Journal of Theoretical and Applied Information Technology
15th February 2019. Vol.97. No 3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A SOCIOMATERIALITY PERSPECTIVE ON INFORMATION SECURITY MANGEMENT IN ICT OUTSOURCING ENVIRONMENT

[1]KYUNG JIN CHA, *[2]HWA JONG KIM

[6] Professor, Kangwon National University, Department of Business Administration, South Korea

[2]Professor, Kangwon National University, Department of Computing and Communications Engineering, South Korea

E-mail: [1]kjcha7@kangwon.ac.kr, [2]hjkim@kangwon.ac.kr
*Corresponding author

ABSTRACT

Large scale ICT outsourcing allows enterprises to reduce ICT costs and procure their competitive advantage as it enables them to focus on core competences. Nonetheless, despite a recent outbreak of ICT adoption among companies; there is serious outsourcing-related concern in regards to data security, such as personal information leakages during IT outsourcing projects. Extant information security studies provide different frameworks to solve these security matters in outsourcing environment by stressing the need for application of information security vulnerability and willingness to comply with security systems analyses. However, several concerns arise as proposed measures only consider internal environment without considering partner or sub-supplier's internal culture. Furthermore, in most cases research is limited to discussing network control and systems supplements using the perspective of technical issues only. Subsequently there is no consideration for the nature of ICT outsourcing security environment which varies depending on size of an organization and complexity of outsourcing stages. Thus this conceptual study proposes new theoretical framework for information security management that concerns characteristics of ICT outsourcing, considers perspective of sociomateriality and aims at strengthening security capabilities in accordance with outsourcing types and organization's characteristics.

Keywords: *Management, Security, Human Factors, Theory*

1. INTRODUCTION

As ICT outsourcing enables enterprises to reduce costs and focus on their core competences its adoption has been increasing. In 2014 demand for new projects utilizing cloud computing, big data and mobility in Korean domestic ICT outsourcing market was increased by 4.6% and expected to reach 29 trillion 9.616 billion won [1]. In the private sector relative utilization of ICT outsourcing for Korean commercial banks and property insurance reached 43.6% and 86% respectively. Nonetheless, great damage is caused by serious security incidents, such as information leakage from sub-supplier companies. Even though companies now become more aware of possible security issues, ICT outsourcing specialists still can't find proper countermeasures for security issues and remain uncertain about the ways to consider security in ICT outsourcing.

According to [2] and [3] establishment and operation of information system through ICT outsourcing will come to 65%, which is quite lower if company utilizes internal resources (75%). Thus outsourcing environment appears to be more vulnerable in terms of security. In fact, analysis of recent information security incidents found that majority of them occurred in companies that utilize ICT outsourcing (Table 1) as a results of low security levels in outsourcing companies, increase of various security controls, inadequate equipment export and etc [4]. Nonetheless corporate security systems are built to mainly respond to outside attacks. According to [3], while companies invest into responding to outside attacks such as hacking, ICT outsourcing sub-supplier's security infrastructure has been analyzed to be very insufficient. Also there are difficulties in conducting physical formal inspection controls due to the lack of employees' awareness in sub-supplier companies. In addition, such systematic and physical administrative environment appears to be weak. In order to effectively respond to these vulnerabilities firm's internal security systems

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

should be structured differently. Thus establishment of guidelines becomes necessary for systematic security management, as it is crucial to consider both cultural characteristics and outsourcing environment in regards to development and operation processes.

Although recent studies on compliance with security systems have made some progress, they considered enterprise environment and security system's development. At the same time research on security levels improvement in ICT outsourcing according to organizational factors in outsourcing environment yet been conducted. Unlike company's internal information security, information security is conducted through physical, technical and managerial controls. However, in the case of ICT outsourcing environment, information security control is difficult to perform within a single place. Thus characteristics of outsourcing and information security from the environmental perspective should be recognized differently. Also, design of countermeasures and enterprise security systems should be conducted differently as well. Considering that, we propose new theoretical framework for information security management that considers ICT outsourcing characteristics and aims to enhance security capabilities according to outsourcing types and organizational characteristics. Consequently, as our research framework is suitable for the concrete and practical outsourcing environment, its results, through further theoretical verifications, can be potentially applied in production and operation processes.

Table 1: Security incidents in the ICT outsourcing environments (Kim et al.: [4])

Date& Organization	Operation Method	Information Leakage (due to)
(10.9) College	Entire system administration by sub-supplier	Installation of server hacking program by staff of sub-supplier's server maintenance department
(11.3) Capital	Security administration by sub-supplier	Access to important system by exploiting information of deleted USA Retirement Accounts
(11.4) Bank	Server management by sub-supplier	Computer network hacking through laptop of sub-supplier's employee
(11.9) Institution	E-passport issuing equipment system operation by external enterprise	Weekly transfer of personal information during period of identification of components to be replaced for passport issuing equipment
(11.9) District office	Computerized operations of District's certified family data managed by external enterprise	Loss of removable hard drive with residential information during computerization of certified family documents
(12.12) Company	Storage of client's information in sub-supplier's server management	Client's information distribution by employees of external sub-supplier
(13.12) Bank	Management of client's information by sub-supplier	Use of removable storage device and document output by employees of external sub-supplier

2. LITERATURE REVIEW

Information security is a safeguard of information and its critical characteristics [5]. It comprises activities, processes and controls of defending data, information and their infrastructure [6] from possible threats, their recognition and further execution of countermeasures [7]. Confidentiality, integrity and availability are core characteristics of information security. These characteristics safeguard information from security risks, prevent security incidents, ensure business continuity and minimize business damages [8].

