ICIC Express Letters
Volume **10**, Number **4**, April **2016**

 ISSN 1881-803X
pp. 767–773

A ROLE OF INFORMATION SECURITY COMMITTEE BASED ON COMPETING VALUES FRAMEWORK

Kunwoo Kim[1] and Jungduk Kim[2]

[1]Department of Security Convergence
Graduate School of Chung-Ang University
[2]Department of Industrial Security
Chung-Ang University
84 Heukseok-ro, Dongjak-gu, Seoul 156-756, Korea
kunwoo.kim317@gmail.com; jdkimsac@cau.ac.kr

Received September 2015; accepted December 2015

Abstract. *Establishing enterprise information security system in a corporate governance dimension is regarded as a critical issue for managing various risks like reinforcement of compliance requirement and significant impact of IT. However, there are lots of obstacles to implement enterprise-wide information security activity and top management commitment seems to be insufficient as a key player. In this situation, participating information security committee can be a good way to vitalize the commitment of top management and its activities are essential for implementing information security governance. However, rarely study a role of information security committee even information security governance has been studied extensively. The purpose of this research is to identify roles of information security committee as an exploratory study. For comprehensive and theoretical study, we derive 4 dimensions from Quinn's Competing Values Framework (CVF) that provides analytic methodology and then we identify 8 roles of information security committee related to the dimensions through literature review. The result is discussed by Focus Group Interview (FGI) which organized 4 specialists in the field of information security to accept their opinion in terms of real business experience and finally, we propose 10 roles of information security committee adjusted the opinions.*
Keywords: Information security committee, Information security governance, Competing Values Framework

1. **Introduction.** This research emerged from the question "How can I get C-level executives commitment for enterprise-wide information security?" Indeed, recently the question has been one of the most important and difficult issues in the field of information security. However, it is hard to get a definitive answer to the question because it is difficult to solve without recognizing paradigm shift of information security. Top management regarded information security as just a technical issue in the past. Therefore, they realized that middle manager or IT department is responsible for information security and consequently top management commitment is insufficient to implement information security program. Nowadays an approach about information security has been surfaced as governance and business issue, and also roles and responsibilities of top management are getting importance to implement enterprise-wide information security well.

In many foreign countries, information security governance focused on accountability and transparency of top management has been studied extensively from the early 2000s. Solms and Solms describe information security governance as the way to overcome 10 deadly sins of information security management [1]. Furthermore, the first deadly sin is that top management is not realizing that information security is a corporate governance responsibility and not performing due care and due diligence. In this circumstance, the information security committee is a good solution to change awareness of top management about information security. Information security committee can be a self-motivation for

realizing their due care and due diligence by participating decision making about information security agenda. However, according to survey analysis of Gartner, the sponsorship of information security committee to security program and participation of business process owner are insufficient [12]. In this case, security program is hard to get sufficient support from the rest of the organization because the information security committee should consist primarily of business representatives. Moreover, without the support of business representatives, it is hard to arbitrate between conflicting security requirement and business requirement.

In fact, the importance of information security governance is often noted but rarely studied a research about information security committee in the meanwhile. A research on information security committee is still in its early stage; thus an exploratory research is required to identify what kind of role the information security committee conducts. The purpose of this research is to identify roles of information security committee as an exploratory study. Because previous study is not sufficient as well as comprehensive, we will derive required dimensions from Quinn's Competing Values Framework that provides analytic methodology as a theoretical approach, and then we will identify roles of information security committee according as each dimension. Furthermore, the results will be discussed by focus group interview which organized information security specialists in order to adjust their opinions in terms of real business challenge.

2. **Literature Review.**

In this section the importance and necessity of information security committee will be explained, and also we will review several researches related to the committee's role and their limitations. In addition, we will introduce Quinn's Competing Values Framework that provides analytic methodology for comprehensive and theoretical study. We expect that the framework is available to be applied as comprehensive and theoretical approach to improve limitations of preceding researches.

2.1. **Information security committee.**

Typically one of functions of generic committee is to mitigate conflict through discussion among the participants [7]. Related to the function, Scholtz and Byrnes emphasize the importance of information security committee to conciliate or arbitrate conflict of interest [11]. Nowadays there are various obstacles to implement information security in terms of enterprise-wide activity. For example, the higher level of information security controls, the higher cost and it affects business productivity. Also there is an obvious contrast between the goal of information security and IT, stability versus efficiency; on this account limited cooperation or conflict between information security department and IT department arises. Therefore, formal and horizontal communication channels are required to overcome the above problem.

