ARTICLE IN PRESS

Discrete Applied Mathematics ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Discrete Applied Mathematics

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

Mathematical model-based security management framework for future ICT outsourcing project

Jewook Moon [a], Chanwoo Lee [b], Sangho Park [b], Yanghoon Kim [c], Hangbae Chang [d,*]

[a] Markany, Republic of Korea

[b] Department of Security Convergence, Graduate School, Chung-Ang University, Republic of Korea

[c] Department of Cyber Security, Far East University, Republic of Korea

[d] Department of Industrial Security, College of Business and Economics, Chung-Ang University, Republic of Korea

ARTICLE INFO

Article history:
Received 16 April 2015
Received in revised form 31 December 2015
Accepted 19 March 2016
Available online xxxx

Keywords:
Mathematical model
ICT outsourcing
Security management
Security management framework

ABSTRACT

The information communication technology (ICT) outsourcing market is growing larger every year from the increasing number of companies that utilize ICT outsourcing, as industry scale increases and industrial specialization intensifies. However, the current circumstance is that security accidents related to ICT outsourcing are continuously occurring at an increasing scale. There is a lack of studies measuring the level of security management of organizational ICT outsourcing, which is the first step in performing security management of ICT outsourcing. In addition, most studies focus on general organizational security management. Accordingly, this paper aimed to design a model to measure the level of security management of companies utilizing ICT outsourcing. Specifically, this paper analyzed security vulnerabilities that could occur in ICT outsourcing that may be mapped with the accorded security measures as solutions to deduce items for ICT outsourcing security inspections. Next, this paper developed an ICT outsourcing security level quantification model by verifying the validity of the security inspection items deduced and by estimating item-specific weighted points. Additionally, the applicability of the ICT outsourcing security level quantification model developed was verified by applying it to actual companies.

1. Background of the study

The effort to gain a competitive advantage in various industries from rapid advancements of industrial technologies is increasing. As a main tool for competitive advantages, a combination of industry and information communication technology (ICT) is becoming an essential operating factor of industrial advancement.

To establish and continue ICT operations, organizations require significant professional labor and technological prowess. However, ICT is not the main business of most organizations and the significant cost needed to obtain significant professional labor and technological prowess is an issue. Additionally, developing and operating ICT with a company's own labor and technological prowess alone is difficult. Accordingly, "ICT outsourcing" is utilized in most cases. Recently, the number of cases of companies that concentrate on their core competencies while entrusting an ICT resource that is not a core

* Corresponding author.
E-mail addresses: paulmoon721@naver.com (J. Moon), chanlee@gmail.com (C. Lee), indsec2015@gmail.com (S. Park), yhkim@kdu.ac.kr (Y. Kim), hbchang@cau.ac.kr (H. Chang).

http://dx.doi.org/10.1016/j.dam.2016.03.013
0166-218X/

Please cite this article in press as: J. Moon, et al., Mathematical model-based security management framework for future ICT outsourcing project, Discrete Applied Mathematics (2016), http://dx.doi.org/10.1016/j.dam.2016.03.013

competency by breaking away from simply improving internal operational efficiency is increasing [9]. Accordingly, the perception of ICT outsourcing is changing given the effort to gain industrial competitiveness. The ICT outsourcing market is continuously growing as a result of the increasing and expanding scope of ICT outsourcing.

Utilizing outsourcing for ICT development and operations results in reducing a company's ICT investment and maintenance costs [1,5]. The issue of increasing security vulnerability exists – in contrast to when internal labor is utilized for ICT development and operations – because such vulnerabilities increase from bringing in and taking out unauthorized equipment and increasing the number of people that can access information. In this regard, security accidents from ICT outsourcing have been increasing recently, which calls for extensive security management of outsourcing. Accordingly, this paper aims to design a model to measure the level of security management for companies utilizing ICT outsourcing. Specifically, this paper analyzes security vulnerabilities that could exist in ICT outsourcing that may be mapped with the accorded security measures to design a system for ICT outsourcing security management.