Research on information security went through several development stages of technical, management and institutional waves [9]. After 2006, fourth wave in development of information security was introduced and regarded as "Security Governance" that put emphasis on management responsibilities and value creation through security [10]. From the organizational perspective, security management in Security Governance becomes important, and therefore enables achievement of more effective and efficient security since it deals with security at the governance-level through administrative security [11]. With such motion of physical, management and technical security systems development, another important flow in information security research can be observed. It concerns organizational features for improvement of employees' compliant behavior and willingness toward security systems. Such studies include perception-belief-preference-intention-behavior-based research that includes various theories [12-19] and were actively referenced by numerous researches. These studies discuss strategic approach for threats issues caused by ignorance, mistakes and deliberate behavior that becomes very useful. Nonetheless, in such studies by substituting variables in each theory, researchers identify influential factors that affect willingness to comply with security policies and end with suggestions for piecemeal measures (e.g. reward and punishment system, etc). Though same theory applies to the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

same influential factor, different results are obtained [20], [21], or influence of security policies in security compliance appears to be lower [22]. Such results are not influential and arouse suspicion, as well as they were judged to be difficult to apply in ICT outsourcing environment. Thus in this research we derive new antecedents and regulation/control variables that reflect ICT outsourcing environment in general information security framework considering past organizational and cultural characteristics.

Unlike information security, in ICT outsourcing research technological capabilities, organizational and management competences of sub-suppliers are presented through their IT capabilities [23], and for order companies-work experience, technical skills, financial resources, self-development [24], customer management skills [25] and etc. are offered through their IT capabilities as well. In addition, a recent study of [26] that regards competencies' complementarity of sub-suppliers and order companies was considered to be important to success of ICT outsourcing. Applying these capabilities to information security in ICT outsourcing environment, interaction of sub-suppliers, and order companies organizational information security might be influential in ICT outsourcing information security. In addition, in ICT outsourcing research stream important project types are treated as control variables. These variables are generally divided into IT consulting service, application development, application management, network installation and maintenance, data center operation an etc, and their analysis is conducted differently. Research on strategic relation development with partner companies in SI industry [27] determined that more than 80% of the ICT outsourcing project development work accounted for outsourcing partner companies and presented success elements of strategic partnership in accordance with Partnership Theory. By considering most important joint goals of long-term partnership as influential factors and analyzing threats of mutual goals conflicts, one long-term partnership was suggested to be applicable to information security issues.

Moreover, comparing to the discussed literature in the prior section; theoretical foundation of information security in the ICT outsourcing environment is far weaker, as most studies are practice-based, and theoretically supported research yet been conducted. In his research, [28] investigated outsourcing security levels through survey, analyzed security threats factors and conclusively presented a plan for improvement of security control levels in management, technical and physical domains. Nonetheless development of a system considering outsourcing environment from the security level direction through general government guide and enterprise security instructions seems to be difficult; as survey results didn't lead to security systems development. In the research on ICT outsourcing risk factors [29] presented very important information security threat risk factors in ICT outsourcing projects that are unauthorized modifications and access of information, its distraction, exploitation and leakage, ICT failure and system's error by surveying security officers and experts. Although risk factors were prioritized by experts, exclusive concentration on identified priority problems and inadequate concentration on possible vulnerabilities can lead to greater risks. Furthermore, in research on IT outsourcing companies' information security management conducted by [30] information security SLA was presented through analysis of information security management system BS 7799 and examination of its application examined by enterprises. Nonetheless, there are still limitations as vulnerabilities of project processes and various organizational characteristics were not taken into account.

3. THEORETICAL FRAMEWORK FOR INFORMATION SECURITY MANAGEMENT IN ICT OUTSOURCING

3.1 The Pattern of Security Incidents in the ICT Outsourcing Environment

Particularly in public and financial institutions ICT outsourcing is actively used, however information security incidents occur frequently. As a result, companies recognize the importance of security and seek security control measures. Nonetheless awareness of security importance in the ICT outsourcing environment that involves external employees and internal systems is still inadequate. In addition to security incidents discussed in Table 1, security incidents that do not have external exposure have been estimated to be much more abundant considering the decline in corporate foreign trust and recognition. Security incidents that are commonly found can be seen with the following patterns:

- ✓ Pattern 1 – Information leakage due to upload of project artifacts to web by employees of sub-supplier;

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- ✓ Pattern 2 – Internet sharing of project artifacts and corporate information through P2P by employees of sub-supplier;
- ✓ Pattern 3 – Information leakage after saving project artifacts of public institution's projects in the external storage device by employees of sub-supplier;
- ✓ Pattern 4 – Information leakage due to sub-supplier employees' awareness of how to access customer system and connect with customers' agents.

