AN EXPLORATION OF GROUP INFORMATION SECURITY COMPLIANCE: A SOCIAL NETWORK ANALYSIS PERSPECTIVE

Research-in-Progress

Chul Woo Yoo
University at Buffalo
Buffalo, NY, USA
chulwooy@buffalo.edu

G. Lawrence Sanders
University at Buffalo
Buffalo, NY, USA
mgtsand@buffalo.edu

Abstract

In the information age, the failure of an organization to make employees comply with its information security policies is regarded as a key threat. For this reason, investigating employees’ information security policy violations has been a major concern in information security research. In most previous studies, information security compliance behavior was investigated at the individual level. The mechanism of information security compliance from a group perspective is not well known, either to practitioners or researchers. Therefore, this study attempts to investigate the impact of group characteristics on information security compliance from a social network perspective. For empirical validation, the survey research method is adopted, and data collection is conducted from 3 organizations in Korea. The results show there are significant connections between group security compliance intention and centrality compliance motivator alignments. Several theoretical contributions and managerial implications are discussed.

Keywords: Group security compliance, information security, social network analysis, deterrence, self-efficacy, rewards
Introduction

Practitioners and researchers recently have agreed that information security cannot be achieved solely through technology-based solutions (Hamill et al. 2005). Although technology-based tools may help an organization improve information security (Straub 1990), they are not able to eliminate the information security risks that an organization may face since many security related issues—such as password setup, encryption tool use, and restrictions on flash drive use—are achieved only through human compliance (Siponen 2005). Genuine success in organizational information security must rely on the consideration of three components: people, processes, and technology (Hamill et al. 2005).

The failure of an organization to make employees comply with information security policies is thus a key threat (Siponen et al. 2010). According to information security studies, employee noncompliance with information security policies is described as a main barrier to organizational information assurance (Puhakainen 2006; Sarkar 2010; Whitman 2003). It is reported that over half of all information systems security breaches are directly or indirectly caused by employees’ poor compliance with information security policies (Dhillon and Moores 2001; Stanton et al. 2005). Investigating employees’ information security policy violation has been a major concern in information security research (Bulgurcu et al. 2010; D’Arcy et al. 2009; Siponen and Vance 2010), although empirical research on end-user security behaviors and the factors influencing them is still in the early stage (Herath and Rao 2009a).

Insiders—that is, employees of an organization—may be more dangerous to an organization than outsiders since insiders have accurate knowledge of informational asset and systems, authorized accessibility to systems, and the opportunity to violate policies (Magklaras and Furnell 2005; Willison and Siponen 2009). The information security literature has suggested several behavioral models that may either enhance employee security policy compliance or explain the mechanisms for computer abuse or security policy violation (Bulgurcu et al. 2010; Pahnila et al. 2007). For example, the use of sanctions based upon deterrence theory is widely advocated (D’Arcy et al. 2009; Herath and Rao 2009b; Siponen et al. 2010) to overcome the problem of employee non-compliance. Other theories presented in the research literature, such as the means to enhance employee information security behavior, include protection motivation theory, neutralization theory, rational choice theory, and principal agent theory, among others (Boss et al. 2009; Bulgurcu et al. 2010; D’Arcy et al. 2009; Herath and Rao 2009b; Siponen and Vance 2010; Siponen et al. 2010; Vance et al. 2012; Willison and Siponen 2009).

However, most studies that apply these theories have investigated information security compliance behavior at the individual level. The mechanism of information security compliance from a group perspective is not well known. Groups such as a department or project team are the basic units of employee work life in an organization. When we only consider the individual as a subject of security compliance, other important mechanisms, such as group norm, group coordination, and others, which form and influence the security compliance deeply related psychological aspect of individual could be overlooked (Ehrhart and Naumann 2004). Further, examining the group level is essential in understanding the organization level since most tasks in an organization are complex and interdependent (Pritchard et al. 1988). According to the studies on social network analysis, in addition to characteristics of the individual, the social network position of individuals and the availability of relevant resources of each group member influence overall group results (Rulke and Galaskiewicz 2000; Sparrowe et al. 2001). Hence, adopting a group aspect in exploring security compliance in an organization can provide essential findings to current literature of information security.

