforcement of ties with a business partner, improved customer service, cost reduction and increased reliability of information were the most important benefits expressed by the majority of respondents.

Three variables in this study were considered in order to capture some of the key benefits that are attributable to

Table 2 Measurement of variables

Latent variable	Construct	Description of items
Internal formal controls	Internal application controls (IFC1)	System login is appropriately controlled by access control procedures such as passwords (IFC1_1)
		Systems are changed only through authorization from the responsible managers (IFC1_2)
		Physical access to the computer room is appropriately controlled (IFC1_3)
		Only authorized personnel can access to the EDI system (IFC1_4)
		File retention policy is effectively applied to all transactions received or generated (IFC1_5)
		Unauthorized access to EDI transactions is effectively controlled (IFC1_6)
	Internal communication controls (IFC2)	EDI messages are checked for duplication, omission or inaccuracy before they are transmitted (IFC2_1)
		EDI messages are checked for duplication, omission or inaccuracy after they are received (IFC2_2)
Third-party formal controls	Third-party communication controls (TFC1)	Third-party network has an appropriate "help desk function" that ensures continuity of service in a timely manner (TFC1_1)
		Third-party network ensures that each message is interchanged with trading partner without excessive delay (TFC1_2)
		Third-party network promptly provides appropriate recovery procedures in the event of network or computer failure (TFC1_3)
		Third-party network ensures that message errors, loss, and duplication are detected before damage occurs (TFC1_4)
		Third-party network automatically tracks and reports the status of message communication (TFC1_5)
	Third-party network service (TFC2)	Third-party network provides appropriate network infrastructure to implement the EDI system (TFC2_1)
		Third-party network supports connections with diverse environments through various protocol conversion services (TFC2_2)
		Third-party network supports connections with diverse environments through providing various message standards (TFC2_3)
Knowledge of control contents	Learning from education (KCO1)	Employees receive appropriate education to be aware of their job content when they are given new task (KCO1_1)
		The technical advice, guidance, and problem solving knowledge that are provided from external institutions are well recognized by all EDI staff members (KCO1_2)
	Learning from experience (KCO2)	EDI staff members can cope promptly with errors in EDI messages using their own experience (KCO2_1)
		EDI staff members frequently cooperate with colleagues to get help while correcting errors (KCO2_2)
Knowledge of control importance	Learning the effect of control deficiency (KIM1)	EDI staff members know which control procedures should be applied strictly for overall system security (KIM1_1)
		EDI staff members are aware of vulnerabilities arising from communication with the third-party network, vendors, and other institutions (KIM1_2)
	Understanding job responsibility (KIM2)	EDI staff members clearly recognize the importance of their responsibility as it affects the performance of other departments (KIM2_1)
EDI performance	Process improvement (PER1)	Internal transaction processing time is greatly reduced after EDI adoption (PER1_1)
		Work process is a functioning smoothly after EDI adoption (PER1_2)
		Requirement of manpower is reduced significantly after EDI adoption (PER1_3)
	Work efficiency (PER2)	Paper work is greatly reduced after EDI adoption (PER2_1)
		Administration cost is greatly reduced after EDI adoption (PER2_2)
		Clerical error is greatly reduced after EDI adoption (PER2_3)
		Making accurate reports for managerial decision support is facilitated after EDI adoption (PER2_4)
	Relation improvement (PER3)	Customer service is greatly improved after EDI adoption (PER3_1)
		Our company improved trust in relations with trading partners after EDI adoption (PER3_2)
		Transportation cost is greatly reduced after EDI adoption (PER3_3)
		Product or service delivery time is greatly reduced after EDI adoption (PER3_4)

EDI: process improvement, work efficiency and improved relations. Process improvement indicates the extent to which the time and manpower needed to exchange information or process EDI tasks is reduced. Work efficiency represents the extent to which the clerical errors and costs inherent in paper systems are reduced and the accuracy of information is improved. Relations improvement indicates the extent to which the relationship with trading partners improves through shorter response times, lower transportation costs and increased information accuracy. Three items for process improvement and four items for work efficiency and relation improvement, all on seven-point Likert-type scales, were used to assess EDI performance. For example, one item under improved relations was, "Our company improved trust in relations with trading partners after EDI adoption." Respondents selected a response reflecting the extent to which they agreed or disagreed with the statement. The final score for each multi-item measure was the average of the item scores in the measure.