Although many organizations and agencies identified these patterns and researched various ways for enhancing information security, in most cases they cease at complementing system from the technical problem perspective and need for network control [31], [32], [33]. Thus, there are limitations in the ICT outsourcing environment, as it is very versatile due to size of organization and piecemeal complexity of outsourcing.

3.2 ICT Outsourcing Characteristics from the Information Security Perspective

Companies should recognize problems concerning various stakeholders that participate in ICT outsourcing and acknowledge that security incidents can be controlled and solved only within an enterprise. In general ICT outsourcing structure (Figure 1), when contract is made between order and sub-supplier companies, sub-supplier has a role of project manager and partner sub-supplier companies participate in outsourcing project together. Order company establishes Protection Level Agreement (PLA) with sub-supplier accordingly with security requirements and then sub-supplier with its partners define PLA again in individual manner.

Such ICT outsourcing environment is faced with many difficulties. In the cases when ICT service companies are subcontracted to other partner companies there are many difficulties because client's information security requirements have to be adjusted and fulfilled. Because of these subcontracting characteristics in ICT outsourcing (in SI industry), cases when access to internal information is permitted have been occurring frequently due to the improper system controls. Although conglomerates owning SI companies leave computer network management to subsidiary companies, these companies with 2 or 3 sub-suppliers trust computer network management and security to commercial companies. Thus information security characteristics of ICT outsourcing were determined as follows:

- ✓ Difficulties in ICT outsourcing due to security process adjustment and fulfillment as a result of collaborative work with various stakeholders
- ✓ Determinants of organizational security levels through interaction with information security in ICT outsourcing environment
- ✓ Need to access, examine and analyze necessary tasks of ICT outsourcing used in developing of company-wide systems due to security incidents
- ✓ Need for administrative powerful information security management in line with promotion plan and control, due to difficulties in centralized decision-making, as a result of various organizational configurations in outsourcing projects.

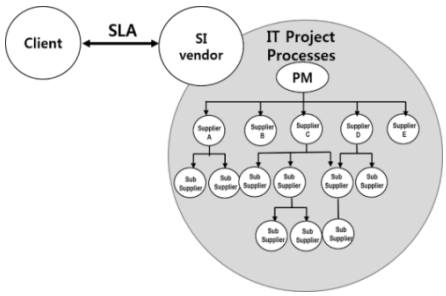

Figure 1: General ICT Outsourcing Security Structure

3.3 ICT Outsourcing Types from the Information Security Perspective

Integrated services in ICT outsourcing projects allows to build information systems in order to achieve company business goals by combining a number of factors related to the ICT [26]. ICT outsourcing types are very diverse in their complexity and scale regarding time spent for conducting outsourcing. In the case of full outsourcing there are risks of important internal corporate information leakage during project progress. Generally ICT outsourcing is divided into 4 broad types of IT consulting, IT system development and deployment, selective outsourcing and IT solution. Alternatively, by analyzing most frequently used outsourcing strategies in accordance with number of sub-suppliers (NSS), outsourcing periods(OP), relationship types(RT) and outsourcing extent(OE), [34] proposed 5 types(T) of outsourcing strategies divided according to strategic management perspective(SMP), economical perspective(EP), and social perspective(SP) (Table2).

Table 2: Outsourcing Strategy Classification

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Strategy		OE	RT	OP	NSS
SMO	T1	Total	Contract	Short-term	Single
EP	T2	Optional	Service-purchasing	Intermediate Term	Single
	T3	Total	Service-purchasing	Intermediate Term	Multiple
SP	T4	Total	Partnership	Long-term	Single
	T5	Total	Partnership	Long-term	Multiple

Looking at proposed IT project types from information security perspective, structure of outsourcing type from social perspective enables effectiveness maximization of information security. This type of outsourcing structure is developed accordingly to time spent on information security process between sub-supplier companies and order suppliers. In case of outsourcing combining total outsourcing and partnership relations, both organizations seek for overall process improvement. Particularly in partnerships; information security levels can be significantly improved by long-term planning availability through mutual trust. In the case of single order contracts without sub-supplying, it becomes easy to establish strong bond between two organizations. Nonetheless, there is a possibility to take advantage from expertise of each company if order companies work in collaboration with various partners, information security structure can still be weak regardless of possible benefits from such collaborative work.

3.4 Piecemeal Information Security Requirements of ICT Outsourcing

As Table 3 shows vulnerabilities of corporate information leakages may differ depending on stages of ICT outsourcing security management process. Therefore the purpose of this study is to investigate how information security requirements vary in their outsourcing stages. In addition, these information security requirements are being further reanalyzed in accordance with 3 principles of confidentiality, integrity and availability. Thus, this study aims at developing security strategy by discussing in details each outsourcing process and defining distinct security levels, as it is described in the Table 4.