For the purposes of this study, we define group security compliance as the collective performance on security policies as influenced by membership in a group. We focus on the group’s social network structure as an important aspect of a group’s characteristics. Every employee in a given group has an individual aptitude regarding such factors as security-efficacy and the perception about sanctions and rewards, among others. For example, self-efficacy in security policy compliance has been investigated as an important antecedent of compliance intention. However, for this study we assume that simple accumulation of individual self-efficacy cannot fully explain a group’s overall self-efficacy.

Our question for research is this: How does alignment between a group’s social network structure and each individual’s information security factors influence group information security compliance? To answer this question, we conducted a multilevel survey as the basis of our study. We adopted social
network analysis to examine the impact of social network position of group members, and employed questionnaire instruments to measure each group member’s perception about security compliance, security efficacy, etc.

This study offers several important contributions to the current literature on information security compliance. It develops and examines a new construct, Centrality Compliance Motivator Alignment. The “motivators” we consider include security efficacy and the use of sanctions and rewards. By using this construct, we will show that a simple inventory of individual compliance of group—made by totaling the sum of the individual compliance—is insufficient to understand the functioning of the group as an ensemble. Additionally, by adopting a social network approach, this study extends the understanding of important concepts existing already in the information security domain.

In the first section of this paper, we discuss the relevant literature and organize the investigated variables. Next, we develop a theoretical model based on a detailed review of relevant information security, economic, sociological, and psychological literature. We then discuss the development of the instrument. We conclude the paper with a discussion of our expected findings, along with their implications for theory and practice.

Information Security in the Organizational Setting

In keeping with our research interest, we review studies that deal with information security from a behavioral perspective. First, from a deterrence perspective, an insider is someone who the organization must train in order to comply with information security policies. In essence, insiders are considered a source and threat potential that need to be monitored. Deterrence theory provides a comprehensive view of the role of the insider. Literature describing deterrence theory discusses such variables as sanctions, severity of punishment, and certainty of detection. Deterrence is considered a primary and effective antecedent that prevents a person from behaving illegally. In practice, a deterrence mechanism is implemented and then investigated. In the literature, sanctions most often are found to have a positive impact on the perceived cost of non-compliance (Bulgurcu et al. 2010; Guo et al. 2011; Pahnila et al. 2007). Severity of punishment is not found to be a significant factor (Herath and Rao 2009a; Herath and Rao 2009b; Li et al. 2010), while certainty of detection is (Herath and Rao 2009a; Herath and Rao 2009b; Li et al. 2010; Siponen et al. 2010). These findings are consistent with those from software piracy studies, which show significant relationships between deterrence variables and non-compliance behavior (Gopal and Sanders 1997; Peace et al. 2003; Yoo et al. 2012).

Protection Motivation Theory (PMT) is another method often adopted in information security compliance literature. PMT proposes that four factors work towards self-protection: the perceived severity of a threatening event, the perceived probability of the occurrence (i.e., vulnerability), the efficacy of the recommended preventive behavior, and perceived self-efficacy (Rogers 1975). Within the context of information security, PMT defines an insider as a human agent who wants to prevent a cyber-security invasion incident by taking an action. Early literature on the topic investigated factors of threat assessment such as perceived vulnerability, perceived severity, and reward, among others (Bulgurcu et al. 2010; Herath and Rao 2009b; Johnston and Warkentin 2010; Vance et al. 2012; Workman et al. 2008). These aspects are conceptualized as the consequential severity of the security threat and the probability of exposure to a substantial security threat. Other variables such as response efficacy and self-efficacy are examined as they are related to the coping assessment (Herath and Rao 2009b; Johnston and Warkentin 2010; Vance et al. 2012; Workman et al. 2008).