The merit of committee is that it helps increasing top management's motivation by decision making related agenda and it leads to continuous commitment. Recently revised ISO/IEC 27001:2013 includes leadership for implementing information security management system as a requirement [4]. The words of management commitment became one of control domains. Also, ISO/IEC 27014:2013, governance of information security, was newly established as an international standard in 2013. The standard consists of R&R and process of governing body [5]. A close look at these changes represents the importance of top management commitment. Scholtz accounts for the role of the information security committee has become an important tool for a coordinated corporate security strategy, for reducing duplication in security spending, for taking control of complex infrastructures and ultimately, for reducing security risk [10]. That means agendas discussed at information security committee include control and direction guidance of information security and risk management.

Fitzgerald describes the necessity of information security committee by stating "Security councils are an essential element to build management commitment, and continued

delivery provides the necessary 'oxygen' to keep the council functioning." [9]. However, there is a contradictory in his suggestion. He suggests that the security council should consist primarily of middle management because it is difficult to obtain the time commitment required to review policies at a detailed level by top management. Also we can understand the concept of council and committee is a different level considering the participants. Even top management has not enough time to review the details of security policy, top management is responsible for decision making and the middle management has limited authority about direction guidance. Moreover, Fitzgerald proposed 6 roles of information security committee; however, the roles are not comprehensive but simply listed up and it is hard to represent required entire roles.

Meanwhile, Scholtz and Byrnes proposed scope and function of information security in terms of multilayer information security governance structure [11]. Even there is difference in that the participants are changeable according as the size and maturity of organization but the vital roles of information security committee are similar to Fitzgerald. Especially interesting from the point of view is that they emphasize the importance of participating business unit manager like HR, legal and compliance department. It presents a communication between information security organization and business unit to align strategy and arbitrate conflict. In addition, Scholtz and Byrnes proposed 8 roles of information security committee; however, the roles are based on experience in terms of business and therefore theoretical explanation is not sufficient. Thus, in order to improve those two limitations, it is required to establish comprehensive and theoretical framework and then required roles of information security committee should be identified.

2.2. **Competing Values Framework.** The Competing Values Framework was originally developed to identify indicators of organizational effectiveness but it has been used one of the most influential and extensively models in the area of organizational research until now [8]. In other words, it provides a methodology which is available to comprehensively analyze among contradictory and exclusive values in organization. The framework is divided into four value dimensions by two axes which is a conflictive concept made up from an emphasis on control to an emphasis on flexibility and from internal to external organizational focus. The dimensions are represented by human relations model, rational goal model, internal process model and open system model.

The human relations model places on the value dimension of flexibility and internal focus, and would emphasize familial relationship among each individual human resource. Thus the core value of this model can be conflict arbitration through communication. Internal process model places on the value dimension of control and internal focus, and would characterize bureaucratic culture. In other words, it is focused on hierarchical oversee, clear role and responsibility for organizational continuity and security. The rational goal model places on the value dimension of control and external focus, and would emphasize effective goal setting and planning. Therefore, the core value of this model is accurate direction guidance for maximizing productivity and efficiency. The open system model places on the value dimension of flexibility and external focus, and would emphasize terms of organizational growth and resource acquisition. Thus, asset allocation and investment related financial and economic value for continuous improvement are included in the model.

As stated above, the Competing Values Framework suggests four dimensions from contrast concept each other and would apply in the field of information security. In terms of information security, there are also competing values represented by level of security control and business efficiency, internal requirement and external requirement.

3. **Roles of Information Security Committee.** In this section, we will derive four dimensions from analyzing the relevance to Quinn's Competing Values Framework and