3.5 Framework Implementation Using Sociomateriality Theory

Even though various vulnerabilities and risk factors are found in outsourcing types and process stages, in most organizations they are generated by people. As employees deal with security-related tasks frequently, their perception of information security is built upon individual organizational and technological factors [35],

Table 3: Information Security Vulnerabilities from Each Stage of Outsourcing Process

System Stage			
Development	**Establishment& Supplement**	**Operation & Disability Response**	**Contract Termination & Change**
Main Task			
Personal configuration development; Sub-supplier selection; Import of equipment; Selection of development site	Development and trial operation	Monitoring and updating; Disability response and management	Usage and internalization; Discussion of future upgrades
Information Flow			
Development and trial operation	Information generation and usage (examination, editing, transferring and etc.)	Information usage and supply (examination, editing, transferring and etc.)	Destruction of information
Vulnerabilities			
Absence of grading management for generated information; Threat of inappropriate system access; Uncertainty of security manager; Uncertainty in development zone's control unit; Unauthorized group access to virus equipment; Information leakage through RFI/RFP transfer	Lack of control in information access; Grant of unnecessary permission; Lack of regulations and guidelines for internal information leakage prevention; Lack of recognition of importance of internal information; Uncertainty in installation of security devices; Information leakage through PC's internet connection development	Information access control; Uncertain security awareness about main security issues; Spread of security incidents due to system manager's unawareness of first response countermeasures	Illegal usage by reclaiming and not destructing gathered information in the previous stage

Table 4: Information Threat Levels in Each Stage of Outsourcing Process

System Stage	Confidentiality	Integrity	Availability
Development	Low	Intermediate	Low
Establishment & Supplement	Intermediate	Intermediate	Low
Operation & Disability Response	High	High	High
Contract Termination & Change	High	High	High

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

therefore no matter how well security systems are developed from the technical, physical and management perspectives, if corporate culture guarding it is not supported, security system is subject to failure. Thus, in order to solve problem of failed system adoption in organization, [36], [37] proposed Sociomateriality Theory (Figure 2).

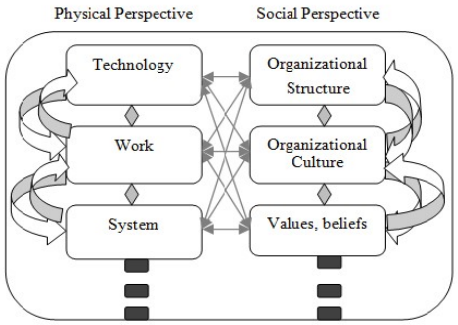

Figure 2: Sociomateriality Theory

According to this theory, because materials availability is the main focus in designing information system there are difficulties in its adoption or actual use. No matter how good the information system is, if it's not actually used by the end-user, it becomes impossible to maintain information system only with materials. In other words, Sociomateriality Theory emphasizes that in addition to conventional technical approach, it is necessary to consider social perspective. Similarly, according to [38] Social Constructivism Theory even though managers with technical knowledge and professional engineers that develop a system emphasize technical elements, depending on system's maturity, managers and organizational structure of employees can maintain and extend information system. Thus social factors become more important than factors of technical materiality, such as listening to employees instead of just commanding them.

It is common for organization management people responsible for security [39], as it can contribute to evoking employees' negative emotions [40]. According to [41] employees that receive proper treatment from organization or it representatives contribute to establishment of high-quality exchange within organization as a result of employees' positive and beneficial reciprocity. Thus, Sociomateriality Theory contributes to operation of entire system in interactions between social and organizational characteristics of an enterprise and technical factors aimed at investigating failures and problems of the system that emphasizes technology. If any characteristics of configuration factors, such as organizational structure, technical elements, organizational work, people and etc are changed, other internal system's factors should be changed too.

According to Sociomateriality Theory, in company's information security rather than focusing on management, technological and physical information security systems altogether, understanding of cultural characteristics and structures of organization that determines people's security behavior should be approached as it can increase effectiveness of information security. Depending on the project's nature, scope of information control will differ; through social integrated perspective of such information security in ICT outsourcing, which varies in depth of information security control depending on organizational and structural characteristics of sub-supplier and order company, complementary information security activation between each element in information security system becomes very important. Figure 3 shows integrated information security management framework applying Sociomateriality Theory aimed at improving information security in the ICT outsourcing environment. Thus, this study emphasizes project characteristics for improving information security levels in ICT outsourcing environment, cultural factors of sub-supplier and order companies, and physical and technical security form mutual relationship as it affects company's security outcomes.