Some researchers investigated habit as an important antecedent to behavioral differences. Vance et al. argue that many actions occur without conscious decision to act and are performed because individuals are accustomed to performing them. Frequently repeated behavior is controlled more by situational cues than conscious decision-making (Vance et al. 2012). The results of that study shows that habit has significant influence on threat appraisal and coping appraisal.

Siponen and Vance argue that employee violation of IS security policies is not always best explained by fear of sanctions because employees may use neutralization techniques (Siponen and Vance 2010). This rationalizing behavior in turn reduces the deterring effect of sanctions. Siponen and Vance applied neutralization theory components (i.e., denial of responsibility, denial of injury, condemnation of the
condemners, defense of necessity, and appeal to higher loyalties) to information security. Their study investigates non-compliance behavior from neutralization and deterrence perspectives. Results show that neutralization components play a significant role in employee non-compliance.

Herath and Rao (2009a) provide the early foundation to the “principal agent” theory of information security. The principal agent theory focuses on individual employees and investigates the role of penalty and social pressure that extrinsically motivate an employee to comply with information security policies. Herath and Rao argue that employees believe that higher levels of information security restrict an employee's ability to follow changing operational routines, and thus they perceive the increased security as counterproductive. The study also shows that monitoring all end-user actions related to information security is extremely costly and may not even be possible.

**Compliance Motivators**

As discussed in the previous section, existing literature establishes and tests many antecedents that, at the individual level, can influence security compliance either directly or indirectly. These include sanctions, threat severity, threat vulnerability, rewards, self-efficacy, and response efficacy (Bulgurcu et al. 2010; Herath and Rao 2009b; Siponen et al. 2010; Vance et al. 2012). Those factors are used to measure individual perception and its impact on security compliance. The fact that individuals respond differently to these factors derives from personal propensities such as risk perception (e.g., a risk-taking person or a risk-avoiding person). One person may regard a security threat as a serious problem to work life while another might think it trivial.

However, some antecedents to security compliance are more variable than other factors in inter-employee relationships since they are formed and affected by an individual’s knowledge or skill. Adding the influence of employee interaction will create further variations in security compliance. Through the sharing of knowledge and assistance, one employee may change another's perception of certain issues (Lin and Joe 2012). For example, some employees could may not know what punishment is associated with information security non-compliance and thus feel they are not likely to be caught or punished if they do not comply with security policies or regulations. On the other hand, other employees may have more information about non-compliance punishment and the certainty of punishment. Conversations between the two types of employees may greatly change the first group's understanding of the certainty of punishment. When it comes to security compliance issues, employees could be educated and helped by their peers.

In a similar vein, some other antecedents, such as security efficacy, could be extended to apply to the group context. For example, let us say that there are two department heads, A and B. They both receive a notice about a new security policy (regarding, for example, password setup or encryption, etc.), and both find it difficult to understand and comply with the new security policy. Both department heads in effect, have a low level of security efficacy and may demonstrate security non-compliance by mistakes or ignorance, rather than intention (Herath and Rao 2009b). Suppose, however, that department head B has a close relationship with a subordinate in the same department who is skillful in security compliance; the department head could be taught about the new security policy. In contrast, department head A also has a knowledgeable employee on his team, but since A is not close to that employee he likely will not learn from him. Nor will the employees in department A obtain the necessary insights regarding the new security policy. In other words, B’s team can show better group compliance than A’s team, even though both teams have sufficient resources within their respective group.