4.4 Procedures

The items were pilot tested extensively with EDI practitioners in ten different organizations prior to administration of the large-scale survey. The participants in the pilot test responded to the initial versions of the items and participated in detailed interviews to improve the quality and readability of the items. The extent to which practitioners felt that they possessed the knowledge necessary to provide appropriate responses was evaluated, and some aspects (such as the sequence and wording of questions) were modified to have more straightforward meanings and to elicit the correct responses for the same underlying construct. All ten practitioners were then interviewed, and a final review was made by four IS professors. This phase helped significantly to refine items and generate reasonable content validity. The questionnaire was answered by EDI staff or managers who were believed to have sufficient knowledge of EDI implementation.

5 Results

The research model depicted in Fig. 1 was analyzed using a structural equation modeling approach. This enabled the researcher to test the relationships within the measures (the measurement model) and the hypothesized relationships (the structural model).

5.1 Measurement properties

The content validity of the items was established through the adoption of constructs that had been validated by other researchers and a pretest with 10 IS professionals. Furthermore, extensive precautions were taken during the early stages of development and pilot testing of the items.

As a result of a separate exploratory factor analysis of the items that measured the EDI controls and related knowledge and of the items for EDI performance, the items for formal controls, knowledge, and performance converged on appropriate constructs for latent variables, as originally envisaged. Items with factor loading values lower than 0.5 were deleted from further analysis. The results generally show that each item loaded higher on its associated construct than any other variable.

The properties of the measurement model were assessed to examine the reliability and validity of the variables. Each item in the initial measurement model was reviewed and, based on the results of a principal component analysis, the items that loaded on multiple constructs or had low item-to-construct loading were deleted. After items and constructs for each latent variable were determined, confirmatory factor analysis was performed.

Figure 2 presents the measurement model. The measures exhibited moderate or high reliability, as the composite reliability ranged from 0.61 to 0.94 (see Table 3). The reliability of the variables was also assessed using Cronbach's alpha. Cronbach's alphas for five multi-item constructs were above or slightly below 0.7, indicating that the scales were internally consistent and reasonably free of measurement error. The average variance extracted for all latent variables exceeded or was slightly below 0.5, and all of the estimated parameters of individual item were significant, indicating high convergent validity [2]. The high values of reliability scores and significant parameter estimates show the proper convergent validity of the variables.

Table 4 shows the discriminant validity of the study measures. The intercorrelations among latent variables do not exceed the square root of the average variance extracted, except for the correlation between internal application controls and knowledge of control importance. For these two latent variables, further study confirmed that the constructs load higher on their associated latent variable than on any other variable.

The correlation between latent variables must be significantly lower than unity in order to achieve discriminant validity. This requires a comparison between one model, where the correlation between these latent variables is not constrained to unity (the correlation is freely estimated), and another model where the same correlation is constrained to unity. A significantly higher χ^2 value for the constrained model versus the unconstrained model can indicate support for discriminant validity [62]. The χ^2 difference, 5.54, is significant ($p < 0.05$). Hence, this indicates that the correlation between the latent variables is