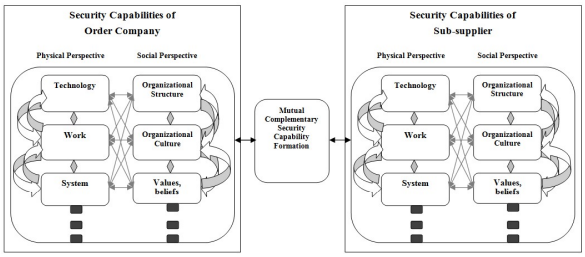

Figure3: Integrated Sociomateriality Theory with ICT Outsourcing Security Framework

According to [42], organizational culture is a comprehensive basic premise and belief, or basic assumptions and values shared by members of organization. Organizational and cultural differences in public and private organizations have been consistently studied in Public Administration Theory [43]. For instance, according to [44] there are powerful bureaucratic tendencies in public organizations, as well as strong obedience to superiors that is different to employees in private

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

organizations. In addition, there is strong resistance to change and somewhat negative perception of work due to the lack of engagement in motivational efforts and organization's stability. Furthermore, it was shown that in public organizations morality is falling and there is lack of management and organization's control that is slightly tolerant of corruption or expediency to some degree in order to achieve smooth business promotion and make profit. Also, public organizations posse citizens', business and governmental data that is more precise [45]. In addition they are expected to prioritize citizen's interests and rights and to maintain certain level of transparency for public access. Thus, information security management in public organizations appears to be quite more effective.

In regard to an organizational structure and size, a notable study of [46] proposed two types of organizational internal forms of single type-U-form and multi type-M type influential to organizations efficiency and performance. In the case of U-form that is suitable for small businesses, although representatives of each department might be effectively controlled due to the relatively small structure. As organization is expanding, drawbacks emerge due to difficulties in effective information exchange. M-form is effectively used in relatively large enterprises in which functional departments autonomously conduct work and decision-making. From then on, various types of organizational structures were proposed: in the form of Holding Company (H-form) each department has strong autonomy and makes major decisions by themselves. In Transitional Multi Divisions (M-form) form there are ongoing communication and relations between parent companies and departments. Corrupted Multi Divisional form, which is similar to M-form, is very influential in parent companies. Finally, X-form combines various organizational structures. According to [46] organizational structure is determined through direction seeking purpose of existence and organization's characteristics. In such organizational structure norms beliefs and values of organization's members about information security controls might vary greatly. Thus in this research, based on the research of [44] on cultural characteristics of public and private organizations and theory of Organizational Structure by [46] we develop a security management theoretical framework that considers characteristics of each organization' type (Table 5).

Table 5: Definition and Characteristics of the Organizational Types

Org Type	Characteristics
U-Pr	Individual efforts and achievements are emphasized; Level of members' self-control is high; Low bureaucratic tendencies; Better compliance with regulations and legal procedures
M-Pr	High self control; Compliance with organization's practices and regulations is low; High bureaucratic and hierarchical tendencies
U-Pu	Relatively strong passive attitudes toward organizational practices; Relatively low compliance with regulations and legal procedures; Bureaucratic tendencies are relatively high
M-Pu	Level of compliance with regulations and legal procedures is high; Bureaucratic and hierarchical tendencies are very high; Strong resistance to change

3.6 Theoretical Framework for Information Security Management Considering Organizational Culture and Outsourcing Characteristics

In this research complementary information security competence development of sub-suppliers and order companies is the most important factor for recognition of substantial security effect in outsourcing environment. Based on the Sociomateriality Theory, in order to develop complementary information security competence, organization's cultural security recognition/atmosphere and technical and physical security capabilities of sub-supplier and order company are seen as preemptive elements. Joint goal setting [47] is a degree of agreement between partners. How well partner's intentions are understood is deeply connected to joint goal setting [48]. According to this, establishing clear objectives becomes important for effective security control. In this research security competences of sub-supplier and order companies can act as complementarities by setting clear joint security objectives. Cultural fusion [49] stands for the degree of effort for sharing values, norms and beliefs between partners. To increase security levels sharing security atmosphere, values and behaviors of between ordering companies and sub-suppliers is imperative.

This study assumes that such fusion effort and understanding will have positive effect on enhancement of complementary security capabilities. When developing security systems of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

sub-supplier's and order companies with complementary capabilities it is important to prioritize trust that can be defined as transactional confidence in partner's integrity and reliability [50]. Here trust is seen as expectations and beliefs sharing risks and benefits of all members in the transaction. In recent years many factors were addressed as important in research about partnerships or outsourcing service providers and beneficiaries [51], [52], [53]. Especially trust in IT sub-supplier has more necessary elements in dependent relationships, and there is also lack of control and management roles in systems of order companies that are similar to outsourcing system development [54]. According to [55] trust in the ICT outsourcing environment can be traced by outcomes that are influential in significant project's achievements and knowledge transfer between order companies and service providers. Even though security systems of sub-supplier's and order companies are well developed, in order to connect with complementarities capabilities on information security trust plays an important role in sharing capabilities security awareness between both companies. More than anything, establishing connection with security effects that recognize such complementary security capabilities is important, and seems to appear differently depending on the outsourcing types and cultural characteristics of each organizational type. For more coherent comprehension, Figure 4 illustrates proposed theoretical framework of information security in the ICT outsourcing environment.