In this study of group influence on information security, we will examine some of the direct antecedents discussed in the literature and highlighted in the above discussion. This study will focus on three antecedents of compliance. They are: sanctions (D'Arcy et al. 2009; Herath and Rao 2009a; Herath and Rao 2009b), self-efficacy (i.e., security efficay) (Bulgurcu et al. 2010; Herath and Rao 2009b; Johnston and Warkentin 2010), and rewards (Pahnila et al. 2007; Vance et al. 2012; Workman et al. 2008). We refer to these antecedents as “compliance motivators.” Based upon previous studies, in this study sanctions are defined as tangible or intangible penalties, such as demotions, loss of reputation, reprimands, monetary or nonmonetary penalties, and unfavorable personal mention in oral or written assessment reports in return for noncompliance with the requirements of the information security policy (Bulgurcu et al. 2010). Security efficacy is defined as an employee’s belief in one’s own skills, knowledge,
or competency about fulfilling the requirements of the information security policy (Bulgurcu et al. 2010). Rewards are defined as tangible or intangible compensation that an organization offers in return for compliance with the requirements of the information security policy (Bulgurcu et al. 2010).

Information Security Compliance at the Group Level

Most of the previous studies on information security compliance have been conducted at the individual level of analysis. However, as several researchers (Bulgurcu et al. 2010; Herath and Rao 2009b) have noted, compliance is related to the workgroup structure (e.g., a department, project team, etc.) and may be affected by group dynamics as well as by individual decision-making. In addition, security compliance is often evaluated in the context of the group. Little research has been done to identify the factors that influence security compliance at the group level. Based upon the findings of existing individual level studies, we postulate that groups that include members who have a high level of perception of sanctions, reward, and efficacy should demonstrate a higher level of compliance than groups that do not have members with these attributes. In other words, groups with members who are knowledgeable about sanctions and rewards with the accompanying self-efficacy will have higher levels of group compliance.

Our study will not just average individual compliance motivations, because this may neglect the substantial underlying heterogeneity in compliance motivators. That is because group members possess different levels of compliance motivators. For instance, previous innovation diffusion studies reveal that individual characteristics (e.g., personal propensity, age, and gender) partially determine the populations of early and late adopters (Wejnert 2002). Individual differences of compliance motivators within a group are partially derived from task characteristics in terms of whether the task is cooperative or individual. For example, an employee may be assigned the task of contacting member companies in order to conduct a specific exhibition, even though the project team may be responsible for the overall preparation of the exhibition. Other tasks may be cooperative and interactive: Selecting an exhibition theme would be based on group decisions rather than on the ideas of just one employee.

It is important to consider how compliance motivators are structured in a work group since heterogeneity of compliance motivators is influential. In predicting group security compliance, the social structure of compliance motivators in a group may be a more critical indicator than averaging individual security compliance. The interactions between group members in terms of their skills and backgrounds are often an important factor in determining group performance (Tziner and Eden 1985). Certain distributions of skill may be more advantageous than others for influencing group performance. For example, suppose two groups have the same average efficacy in security compliance, but in one group the users who are highly security compliant are also high status and willing and able to share their expertise, while in the other, the top users are inaccessible or difficult to deal with. It seems reasonable to suggest that the first group will do a better job of making use of its members' expertise.

To maximize the group's collective security compliance, members with high compliance motivators should be easily accessible so that they may share their knowledge and assist others in the group. In other words, they should have a high level of centrality within the social network (Freeman 1979). More specifically, they should have a high degree of eigenvector centrality (Bonacich 1972). Eigenvector centrality is the centrality of an individual to whom he or she is connected. A person's eigenvector centrality in the network is a function of having connections with others who are well connected in the network. Eigenvector centrality has been associated with power and influence (Baum et al. 2005) as well as information access (Rodan and Galunic 2004). Thus, individuals with high eigenvector centrality strongly affect the groups they are part of, both because they are well positioned to diffuse information and practices (Borgatti 1995) and because centrality can confer status, making it more likely that others will adopt the concepts and practices of the central person. Group security compliance performance should, therefore, be improved if the most central members of the group are the more compliance-motivated employees.