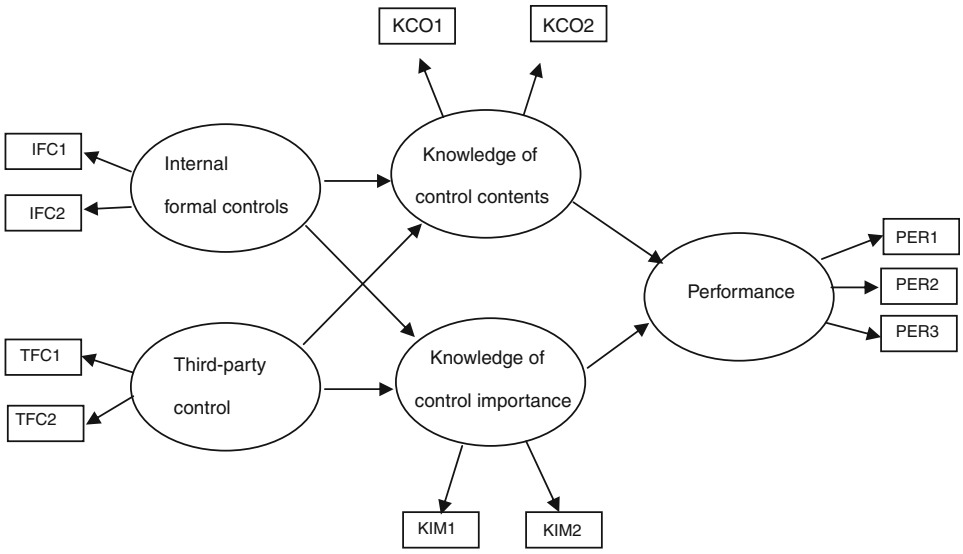

Fig. 2 Measurement and structural model

Table 3 Reliability and convergent validity of measures

Latent variable	Construct	Parameter estimate	*t*-Value	Individual item reliability	Composite reliability	Average variance extracted
Internal formal controls	Internal application controls (IFC1)	0.55	6.21	0.88	0.61	0.44
	Internal communication controls (IFC2)	0.77	8.13	0.90		
Third-party formal controls	Third-party communication controls (TFC1)	0.94	12.95	0.87	0.94	0.88
	Third-party network service (TFC2)	0.93	13.71	0.75		
Knowledge of control content	Learning from education (KCO1)	0.73	9.53	0.79	0.83	0.72
	Learning from experience (KCO2)	0.95	12.98	Not applicable		
Knowledge of control importance	Learning the effect of control deficiencies (KIM1)	0.81	10.55	0.69	0.73	0.57
	Understanding job responsibility (KIM2)	0.70	8.90	0.67		
EDI performance	Process improvement (PER1)	0.76	10.24	0.81	0.84	0.64
	Work efficiency (PER2)	0.84	11.57	0.88		
	Relation improvement (PER3)	0.80	10.90	0.80		

Table 4 Intercorrelations among constructs (the diagonals represent the square root of the average variance extracted)

Latent variables	(1)	(2)	(3)	(4)	(5)
Internal formal controls (1)	0.67				
Third-party formal controls (2)	0.41	0.94			
Knowledge of control content (3)	0.62	0.46	0.85		
Knowledge of control importance (4)	0.78	0.52	0.76	0.76	
EDI performance (5)	0.43	0.45	0.32	0.41	0.80

significantly lower than unity. These results show that the measurement model had discriminant validity and that it properly fit the data.

5.2 Test of hypotheses

Structural equation modeling was used to test the research propositions. The research model specifies the existence of an intervening variable (knowledge of controls) between the antecedent variables (internal formal controls, third-party controls) and the consequent variable (performance). Figure 2 shows the structural and measurement models. The structural model indicates the existence of indirect effects between an antecedent variable and its consequent variable. The findings indicate that the structural model provides a good model for the data set. The goodness of fit index (GFI) is 0.930, which is larger than the 0.9 usually

considered reasonable [29]. Although the value of χ^2 is significant, all other fit indices are within the range suggestive of a good model fit.

As indicated in Fig. 2, most path coefficients are as hypothesized. Path coefficients and their significance are shown in Table 5. The paths represent *direct* and *indirect* effects depending on whether they mediate other variables. The paths from formal controls (internal and third-party) to knowledge of controls (content and importance) are significant. The path from knowledge of controls content to performance is also significant, which leads to a significant indirect effect of controls on performance.