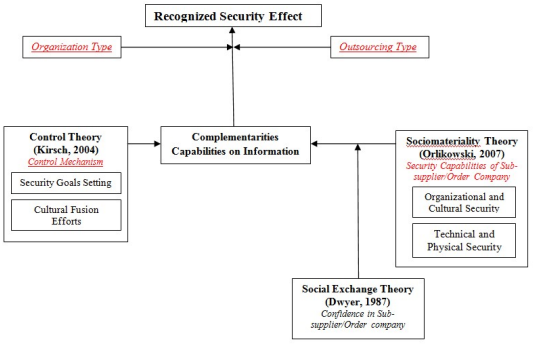

Figure 4: Sociomateriarity Framework for Information Security Management in ICT Outsourcing Environment

4. IMPLICATIONS

In conceptualizing on information security management for the ICT outsourcing environment we were able to yield at important implications that with further examinations can be applied in the actual production and operation processes. Our major theoretical implication is that with our novel framework we were able to extend previous research on information security management as we highly emphasize a bilateral perspective that is critical to consider for achieving security success in the ICT outsourcing environment [25]. In addition, by synthesizing a theory of Sociomateriality in our theoretical framework we make an innovative contribution to the existing information security research. Considerations of organization's cultural security recognition and technical security capabilities of sub-supplier's and order companies are crucial to develop complementary information security competence, thus it becomes critical to reach substantial security effect.

Our research also has practical implications that can be used to achieve successful information security management in the ICT outsourcing environment. We designed theoretical framework of security capability reinforcement on the organizational level that controls for outsourcing strategy types and organizational and cultural characteristics. Thus our research establishes information security countermeasures from research outcomes in ICT outsourcing project, which can be used as practical guidelines. In addition, order and sub-supplier companies can achieve mutual understanding of values, norms and beliefs and establish clear objectives between each other through formal and informal meetings [56]. This will help to achieve joint security goals and contribute to the strong fusion efforts between both parties. By exercising such meetings on the frequent bases will not only enable managers of sub-supplier and order companies to transfer important information, but also contribute to establishing control mechanism in outsourcing projects which will strengthen trust between both parties, as they will be able to achieve understanding of each other's intentions. Furthermore, drawing upon the theory of Sociomateriality, we emphasize the importance of designing "people-oriented" corporate culture. In other words an environment that does not just exercise a technical approach in information security management but also considers social factors. This can be done by avoiding commanding style in communication with employees, listening to them and addressing in the polite and carrying manner. Exercising such practices contribute to establishing employee-oriented environment and don't evoke employees' negative emotions [39], [40], which as a result can help to achieve proper

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

compliance to security measures as employees will be more willing to cooperate with the management in such friendly and empowering environment.

At last, considering novel propositions of our research, with future empirical examinations it results can be applied for successful information security management in the concrete and practical outsourcing environment. Recently some companies started making efforts towards analyzing and improving information security vulnerabilities in the outsourcing environment, by redesigning their security system for all outsourcing projects. However characteristics of outsourcing environment, process stages and at all were not reflected as redefined security system in its existing physical and management control couldn't progress, as customers concerns didn't decrease and security incidents in outsourcing partner companies didn't stop. Thus, if security solutions that passed theoretical verification emerged with our future research they can be widely used by production and operation companies.

5. CONCLUSIONS

This research analyzes patterns through case studies of information security in outsourcing, and technical/physical/management vulnerabilities specialized for ICT outsourcing environment that are different with existing general information security research. In particular we present detailed security management plan for outsourcing environment by diagnosing information risk levels accordingly to information flow of each process stage of outsourcing projects. In addition, our plan analyzes each type of information security structure by examining outsourcing types from the strategic, economic and social perspectives. Furthermore, with our proposed novel theoretical framework, even in its conceptual state, existing research can be extended by considering information security management from a new perspective and establish information security countermeasures from research outcomes in ICT outsourcing project, which can be used as practical guidelines. With prospective research aspirations, future empirical examinations might result in the novel contributions for the practical ICT outsourcing environment considering that our research was already able to extend extant domain by synthesizing new perspectives in the proposed theoretical framework.

ACKNOWLEDGMENTS

This study was supported by 2016 Research Grant from Kangwon National University (520160512) and the National Research Foundation of Korea (NRF-2018S1A5A2A01039413)

REFERENCES

[1] Ministry of Science, ICT and Future Planning, "Information and Communications Technology Market Forecast", Report No.21, 2013.

[2] Small and Medium Business Administration, "A Survey on Technology Security Capabilities for Small and Medium Enterprises", Report No.4, 2012.

[3] M. S. Sim, "An Empirical Study on the Improvement of Security Levels in IT Outsourcing Services", Master Thesis from Kunkuk University, 2013.

[4] Y.H. Kim, J.W. Moon, S. H. Hwang, and H.B. Chang, "A Study on Security Management in ICT Outsourcing Environment", *Journal of Society for Information Security*, Vol. 24, No. 1, 2014, pp. 23-31.

[5] M. Whitman and H. Mattord, "Principles of Information Security", Cengage Learning, 2011.