Centrality—Compliance Motivators Alignment

In this study, we conceptualize the alignment between centrality and compliance motivator within a group as Centrality-Compliance Motivators Alignment, or CCM-Alignment. CCM-Alignment is shown as a
continuum ranging from a strong positive alignment to a strong negative alignment. A strong positive alignment could be made between node centrality and a compliance motivator when the most compliance-motivated employee tends to be the most central. A strong negative alignment could be established between centrality and a compliance motivator when the more compliance-motivated employee tends to be the most marginal. In the study, these three constructs are defined as follows respectively. Centrality security efficacy alignment refers to a state of a group whose members have good efficacy in complying with security policy and are socially centered in group network. Centrality sanctions alignment refers to a state of a group whose members have good awareness and knowledge on sanctions derived from security violation and are socially centered in group network. Lastly, centrality rewards alignment refers to a state of a group whose members have good awareness and knowledge on rewards that can be attained from complying with security policy and are socially centered in group network. Figure 1 provides an example of centrality security efficacy alignment within the social network structure.

![Image](image.png)

* Circle indicates node (i.e., an employee in the group).
** Number in the circle indicates the level of security efficacy of node in 5 Likert scale.

Group level security compliance could be influenced by CCM-Alignment in several ways. First, people who have high centrality could contribute to a group's security compliance by complying with the information security policies directly. Central people in a social network are located in important positions within the knowledge transfer and work flows of the group (Borgatti and Cross 2003; Brass 1984). According to the literature on individual security compliance, higher compliance motivators will be associated with higher individual compliance, and the higher individual compliance of key group members will have greater effects on group compliance.

Second, group security compliance may be enhanced by people located in the center of a social network since they have the ability to support and influence others. Group members could monitor other members' compliance behavior (Herath and Rao 2009a) or ask other members to comply with specific information security policies, such as encrypting email (D'Arcy et al. 2009). In understanding and complying with security policies, people may expect help and advice from those with whom they are connected, so more requests about help or advice could be delivered to central people. If these central people have a greater understanding of safety, sanctions, reward, and the ability to carry out security policies, their help or advice could be more valuable in enhancing group level compliance performance. Furthermore, sharing the experiences and knowledge of how other employees go through difficulties with security policy compliance, and understanding the situations that they may face in the organization in terms of information security, may enable central people to provide better support for group security compliance problems. Supporting the employees' security compliance is often not an individual challenge but rather a collective one that requires the involvement and resources of all group members (Siponen 2000). If the highly compliance-motivated people have more centrality in the group social network, they
will easily capture the network resources available and better utilize those resources to address collective problems.

Third, other group members’ security compliance could be influenced by highly compliance-motivated employees. A group’s social network could be an important source of information and attitudes regarding information security policy compliance (Bulgurcu et al. 2010; Herath and Rao 2009a; Herath and Rao 2009b), and higher eigenvector centrality represents greater network influence (Bonacich 1972). Sincere employees, even though they are not the formal leaders of the group, often substantially influence peers’ compliance (Herath and Rao 2009a). According to previous literature, family members who are highly proficient in IT often influence the degree to which other members of the family group adopt and use IT products (Kiesler et al. 2000). If members who are highly motivated to be compliant are central to the group’s social network, they will be better positioned to influence the group in ways that promote effective security compliance. People in workgroups are also more likely to comply with security policies if they perceive that coworkers have been well trained to comply with security policies and have appropriate reasons to do so (Herath and Rao 2009a). The actions and behaviors of central group members are typically more visible than the behavior of other members, so highly compliance-motivated central members may model effective use behaviors and give others the confidence to comply with security policies.