2. Previous studies

Karabulut, Kerschbaum, Massacci, Robinson and Yautsiukhin [7] focus on the problem of guaranteeing appropriate security when storing data on a contractor's server. They introduce several important definitions and identify a number of challenges and issues. They argue that external metrics are more meaningful for a client and propose some that can be used for PLA. In their article, they focus more on the technical side of the agreement. One problem that they omit is the issue of enforcement, which must be considered before applying PLA as a contract.

Hamlen and Thuraisingham [3] discuss various security challenges for outsourcing both data management and software development activities. In particular, their paper discusses security issues pertaining to the data-as-a-service and software-as-a-service models, and supply chain security issues. They also present relevant standards for data outsourcing. Their goal is for the composite system to be secure even if the individual components developed by multiple organizations might be compromised. They argue that data production has numerous similarities to developing a product in the supply chain process, and data must be shared securely in the outsourcing process. In addition, security concerns for mobile code in service-oriented architectures motivate the realization of security itself as a service.

Sherwood [14] examines the main issues concerning the security of business information in outsourced systems and networks. He reviews the strategy that management should follow to ensure that its business information is adequately secured under such conditions during pre-contract negotiations and that must be integral to the outsourcing agreement.

Khalfan [4] presents an overview of a national case study that explores the information security considerations in information systems/information technology (IS/IT) outsourcing projects in the public and private sectors of Kuwait, where the data collection for this study was carried out. The author states that organizations need to exercise caution when selecting a partner (i.e., vendor). Additionally, organizations must properly and adequately address their security concerns as they establish and develop their security policies, which should be concise, effective, and cover all security layers. Outsourcing contracts should include robust provisions for information security, particularly in drafting the SLA. This study may provide good input to IT policy makers and managers in different sectors in Kuwait. The findings also provide insights into how, as an information system strategy, outsourcing practices are managed in the context of Kuwait.

Oladapo, Zavarsky, Ruhl, Lindskog, and Igonor [12] review and extract IT security risk elements that culminated in a flowchart to aid decision making with respect to IT security outsourcing. This research, which reviews the NIST overview approaches on IT security services acquisition and management, contributes to this area by conducting a more detailed study on the initiation phase of the information security services life cycle and by introducing a decision-making flowchart to complete this first phase of acquiring IT security services. This research will assist managers who need to make decisions around IT security outsourcing. Although this research is an initial attempt at analyzing this topic, it represents an interesting avenue for further studies in the expansion of other phases of the SDLC of outsourcing projects.

Zulkarnaen Khidzir, Mohamed, and Arshad [10] focus on conducting an empirical study on the relationship between the difficulties and practices of information security risk management (ISRM) in ICT outsourcing. The findings of their study show that the ISRM process difficulties influence the ICT outsourcing practices. These findings assisted in discovering the influence of the strength between the difficulties and practices of the information security risk management approach in ICT outsourcing projects. The findings reveal that risk treatment plan implementation and risk monitoring process difficulties could not influence the practices of private and government agencies with respect to their ICT outsourcing project implementations. Furthermore, the findings could encourage additional research to improve process adaptability by improving the usability and flexibility of the processes suitable for the ICT outsourcing environment. As a result, managing information security risks in ICT outsourcing becomes more effective through dedicated processes designed for information security risk management in ICT outsourcing.

Zhang, Borisov, and Yurcik [17] analyze the logs used for security analysis with a concern for privacy and propose constraints on the anonymization of security monitor logs. They believe that if the anonymization solution fulfills the constraints, managed security services providers (MSSPs) can efficiently detect attacks and simultaneously protect privacy. They propose a new architecture for outsourced security monitoring, in which anonymized logs are sent to a monitoring provider to protect the security and privacy of an organization. The new architecture can remove an important barrier to the use of MSSPs. Their studies show that our proposed architecture represents a promising approach for future security

Please cite this article in press as: J. Moon, et al., Mathematical model-based security management framework for future ICT outsourcing project, Discrete Applied Mathematics (2016), http://dx.doi.org/10.1016/j.dam.2016.03.013