Each of the paths in the full model (Fig. 1) was constrained to zero in order to test the four hypotheses concerning indirect effects of controls. For instance, the first submodel tests whether internal formal controls affect performance through their effect on knowledge of control content. The path from internal formal controls to knowledge of control importance was fixed at zero to test Hypothesis 1-1. Four constrained sub-models were used suggested to test the indirect effect of controls on performance through their effect on each construct of knowledge of controls. The constrained models to test Hypotheses 1-1, 1-2, 2-1, and 2-2 were as follows:

(1) Submodel 1: the path from internal formal controls to knowledge of control importance was fixed at zero.
(2) Submodel 2: the path from internal formal controls to knowledge of control contents was fixed at zero.
(3) Submodel 3: the path from third-party controls to knowledge of control importance was fixed at zero.
(4) Submodel 4: the path from third-party controls to knowledge of control contents was fixed at zero.

Table 6 shows that the indirect effects of internal formal controls and third-party controls on performance through knowledge of control content and importance were all significant, which supports Hypotheses 1-1, 1-2, 2-1 and 2-2. Knowledge of control content and importance were both all critical to the effectiveness of internal formal controls and third-party controls. The standardized effect can be used to compare the relative strength of each effect. The indirect effect of third-party controls through knowledge of control importance is the highest, and this indicates that EDI staff members should understand the importance

Table 5 Causal effects between formal controls, knowledge, and performance in the full model

Causal path	Direct or indirect effect	MLE	Standardized coefficient	*t*-Value
Internal formal controls → knowledge of control contents	Direct effect	0.945	0.897	4.693**
Internal formal controls → knowledge of control importance	Direct effect	1.172	0.786	5.074**
Third-party formal controls → knowledge of control contents	Direct effect	0.414	0.588	5.571**
Third-party formal controls → knowledge of control importance	Direct effect	0.411	0.412	5.260**
Knowledge of control contents → performance	Direct effect	1.444	1.049	2.129*
Knowledge of control importance → performance	Direct effect	−0.594	−0.611	−1.182
Internal formal controls → performance	Indirect effect	0.669	0.461	3.851**
Third-party formal controls → performance	Indirect effect	0.354	0.365	4.887**

MLE maximum likelihood estimate

* $p < 0.05$, ** $p < 0.01$)

Table 6 Indirect effects of formal controls on performance in constrained submodels

Submodel Model	Indirect effect	Standardized effect	*t*-Value
Submodel Model 1	The indirect effect of internal formal controls on performance through knowledge of control content (H1-1)	0.272	2.91**
Submodel Model 2	The indirect effect of internal formal controls on performance through knowledge of control importance (H1-2)	0.239	2.56*
Submodel Model 3	The indirect effect of third-party controls on performance through knowledge of control content (H2-1)	0.366	4.12**
Submodel Model 4	The indirect effect of third-party controls on performance through knowledge of control importance (H2-2)	0.380	4.16**

* $p < 0.05$, ** $p < 0.01$

of third-party controls in order to improve control effectiveness by determining the most important functions to be provided by third-party controls.

6 Discussion

The results indicate that the application of formal controls and the level of knowledge are strongly related. Using internal formal and third-party controls requires some knowledge of these controls in terms of their content and importance. Many IS technologists in particular put less importance on the social and business aspects of security and controls and assume that their technology will operate in a benign rather than a hostile environment [47]. As loss situations occur infrequently and security does not appear to increase productivity or performance, EDI staff members are likely to be unaware of the need for being alert to loss and of their responsibility for security. The risks and consequences of losses and control deficiencies in internal applications, at the communication interface, on the VAN, or in the details of control procedures should be clearly understood by EDI staff members. This enhances their skills, attentiveness, care and positive motivation. Otherwise, adherence to existing controls, and their effect on system performance, becomes lower. When EDI staff members are aware of the vulnerabilities arising from communication with a third-party network, vendors or other institutions, they are better prepared for unexpected risks and actively apply control procedures such as contingency planning, making backup files and leaving an audit trail.