In other words, whether the result of an individual's greater direct impact on the group's work is attributable to their ability to better help others when needed or to their informal influence that encourages others to comply with security policies effectively, the alignment of compliance motivators with eigenvector centrality within a group should be positively related to the group’s compliance. We state this formally as Hypotheses 1, 2, and 3:

**H1: A group’s centrality security efficacy alignment has a positive relationship with group level security compliance.**

**H2: A group’s centrality sanctions alignment has a positive relationship with group level security compliance.**

**H3: A group’s centrality rewards alignment has a positive relationship with group level security compliance.**

### Research Methodology

Centrality-Compliance Motivators Alignments (CCM Alignments) are used as independent variables. To construct these group level variables, compliance motivators and eigenvector centrality at the individual level will be measured. Measurement instruments of compliance motivators are derived from previous studies, and have been adapted and adjusted for this specific context (Bulgurcu et al. 2010). This survey questionnaire also provides respondents with a roster of group members. Individual centrality scores will be calculated from collected network data by using Netminer (Liebowitz 2005), which is used to calculate individual eigenvector centrality scores. To measure centrality, we use the following questions: (1) On average, how often do you interact with this person? (Never, Rarely, Monthly, Weekly, Daily, many times per day), (2) How close is your working relationship with this person? (Very Close, Close, Normal, Distant, Very Distant). Respondents can rate the frequency (1–5) and depth (1–5) of their interactions with each person in their group. The responses in regard to interactions with individuals will be summed to create a measure of interpersonal tie strength. Asymmetric ties will be symmetrized by adopting the minimum method (Borgatti et al. 2002). This method is standard in social network analysis literature (Hansen 1999), particularly in research of multimodal networks (Kane and Alavi 2005).

Since we are exploring the movement of security knowledge across the network, eigenvector centrality is an appropriate measure for the study (Bonacich 1972). Eigenvector centrality is a node centrality in which nodes are scored more highly depending on their connections to well-connected nodes. It is a recursive measure in which a node’s centrality is proportional to the sum of centralities of the nodes to which they are connected, weighted by the strength of connection (Bonacich 1972). Unlike other centrality measures that explain geodesic paths like closeness and betweenness, the eigenvector centrality does not assume that information only moves along the shortest network path. Rather, individuals share information along multiple paths, and not just the shortest path. Further, eigenvector centrality does not assume that the
information flows from node to node (Ferriani et al. 2009). Instead, the eigenvector centrality assumes that information can move through unrestricted paths or geodesics.

The alignments between compliance motivators and individual centrality for a given group are calculated by the Pearson correlation coefficients between members' compliance motivators and their eigenvector centrality in the interaction network. This method, using correlations as independent variable input, is well developed in social network analysis (SNA) and other social science literatures (Kane and Borgatti 2011). Precedent instances of using correlation coefficients as independent variables are easily found in the literature. For example, Caldwell and O'Reilly (1990) conceptualize person-job fit scores by calculating correlations between job requirement assessments and individual competencies. These person-job-fit scores are used as antecedents of outcomes, including job performance and satisfaction. Another instance is found in Kane and Borgatti’s work (Kane and Borgatti 2011). They investigate the correlations between the social network structures of organizations and members’ information systems proficiency, and these correlations are used to examine the impact on organizational performance. This approach is also similar in multi-level modeling (Bryck and Raudenbush 2001; Snijders and Bosker 2011). In multi-level modeling, regression coefficients from individual level regression are used as data in group level regression (Luke 2004).

In our study, positive correlation coefficients between compliance motivators and centrality imply that highly compliance-motivated members are located in a central network position in the group. For example, when the member of a group has great efficacy in complying with the security policy of an organization has high centrality in a network, this group can have a high correlation coefficient, which can be close to 1, from the relationships between the security efficacy of individual and centrality of individual. High alignment enables compliance-motivated members to benefit other members. On the other hand, a zero correlation means that compliance motivators are distributed randomly in terms of social network centrality. In this case, the influence of compliance-motivated members on other members would not be enough to change the atmosphere of the entire group. Finally, a negative correlation value indicates that highly compliance-motivated members are located in the margin of the social network. In this situation, highly compliance-motivated members have little if any influence on other members since they are not easily accessible. Consequently, continuous correlation values, from -1 to 1, are used in the study as an independent variable.