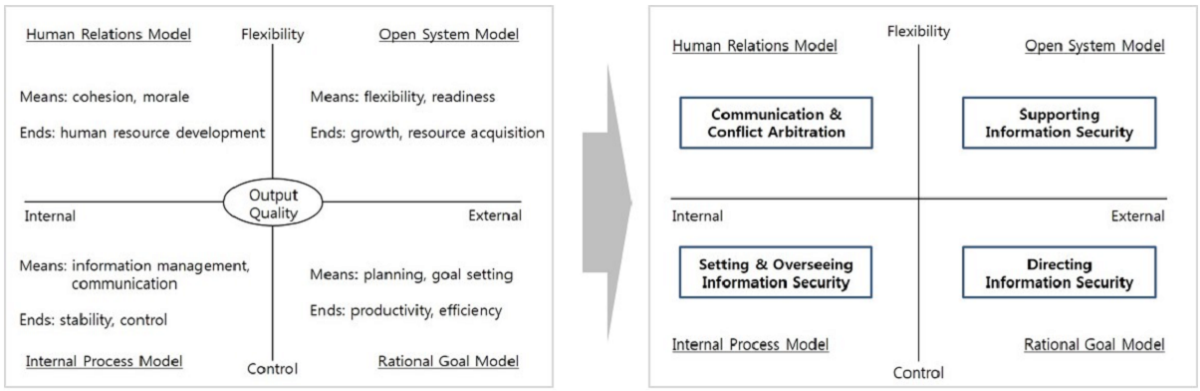

FIGURE 1. Four dimensions derived from Quinn's Competing Values Framework

identify roles of information security committee related to the dimensions. Figure 1 shows that how four dimensions are derived from the framework (the left side of Figure 1), and how to be replaced in terms of information security fields. The relationship among each dimension and related roles of information security committee are as follows.

First of all, the human relations model is focused on familiar relationship between each other. For better relationship in terms of information security, it is required to conciliate or arbitrate conflict caused by contrast requirements between information security and business [11]. Gartner suggests that, as organizations take an increasingly risk-based approach to manage their security programs, an arbitration function will become increasingly significant [12]. At this time interacting with CXOs is a necessary factor and specially the role of CISO (Chief Information Security Officer) is very important [3]. Within the committee, the CISO is the key person as a leader of information security organization. In order to meet business requirement, CISO should liaise with business unit manager and process owners for ongoing alignment [13]. Thus, the human relations model can be replaced to 'communication and conflict arbitration' as one of dimensions of information security committee, additionally liaising with business unit and implementing risk-based information security program can be included at the dimension as required roles of information security committee.

Second, internal process model is focused on hierarchical oversee and establishing clear roles and responsibilities for organizational continuity and security. In terms of information security field, it is required to establish, communicate and ensure the respective accountabilities for information security program and then oversee the program performance [8,10]. According to Tuckman's group development model represented by forming, storming, norming, and performing, there exist lots of arguments related to individual role at the storming stage so establishing role and responsibility is a vital activity for stepping up to the next stage, norming and performing [2]. Furthermore, for maintaining business continuity, information security committee should review and advise the extent to which information security program meets business goal [13]. In terms of the performance management, therefore, overseeing and monitoring performance of information security is important [9,11]. Thus the internal process model can be replaced to 'setting & overseeing information security' as one of dimensions of information security committee, additionally defining respective accountability and monitoring security program performance can be included at the dimension as major roles of information security committee.

Third, the value of rational goal model as stated at previous section is focused on effective goal setting and planning. It means that it is important to give a direction to organizational efforts, and also a leadership is increasingly required to go to right way and do right things. At this point of view in terms of information security, CISO, the

leader of information security organization, has a responsibility for leading and supporting the information security committee and makes it possible to decide right direction. Information security committee also should formalize reasonable security policy [9,11] and guide the security and risk program and architecture strategy [11]. Moreover, prioritizing information security efforts in accordance as security policy and strategy is required to get right direction [9]. Thus, 'directing information security' can be one of dimensions of information security committee with high relevance to rational goal model. In addition, review and approval of security policy and strategy and prioritization of information security effort can be included at the dimension as important roles of information security committee.

Finally, the open system model is focused on organizational growth and resource acquisition. That means an effort such asset allocation and financial supporting is important for continuous improvement. In terms of information security, the information security committee forms the backbone for sustaining organizational support for comprehensive information security program [9]. Especially information security committee should seasonably approve and allocate the budget of the enterprise security program and also assessing the value of information security investment for budget approval is required to implement as prior activity [11]. In doing so, a financial support from information security committee makes it possible to prevent information security incident. Thus, the open system model can be replaced to 'supporting information security' as one of dimensions of information security committee, and additionally assessment for value of security investment and allocation of security budget can be included at the dimension as supporting roles of information security committee.

4. **Discussion.** We discussed every role based on each dimension derived from Quinn's Competing Values Framework with specialists in the field of information security for the purpose of review whether each role is necessary or applicable to organization through focus group interview. The focus group interview is a form of qualitative research in which researcher can get meaningful data that is hard to derive from literature study as well as statistical analysis, and it is useful to exploratory study in case of lack of preceding research or for developing construct and item for empirical study [6]. A focus group is generally composed of 4 to 12 people, and a small group of 4 or 5 participants afford more opportunity to share ideas [6]. In this study, the focus group is composed of 4 specialists: a CISO over 20 years of work experience at ICT company, a professor over 20 years of study experience, a senior consultant over 15 years of work experience and a security manager 15 years of work experience at manufacturing company in the field of information security for the purpose of review whether each role is necessary or applicable to organization. The interview was held on March 19 in 2015 and it lasted for two hours.