The adoption of complex technology includes a process of reducing knowledge barriers. Building up the necessary skill set is a key issue for many innovation-adopting organizations considering that the lack of a skilled labor force lowers the probability of success in implementing EDI [13]. EDI controls which increase the potential for EDI implementation success require a satisfactory level of competence in control technologies [38]. For instance, continuous process monitoring using techniques such as embedded audit modules can immediately identify and resolve critical problems as they occur. The full implementation of automated controls requires extensive expertise and expense [34]. Formal controls should include the planning, implementation, and operation of these technical controls, which demands expertise in these concurrent audit techniques or integrated test facilities. Organizations that have a high degree of knowledge of controls do not have to seek specialists outside the company to fulfill control requirements and can maintain adequate quality in establishing safeguards against various threats. Knowledgeable EDI staff members constitute a high-quality resource in the development of EDI controls.

The relationship between third-party controls and knowledge of controls indicates that sufficient expertise and commitment should exist to ensure the security of data in transit, either mail boxed with a third-party network provider or en route to the trading partner. As a large portion of the control procedures are provided by the third-party, significant risk can arise from this company. For instance, third-party staff could introduce invalid or unauthorized transactions, causing inaccurate financial reporting, wasted production and other business losses [9]. Transactions that leave the corporate entity may not be subject to the same security procedures, but EDI staff should be aware of the cross-vulnerabilities and understand which control procedures should be enforced strictly by the third-party for overall system security. If EDI managers detect major differences in philosophy (necessity, objective, priority of controls) with third-party network providers over security issues, they should ensure that they are resolved or at least understood.

7 Conclusions and implications

This study integrated a theoretical perspective and the empirical findings of research on IS security, EDI management and controls and proposed and tested a structural equation model examining the role of knowledge in the relation between formal EDI controls and EDI performance. The purpose of this study was to separate EDI controls and knowledge of controls and to investigate the effect of the former through the latter on performance from a social and behavioral perspective. To verify the relationship between formal controls and knowledge, it is proposed that these have their own factors representing the multidimensional aspects of these concepts. The results indicate that knowledge plays an important mediating role in the effectiveness of controls; that is, EDI adopters can achieve operational and competitive benefits from a high level of knowledge of control contents and importance. The findings provide a number of implications for research and practice.

7.1 Implications for practice

EDI controls have emerged as one of the critical issues facing EDI adopters. They signify the need for a better understanding of the control structures that lead to benefits from EDI. The results of this study indicate the importance of knowledge management within the context of IS security and controls. EDI practitioners should possess knowledge to identify, solve and broker new or routine security and control problems. EDI management should also pay attention to "tacit" knowledge—something not easily

visible and expressible, that are often accumulated from experience and informal interaction. This subjective and intuitive knowledge of EDI security helps EDI staff members have the values, responsibility, commitment and capability needed in their security-related behavior.

Managers should stimulate brainstorming, cooperation, and interaction among employees to enhance commitment and internalize the learning that takes place from other institutions or skills shared with others. The sense of responsibility is enhanced when EDI staff members are highly aware of control importance and vice versa. Management should focus on aspects of responsibility in planning security measures, such as employee morale monitoring, clear job descriptions and expectations, and separation of duty in input, operation, programming and output duties [5]. Organizations that make training available in EDI and security tools achieve greater levels of EDI sophistication and performance. Organizations can implement basic levels of EDI with little training, but the development and management of the advanced features of EDI demands training. User training, a typical method of knowledge management, is considered to be one of the critical factors that reduce resistance to change and subsequently lead to system success. EDI-specific studies have validated the usefulness of user training as it affects successful implementation of EDI systems.

Management can also define the scope of action privileges that limit the user's authority level and the type of resources authorized for use. An authorization matrix may be made, which shows the authorization function in terms of a matrix where the rows and columns represent users and resources, respectively, and the elements show the action privileges that each user possesses regarding each resource [63]. At that point, management should identify persons ("asset owners") who are responsible for every specified resource. Holding individuals personally responsible increases their perception of the importance of the controls as well as their sense of responsibility.