[6] N. Z. Khidzir, A. Mohamed and N. H. Arshad, "Information Security Requirement: The Relationship between Information Asset Integrity and Availability for ICT Outsourcing", *Lecture Notes on Information Theory*, Vol. 1, No. 3, 2013.

[7] D. Zissis, and D. Lekkas, "Addressing Cloud Computing Security Issues", *Future Generation Computer Systems*, Vol. 28, No. 3, 2012, pp. 583-592.

[8] N. Z. Khidzir, A. Mohamed and N. H. Arshad, "Information Security Risk Factors: Critical Threats Vulnerabilities in ICT Outsourcing", In Information Retrieval and Knowledge Management,(CAMP), *International Conference on IEEE*, 2010, pp. 194-199.

[9] B. Von Solms, "Information Security—The Third Wave?", *Computers and Security,* Vol. 19, no. 7, 2000, pp. 615-620.

[10] B. Von Solms, "Information Security–The Fourth Wave", *Computers and Security*, vol. 25, No. 3, 2006, pp. 165-168.

[11] G. Stoneburner, A. Y. Goguen, and A. Feringa, "Sp 800-30. Risk Management Guide for Information Technology Systems", *NIST Special Publication 800-30*, 2002.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[12] J. D'Arcy, A. Hovav and D. Galletta, "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: a Deterrence Approach", *Information Systems Research*, Vol. 20, No. 1, 2009, pp. 79-98.

[13] S. R. Boss, L. J. Kirsch, I. Angermeier, R. A. Shingler and R. W. Boss, "If Someone is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security", *European Journal of Information Systems*, Vol. 18, No. 2, 2009, pp. 151-164.

[14] B. Bulgurcu, H. Cavusoglu and I. Benbasat, "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness, *MIS Quarterly*, Vol. 34, No. 3, 2010, pp. 523-548.

[15] T. Dinev and Q. Hu, "The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies", *Journal of the Association for Information Systems*, Vol. 8, No. 7, 2007, p. 23.

[16] Q. Hu, Z. Xu, T. Dinev and H. Ling, "Does Deterrence Work in Reducing Information Security Policy Abuse by Employees?" *Communications of the ACM*, Vol. 54, No. 6, 2011, pp. 54-60.

[17] A. C. Johnston and M. Warkentin, "Fear Appeals and Information Security Behaviors: An Empirical Study, *MIS Quarterly*, Vol. 34, No. 3, 2010, pp. 549-566.

[18] P. Puhakainen and M. Siponen, "Improving Employees' Compliance through Information Systems Security Training: An Action Research Study", *MIS Quarterly*, Vol. 34, No. 4, 2010, pp. 757-778.

[19] M. Siponen and A. Vance, "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations", *MIS Quarterly*, Vol. 34, No. 3, 2010, p. 487.

[20] C. L. Claar and J. Johnson, 2012. "Analyzing Home PC Security Adoption Behavior", *Journal of Computer Information Systems*, Vol. 52, No. 4, 2012, pp. 20-29.

[21] B. Y. Ng, A. Kankanhalli and Y. C. Xu, "Studying Users' Computer Security Behavior: A Health Belief Perspective", *Decision Support Systems*, Vol. 46, No. 4, 2009, pp. 815-825.

[22] J. Mills, K. Platts and M. Bourne, "Applying Resource-Based Theory: Methods, Outcomes and Utility for Managers", *International Journal of Operations and Production Management*, Vol. 23, No. 2, 2003, pp. 148-166.

[23] S. Kim and Y. S. Chang, "Critical Success Factors for IS Outsourcing Implementation from an Inter-organizational Relationship Perspective", *The journal of computer information systems*, Vol. 43, No. 4, 2003, pp. 81.

[24] N. Levina and J. W. Ross, "From the Vendor's Perspective: Exploring the Value Proposition in Information Technology Outsourcing", *MIS Quarterly*, Vol.27, No.3, 2003, pp. 331-364.

[25] H. S. Han, J. N. Lee, J. U. Chun and Y. W. Seo, "Complementarity between Client and Vendor IT Capabilities: An Empirical Investigation in IT Outsourcing Projects", *Decision Support Systems*, Vol. 55, No. 3, 2013, pp. 777-791.

[26] K. J. Cha, Z. Lee and J. S. Cha, "Strategies for Successful Supplier Relationship Management(SRM) in the SI Industry", *Journal of Society for e-Business Studies*, Vol. 17, No. 3, 2012, pp. 105-116.

[27] M. S. Sim, "An Empirical Study on the Improvement of Security Levels in IT Outsourcing Services", Master Thesis from Kunkuk University, 2013.

[28] N. Z. Khidzir, A. Mohamed and N. H. Arshad, "Information Security Risk Factors: Critical Threats Vulnerabilities in ICT Outsourcing", In Information Retrieval and Knowledge Management,(CAMP), *International Conference on IEEE*, 2010, pp. 194-199

[29] J. W. Ko, 2005. "A Study on Information Security Management Measures of IT Outsourcing Companies Based on Case Studies", Master Thesis from Yonsei University, 2005.