Dependent Variable

We measure the dependent variable (i.e., group security compliance) as an aggregated form of individual responses on group security compliance. According to the definition of group security compliance presented in the Introduction, we assume that, comparatively, group members have homogeneous security compliance characteristics (Klein et al. 1994), even though some variation does exist among members. Therefore, an aggregation of individual responses on group security compliance responses could represent a group tendency and thus a good justification for researchers who are concerned with such an aggregation (Glick 1985). In addition, after data collection we will conduct the method that calculates inter-rater reliability using the interclass correlation coefficient (ICC) (Shrout and Fleiss 1979), and James’ index (rwg) (James et al. 1993). If further validation is necessary, more discussion will be made to resolve this issue.

This method has been used by other researchers for group-level studies. For instance, Neal and Griffin use the aggregated form of individual response to safety behavior for group-level measurement (Neal and Griffin 2006). Harrison et al. aggregate individual ratings of group cohesiveness to the group level by calculating the mean rating of cohesiveness within each group (Harrison et al. 1998). The assumption underpinning the adoption of aggregates to represent a higher level characteristic is that the aggregated variable represents another form of the construct at a higher level of analysis (Rousseau 1985).

Control Variables

This study suggests additional variables that should be included in analysis of information security because of their potential influence on group security compliance. The model adopts network centralization as a control variable to ensure that the social network structure did not contribute to
differences in group security compliance among groups. As a proxy of dispersion in the centralities of the various nodes, centralization confirms whether the network was represented by a few highly central nodes with remaining nodes in marginal positions (Freeman 1979). We also control group characteristics, including gender composition in the group, average tenure of members in the group, average age of the group, and number of members of the group. According to previous security studies, gender is found to affect security compliance (Herath and Rao 2009b): Females tend to show higher compliance with organizational security policies than males. The organization itself is also included as a control variable to explain potential differences in security compliance behavior among employees in different organizations (D’Arcy et al. 2009).

Further, to control overall level of group compliance, instruction about what is good security compliance and what is bad security compliance will be given to respondents in the survey. Plus, this study will control the impact of variance of the average of group member's compliance motivators (i.e., security efficacy, rewards, and sanctions) by treating them as control variables. In that case, we can isolate and examine the alignment between compliance motivators (i.e., security efficacy, rewards, and sanctions) and group network structure.

Discussion

The findings of this study might offer important contributions to the literature of information security. One of our key contributions is developing and testing the new construct we refer to as Centrality Compliance Motivators Alignment or CCM Alignment. Our new construct will show that a simple inventory of group capabilities, made by totaling the sum of the individual capabilities, is insufficient to understand the function of the group as an ensemble. Group performance and effectiveness depend on the structure and configuration of group resources (Kozlowski and Klein 2000). In this paper, we not only offer the new group-level construct of Centrality Compliance Motivators Alignment as a theoretical concept, but also present a simple and effective way to measure it.

Second, by adopting a social network analysis approach, this study extends our understanding of existing important concepts in the information security domain. We posit that the results will reveal that the differences in the social network structure of group and individual group member characteristics will influence group compliance behavior.

Finally, this study also provides practical implications regarding screening and utilizing employees who have high levels of security knowledge because these employees could be an important factor in enhancing the impact of deterrence initiatives. We hope to illustrate that employees with high levels of security knowledge who are socially accessible will improve compliance and possibly deter security breaches. If a company can determine which person is central to the group or who has a high ability to comply with security policies, a company could also focus its resources on educating that employee on security topics, or even take additional steps to increase that employee’s centrality. In this way, a company can improve overall security education and increase group compliance.

Acknowledgments

The authors would like to thank the track chairs, AE and referees for their detailed feedback for enhancing the scope, methodology, and contribution of our work. We are also indebted to the Dr. Fred Dansereau for offering valuable help for the group level analysis issue of the paper.

References