Identifying a comprehensive list of the assets (personnel, hardware, software, data) that exist in the computer installation and valuing them may develop users' sensitivity to the possible consequences of a security threat [63], and designing a control matrix, a matrix conceptualization of controls that reduces expected losses (with columns that represent causes of loss and rows that indicate controls exercised over the causes) may help to show the importance of controls in reducing the expected loss from each cause. The results of asset valuation will help to identify what expenditure on controls can be justified. This should be accompanied by other security management steps (identification and assessment of threats and vulnerabilities) and risk analysis in order to examine control importance accurately in terms of the expected losses that controls can reduce. The effectiveness of controls will improve after existing controls are modified or when new controls are implemented to enhance their overall benefit.

7.2 Implications for research

Given the relative newness of the academic literature on EDI controls, this study provides a theoretical framework that should allow future studies to examine the relations among formal controls, informal aspects of controls (knowledge in this study) and performance. The two dimensions of knowledge suggested here can be divided into several additional dimensions; for instance, knowledge of control content may be further segmented into knowledge regarding controls on IS design, implementation and operation; or regarding controls on applications such as production, accounting, logistics and marketing. It would be interesting to examine the different effects of the corresponding knowledge on performance. A study investigating organizational and IS characteristics that could stimulate knowledge generation in EDI security and controls is needed. Knowledge is supposed to emerge out of a complex process involving social, situational, cultural and institutional actors. A conceptual structure for understanding and enhancing the management of EDI controls can be further examined in terms of organizational culture and its effect on controls and knowledge management. For instance, reliance on trust leads to trading partners establishing cooperative IORs (Interorganizational Relations) without the use of formal contracts and safeguards [50]. As trust is further affirmed, formal controls are used less and the demand for accurate and reliable knowledge becomes greater, as it may complement or substitute for formal contractual safeguards.

Another future line of research would be to extend the proposed framework to other IS innovations. It is important to investigate whether existing research frameworks can be applied and generalized in different IS contexts or to different dependent variables, such as implementation or computer abuse intentions. Additional factors are needed in the theoretical model. For instance, organizational learning and politics are important factors for the successful implementation of e-mail [52]. The potential social effects of the implementation, including its effect on power distribution and the negotiation process between management and employees, should be considered in the implementation and (of course) control of e-mail.

When the variable is computer abuse judgment, the psychological trait of responsibility denial is a critical factor [23]. Researchers must use a multifaceted approach to IS controls for individual or organizational level studies based on various theories such as deterrence, agency, motivation theory or innovation-diffusion theory.

Acknowledgment This research was supported by WCU (World Class University) program through the National Research Foundation of Korea funded by the Ministry of Education, Science and Technology (Grant No. R31-2008-000-10062-0).