There was fully consensus as to dimensions among the specialists but related to roles, additional comments were suggested. One of opinions is suggested that it is required to have a prior mediation about expected conflict between CISO and other participants before the committee meeting. This communication activity can be an efficient way to reduce conflict within decision making process and the prior cooperation might be included in dimension of communication and conflict arbitration. Another opinion related to supporting information security is suggested that it is required to recommend to CEO or BoD (Board of Directors) about things that are necessary for continuous improvement. They expect this role of information security committee makes it possible to support enterprise-wide information security. However, actually CEO and BoD, sometimes other CXOs, are hard to participate in the information security committee for a variety of reasons even they are required to play a key role. One of rational solutions for this, major agendas only should be reported to CEO and BoD at no matter what kind of committee such as steering committee, risk management committee and compliance committee. Therefore,

role about recommendation to CEO & BoD for security improvement might be included in dimension of supporting information security. Besides the above opinions, there were several discussion subjects such as committee member, meeting frequency and major agenda; on the other hand they were excepted from this study because it is not related to the research question directly. Table 1 shows roles of information security committee that we propose and it includes revised result from discussion through focus group interview as a qualitative research. We expect that the result can be used as constructs or items for empirical study.

Table 1. Revised roles of information security committee

CVF	Dimension	Role
Human Relations Model	Communication & Conflict Arbitration	Liaise with business unit
		Implement risk-based approach
		Request for prior cooperation
Internal Process Model	Setting & Overseeing Information Security	Define respective accountability
		Monitor security program performance
Rational Goal Model	Directing Information Security	Review and approve security policy and strategy
		Prioritize information security effort
Open System Model	Supporting Information Security	Assess the value of security investments
		Allocate security budget
		Recommend to CEO & BoD for security improvement

5. **Conclusions.** Recently a security incident has consistently happened and even information security is regarded as a social responsibility. Moreover, there are various obstacles related to management and operation of information security that have to overcome for business continuity. However, the thing is that most of organizations still take just technical approach regardless of paradigm shift. We believe that a commitment of top management including business units is a vital factor for implementing enterprise-wide information security in this situation because information security is a business issue.

This research offers roles of information security committee based on robust framework with theoretical linkages as one of ways to increase commitment of top management in governance environment. As a result, four comprehensive dimensions are derived from Quinn's Competing Values Framework and finally 10 roles of information security committee in accordance with each dimension are proposed through literature and focus group interview. While this research is a meaningful attempt to help top management and decision maker understand their duty, there are some limitations in terms of generalization and validity. Therefore, we will conduct a survey whether proposed roles and how much the roles provide positive values to information security and business performance as a future study.

Acknowledgment. This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2015-H8501-15-1018) supervised by the IITP (Institute for Information & communications Technology Promotion).

REFERENCES

[1] B. von Solms and R. von Solms, The 10 deadly sins of information security management, *Computers & Security*, vol.23, pp.371-376, 2004.

[2] B. W. Tuckman, Developmental sequence in small groups, *Psychological Bulletin*, vol.63, no.6, pp.384-399, 1965.

[3] D. Whitten, The chief information security officer: An analysis of the skills required for success, *Journal of Computer Information Systems*, vol.48, no.3, pp.15-19, 2008.
[4] ISO/IEC 27001:2013, *Information Technology – Security Techniques – Information Security Management Systems – Requirements*, 2013.
[5] ISO/IEC 27014:2013, *Information Technology – Security Techniques – Governance of Information Security*, 2013.
[6] R. A. Krueger and M. A. Casey, *Focus Groups: A Practical Guide for Applied Research*, SAGE Publications, Inc., Thousand Oaks, CA, 2000.
[7] P. J. Dadalt, Earnings management and corporate governance: The role of the board and the audit committee, *Journal of Corporate Finance*, vol.9, no.3, pp.295-316, 2001.
[8] R. E. Quinn and J. Rohrbaugh, A spatial model of effectiveness criteria: Towards a competing values approach to organizational analysis, *Management Science*, vol.29, no.3, pp.363-377, 1983.
[9] T. Fitzgerald, Building management commitment through security councils, *Information Systems Security*, vol.14, no.2, pp.27-36, 2005.
[10] T. Scholtz, The role of the corporate information security steering committee, *SC Magazine*, 2003.
[11] T. Scholtz and F. C. Byrnes, Information security and governance: Forums and committees, *Gartner*, G00207477, 2010.
[12] T. Scholtz, Survey analysis: Information security governance, *Gartner*, G00262134, 2014.
[13] IT Governance Institute, *Information Security Governance: Guidance for Boards of Directors and Executive Management*, 2nd Edition, U.S.A., 2006.