[30] Financial Service Commission (FSC), "A Strategy for Successful Security Management for Outsourcing Service Companies", 2011.

[31] Koscom, "Information Technology Outsourcing Human Resource Survey Report", 2011.

[32] National Intelligence, "Security Management Regulation Check List, 2011.

[33] National Internet Development Agency of Korea, "A Final Report on Information Security Survey for Corporate Organization", 2011.

[34] J. N. Lee, S. M. Miranda and Y. M. Kim, "IT Outsourcing Strategies: Universalistic, Contingency, and Configurational Explanations of Success", *Information Systems Research*, Vol. 15, No. 2, 2004, pp. 110-131.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[35] E. Albrechtsen, "A Qualitative Study of Users' View on Information Security", *Computers and Security*, Vol. 26, No. 4, 2007, pp. 276-289.

[36] W. J. Orlikowski, "Sociomaterial Practices: Exploring Technology at Work", *Organization Studies*, Vol. 28, No. 9, 2007, pp. 1435-1448.

[37] W. J. Orlikowski, and S. V. Scott, "Sociomateriality: Challenging the Separation of Technology, Work and Organization", *The Academy of Management Annals*, Vol. 2, No. 1, 2008, pp. 433-474.

[38] T. P. Hughes, "The Evolution of Large Technological Systems. The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology, 1987, pp. 51-82.

[39] M. E. Kabay, "Using Social Psychology to Implement Security Policies", *Computer Security Handbook*, Vol. 35, No. 1, 2002.

[40] A. McIlwraith, "Information Security and Employee Behavior:How to Reduce Risk Through Employee Education", *Training and Awareness, Gower Publishing, Ltd*, 2006.

[41] R. P. Settoon, N. Bennett and R. C. Liden, "Social Exchange in Organizations: Perceived Organizational Support, Leader–Member Exchange, and Employee Reciprocity, *Journal of Applied Psychology*, Vol. 81, No. 3, 1996, pp. 219.

[42] E. H. Schein, "Organizational Culture and Leadership: A Dynamic View", San Francisco, 1985.

[43] H. G. Rainey, "Public Agencies and Private Firms Incentive Structures, Goals, and Individual Roles", *Administration and Society*, Vol. 15, No. 2, 1983, pp. 207-242.

[44] W.H . Kim, "A Comparative Analysis on Organizational Climate between Public Organization and Private Organization", Report from Research Center for Social Science, DaeJeon University, 1996.

[45] M. Bishop, "What is Computer Security?", *Security and Privacy, IEEE*, Vol. 1, No. 1, 2003, pp. 67-69.

[46] O. E. Williamson, "Markets and Hierarchies", New York, 1975, pp. 26-30.

[47] J. K. Benson, "The Interorganizational Network as a Political Economy", *Administrative Science Quarterly*, Vol.20, No.3, 1975, pp. 229-249.

[48] A. Rai, S. Borah and A. Ramaprasad, "Critical Success Factors for Strategic Alliances in the Information Technology Industry: An Empirical Study", *Decision Sciences*, Vol 27, No. 1, 1996, pp. 141-155.

[49] M. R. Bate, I. A. Bonnell and N. M. Price, 1995. "Modeling Accretion in Protobinary Systems", *Monthly Notices of the Royal Astronomical Society*, Vol. 277, No. 2, 1995, pp. 362-376.

[50] R. M. Morgan and S. D. Hunt, "The Commitment-Trust Theory of Relationship Marketing", *The Journal of Marketing*, Vol. 58, No.3, 1994, pp. 20-38.

[51] J. Y. Mao, J. N. Lee and C. P. Deng, C. P., "Vendors' Perspectives on Trust and Control in Offshore Information Systems Outsourcing", *Information and Management*, Vol. 45, No. 7, 2008, pp. 482-492.

[52] J. Y. Park, K. S. Im, and J. S. Kim, "The role of IT Human Capability in the Knowledge Transfer Process in IT Outsourcing Context" , *Information and Management*, Vol. 48 No. 1, 2011, pp. 53-61.

[53] J. N. Lee and B. Choi, "Effects of Initial and Ongoing Trust in IT Outsourcing: A Bilateral Perspective", *Information and Management*, Vol. 48, No. 2, 2011, pp. 96-105.

[54] P. Hart, and C. Saunders, "Power and Trust: Critical Factors in the Adoption and Use of Electronic Data Interchange", *Organization Science*, Vol. 8, No. 1, 1997, pp. 23-42.

[55] H. S. Kim, S. C. Park, and J. W. Kim, "Effect of Knowledge Transfer on IS Outsourcing Projects", *Korean Business Review*, Vol. 40, No. 4, 2011, pp. 987-1013.

[56] T. L. Huber, T. A. Fischer, L. Kirsch, and J. Dibbern, "Explaining Emergence and Consequences of Specific Formal Controls in IS Outsourcing-A Process-View", In System Sciences (HICSS), *47th Hawaii International Conference*, 2014, pp. 4276-4285.