References

1. Albrecht CC, Dean DL, Hansen JV (2005) Marketplace and technology standards for B2B e-commerce: progress, challenges, and the state of the art. Inf Manag 42:865–875
2. Anderson J, Gerbing D (1988) Structural equation modeling in practice: a review and recommended two-step approach. Psychol Bull 103(3):411–423
3. Attewell P (1992) Technology diffusion and organizational learning: the case of business computing. Organ Sci 3(1):1–19
4. Banerjee S, Golhar DY (1994) Electronic data interchange: characteristics of users and nonusers. Inf Manag 26:65–74
5. Baskerville R (1988) Designing information systems security. Wiley, Chichester, UK
6. Benesko G, Teplitzky P (1994) Security and controls for EDI. Inf Syst Secur Summer:15–19
7. Benesko G, Teplitzky P (1995) EDI integrity controls. Inf Syst Secur Winter:21–25
8. Blumstein A, Cohen J, Nagin D (1978) Deterrence and incapacitation: estimating the effects of criminal sanctions on crime rates. National Academy of Sciences, Washington, DC
9. Chan S, Govindan M, Picard JY, Leschiutta E (1993) EDI for managers and auditors. Electronic Data Interchange Council of Canada, Toronto, ON
10. Chircu A, Kaufman RJ (2000) Reintermediation strategies in business-to-business electronic commerce. Int J Electron Commerce 4(4):7–42
11. Chwelos P, Benbasat I, Dexter AS (2001) Research report: empirical test of an EDI adoption model. Inf Syst Res 12(3):304–321
12. Computer Security Institute (CSI) (2008) CSI/FBI computer crime and security survey. CMP Media LLC. http://www.gocsi.com/forms/csi_survey.jhtml
13. Crook CW, Kumar RL (1998) Electronic data interchange: a multi-industry investigation using grounded theory. Inf Manag 34:75–89
14. Davenport TH, Klahr P (1998) Managing customer support knowledge. Calif Manag Rev 40(3):195–208
15. Dhillon G, Backhouse J (1996) Risks in the use of information technology within organizations. Int J Inf Manag 16(1):65–74
16. Dodgson M (1994) Organizational learning: a review of some literatures. Organ Stud 14(3):375–394
17. Down A (2002) Integrating EDI systems across and beyond your enterprise. IBM White Papers, Somers, NY (available at www-3,ibm.com/software/integration/wdi/library/whitepapers/edi_v1c.pdf)
18. Emmelhainz MA (1990) Electronic data interchange: a total management guide. Multiscience Press, Inc, Van Nostrand Reinhold, New York
19. Frank J, Shamir B, Briggs W (1991) Security-related behavior of PC users in organizations. Inf Manag 21:127–135
20. Guha S, Grover V, Kettinger WJ, Teng JTC (1997) Business process change and organizational performance: exploring an antecedent model. J Manag Inf Syst 14(1):119–154
21. Hamel G, Prahalad CK (1994) Competing for the future. Harv Bus Rev 72(4):122–132
22. Hammer M (1990) Reengineering work: don't automate, obliterate. Harv Bus Rev July–August:104–112
23. Harrington SJ (1996) The effect of codes of ethics and personal denial of responsibility on computer abuse judgments and intentions. MIS Q 20(September):257–278
24. Hart P, Saunders C (1997) Power and trust: critical factors in the adoption and use of electronic data interchange. Organ Sci 8(1):23–42
25. Hedrick A (2001) Reports of EDI's death were premature. AMR Research, Sunday, July 01 (available at www.amrresearch.com/Content/view.asp?pmillid=13446&docid=577)
26. ISACA (1990) EDI control guide. Information Systems Audit Control Association, EDI Council of Australia, Sydney Chapter
27. Jamieson R (1994) EDI: an audit approach. The EDP Auditors Foundation, Inc., Rolling Meadows, IL
28. Jaworski BJ (1988) Toward a theory of marketing control: environmental context, control types, and consequences. J Mark 52(July):23–39
29. Joreskog KG, Sörbom D (1989) LISREL 7: a guide to the program and applications, 2nd edn. SPSS Inc., Chicago, IL
30. Joseph GW, Blanton JE (1992) Computer infectors: prevention, detection, and recovery. Inf Manag 23:205–216
31. Kanakamedala K, King J, Ramsdell G (2003) The truth about XML. McKinsey Q 3:9–13
32. Kaefer F, Bendoly E (2004) Measuring the impact of organizational constraints on the success of business-to-business e-commerce efforts: a transactional focus. Inf Manag 41:529–541
33. Kuan KKY, Chau PYK (2001) A perception-based model for EDI adoption in small businesses using a technology-organization-environment framework. Inf Manag 38:507–521
34. Lawrence CM (1988) Usage of concurrent EDP audit tools. EDP Audit J 3(Fall):49–54
35. Lee S, Han I (2000) Fuzzy cognitive map for the design of EDI controls. Inf Manag 37:37–50
36. Lee KC, Lee S (2007) Causal knowledge-based design of EDI controls: an explorative study. Comput Hum Behav 23(1):628–663
37. Lee S, Ahn H (2009) Structural equation model for EDI controls: controls design perspective. Expert Syst Appl 36(2) (Part 1):1731–1749
38. Lee S, Han I, Kym H (1998) The impact of EDI controls on EDI implementation. Int J Electron Commerce 2(4):71–98
39. Liang H, Xue Y, Byrd TA, Rainer RK (2004) Electronic data interchange usage in China's healthcare organizations: the case of Beijing's hospitals. Int J Inf Manag 24:507–522
40. Marcella JA, Chan S (1993) EDI security, control, and audit. Artech House Inc., Norwood, MA
41. McGowan MK, Madey GR (1998) The influence of organization structure and organizational learning factors on the extent of EDI implementation in U.S. firms. Inf Resour Manag J 11(3):17–27
42. Mehrtens J, Cragg PB, Mills AM (2001) A model of Internet adoption by SMEs. Inf Manag 39:65–176
43. Mount I (2003) Why EDI won't die. Business 2.0 Magazine, August 1 (available at www.business2.com/b2/subscribers/articles/0,17863,515887-1,00.html)
44. Nakayama M (2003) An assessment of EDI use and other channel communications on trading behavior and trading partner knowledge. Inf Manag 40:563–580
45. Ngai EWT, Wat FKT (2002) A literature review and classification of electronic commerce research. Inf Manag 39:415–429
46. Nonaka I, Takeuchi H (1995) The knowledge-creating company: how Japanese companies create the dynamics of innovation. Oxford University Press, New York
47. Parker DB (1994) A guide to selecting and implementing security controls. Inf Syst Secur Summer:75–86
48. Pearson FS, Weiner NA (1985) Criminology: toward an integration of criminological theories. J Crim Law Criminol 76(1):116–150
49. Ramamurthy K, Premkumar G (1995) Determinants and outcomes of electronic data interchange diffusion. IEEE Trans Eng Manag 42(4):332–351

50. Ring PS, Van de Ven AH (1994) Developmental processes of cooperative interorganizational relationships. Acad Manag Rev 19(1):90–118
51. Rogers EM (1983) Diffusion of innovations. The Free Press, New York
52. Romm CT, Pliskin N, Rifkin WD (1996) Diffusion of E-mail: an organizational learning perspective. Inf Manag 31:37–46
53. Ropponen J, Lyytinen K (1997) Can software risk management improve system development: an exploratory study. Eur J Inf Syst 6:41–50
54. Sánchez AM, Pérez MP (2005) EDI and moderating effect of interorganizational cooperation in the supply chain. J Organ Comput Electron Commerce 15(2):83–104
55. Senn AJ (1998) Expanding the reach of electronic commerce: the Internet EDI alternative. Inf Syst Manag Summer:7–15
56. Sia SK, Neo BS (1997) Reengineering effectiveness and the redesign of organization control: a case study of the inland revenue authority of Singapore. J Manag Inf Syst 14(1):69–92
57. Smith AD (2005) Accountability in EDI systems to prevent employee fraud. Inf Syst Manag 22(2):30–38
58. Soliman KS, Janz BD (2004) An exploratory study to identify the critical factors affecting the decision to establish Internet-based interorganizational information systems. Inf Manag 41:697–706
59. Son JY, Narasimhan S, Riggins FJ (2005) Effects of relational factors and channel climate on EDI usage in the customer–supplier relationship. J Manag Inf Syst 22(1):321–353
60. Teo HH, Wei KK, Benbasat I (2003) Predicting intention to adopt interorganizational linkages: an institutional perspective. MIS Q 27(1):19–49
61. Ulfelder S (2004) B2B exchange survivors. Computerworld (available at www.computerworld.com/managementtopics/ebusiness/story/0,10801,89568,00.html), February 2, 12:00 PM ET
62. Venkatraman N, Ramanujam V (1987) Planning system success: a conceptualization and an operational model. Manag Sci 33(6):687–705
63. Weber R (1999) Information systems control and audit. Prentice Hall Inc, Upper Saddle River
64. Wiig KM (1997) Knowledge management, where did it come from and where will it go. Expert Syst Appl 13(1):1–14
65. Witte CL, Grunhagen M, Clarke RL (2003) The Integration of EDI and the Internet. Inf Syst Manag 20(4):58–65
66. Zviran M, Haga WJ (1999) Password security: an empirical study. J Manag Inf Syst 15(4):161–185