The African Journal of Information Systems

Volume 10
Issue 4 *Special Issue: Information Technology and the African Networked Society.*

Article 1

September 2018

An Organizational Communication Approach to Information Security

Kofi Arhin
Ghana Institute of Management and Public Administration, karhin@gimpa.edu.gh

Gamel O. Wiredu
Ghana Institute of Management and Public Administration (GIMPA), gwiredu@gimpa.edu.gh

The African Journal of Information Systems

An Organizational Communication Approach to Information Security

Research Paper – Special Issue

Volume 10, Issue 4, October 2018, ISSN 1936-0282

Kofi Arhin

Ghana Institute of Management and Public Administration (GIMPA)
karhin@gimpa.edu.gh

Gamel O. Wiredu

Ghana Institute of Management and Public Administration (GIMPA)
gwiredu@gimpa.edu.gh

(*Received October 2017, accepted April 2018*)

ABSTRACT

Organizations thrive on efficient information management systems as they support activities. Hence, these systems need to be protected from attacks that threaten their existence and use. Although non-technical information security ideas have been espoused by researchers, they have excluded the role of organizational communication. As such, this study explains information security from an organizational communication perspective. Drawing upon a framework of discourse and organizational change, we analyze an empirical case of how information security in an organization is implicated by communicative actions, deep structures, and communication traits. The analysis reveals that (1) prevention of security breaches is achieved by structures of domination and clarity in communicative action mediated by a reserved communication trait; and (2) response to information security breaches is achieved by structures of signification and legitimation, inter-departmental collaboration, and knowledge-rich communication mediated by an outspoken communication trait. Implications of these insights for theory and practice are discussed.

Keywords

Information security, communication traits, organization, communication, structure, interpretive schemes

INTRODUCTION

In today's global context, effective communication between employees within an organization is key to its growth and development (Karanges et al., 2015; Neves and Eisenberger, 2012). Heracleous and Barrett (2001) emphasize that communication facilitates organizational change or reality. In this paper, we present information security as one of such organizational realities (Safa et al., 2015). Thus, in an organizational context, communication can function as a mechanism for securing or compromising information through the management of people and technology (Backhouse and Dhillon 1996). This

is inherent in the work of Ahmad et al. (2015) who establish that information security is an inter-departmental effort rather than an IT-department-only effort— and inter-departmental collaboration requires a good communication culture (Hoof et al., 2004).

Earlier strategies for securing information were technical in nature with products and tools such as firewalls, intrusion detection systems and antiviruses (Crossler et al., 2013). To complement these efforts, non-technical measures have been espoused to enhance information security. For instance, before an antivirus can work, the user's effort to install it should be considered as part of strategies for securing information. This act of the user can be achieved through organizational policies and training, among others (Safa & Von Solms, 2016). Technical and non-technical measures must be combined at both the prevention and response levels of developing information security interventions (Baskerville et al., 2014). Information security is therefore the process of enhancing the confidentiality, integrity and availability of information (Ning et al., 2013) through preventive and responsive strategies. However, a review of information security literature reveals that the role of organizational communication is under-researched.

This limitation suggests the need for a focused research attention on the problem of organizational communication as an approach to the understanding of information security. A focused attention will transcend the limited attention paid to the problem in existing explanations because it will allow a more comprehensive study of the dynamics of organizational communication in terms of deep structures, communicative actions, and individual communication traits. In view of this, the paper draws upon Heracleous and Barrett's (2001) framework of discourse to explain how and why organizational communication implicates information security. Data from an empirical study of an employment agency's efforts to secure information through communication are analysed to provide the explanation. Hence the research answers the question *how is organizational communication implicated in information security*? This research reveals that (1) prevention of security breaches is achieved by structures of domination and clarity in communicative action mediated by a reserved communication trait; and (2) response to information security breaches is achieved by structures of signification and legitimation, inter-departmental collaboration, and knowledge-rich communication mediated by an outspoken communication trait. The paper is divided into seven distinct sections. Section one introduces the background and motivation of the study. This is followed by the literature and theory section which discusses perspectives of existing research in information security. The methodology follows with the justification for the selected philosophy, strategy, approach and data collection methods. Section four displays the results of the data collected. The data collected are analysed in section five and is proceeded by the discussion and conclusion.

LITERATURE AND THEORY

Information Security

Literature is replete with the usefulness of information to organizations. However, there continues to be a rise on attacks on organizational information resources (Ab Rahman & Choo, 2015; Thomson and van Niekerk, 2012). Von Solms and Van Niekerk (2013) posit that all information security efforts are founded on three principles namely; the confidentiality, integrity and availability (CIA). These three principles are collectively known as the CIA triangle. Although there have been arguments suggesting the CIA is not broad enough, Sumra et al. (2015) assert that the CIA triad is the major component of all information security goals. Confidentiality of information refers to a state whereby information is inaccessible to unauthorized persons. Integrity means that information cannot be modified or corrupted by unauthorized persons. Availability refers to the ability to access information when it is needed. For the purposes of data collection, the study adopted Farahmand et al.'s (2004) breakdown of threats to organizational information into five (5) broad headings. These include i) destruction of information

and other resources (Availability), ii) corruption or modification of information (Integrity), iii) theft, removal or loss of information and/or other resources (Confidentiality, Availability), iv) disclosure of information (Confidentiality) and v) interruption of services (Availability). Evidently, the inability of an organization to secure its information is a threat to the organization's very existence.

Baskerville et al. (2014) assert that strategies to tackle threats to information security should be implemented at both prevention and response levels. In agreement with this, Cezar et al. (2013) reveal that it is impracticable to attain information security goals in an organization without combining prevention, detection and response strategies. However, we find detection to be an initial part of the response to security breaches as explained by Baskerville et al. (2014). Previous strategies for tackling challenges with information and computer security in organizations have been technical in nature (Kolkowska and Dhillon, 2013). Examples of these technical strategies include antivirus, firewalls, intrusion detection systems, among others. However, threats to information continue to rise (Crossler et al., 2013). As such, non-technical measures of securing information have been proffered to augment technical efforts (see for example Dhillon et al., 2017). Although there is a growing emphasis on literature that advocate for non-technical strategies, the role of organizational communication in securing information has been overlooked.

Pattinson and Anderson (2007), in an attempt to contribute to information security from a communication perspective focus on one aspect of verbal communication, that is, text, and the initial stage of information security strategy, that is, prevention. They admit that their findings could have been improved had they expanded the concept of communication and information security strategy. They however argue that their findings were enough to claim that communication does play a vital role in securing information. Stavrou et al. (2014) also relate information security concerns with organizational communication and people's intentional acts. However, their explanation of information security is only conceptual because it draws upon a literature survey of existing approaches. Moreover, it also focuses more on the broad issue of responsible organizational actions than the subsidiary issue of organizational communication.

Other proponents of a broader socio-technical approach to addressing organizational information security problems advocate for involvement of managers to enforce policies to prevent external attacks (Baskerville et al., 2014). This has also contributed to the development of frameworks, manuals, and strategies of communication to align employees to organizational goals. However, Richmond, et al. (2001) argue that the fact that an employee is "told" something does not necessarily mean that the same employee has been communicated to. For example, in the situation where an employee is provided a security manual to study and adhere to, there is no guarantee that he or she is going to act according to what has been communicated in the manual. Uffen et al. (2012) also in a bid to explain how personality traits affect information security in organizations focus on the role of managers, ignoring other employees who are one of the main targets of information security interventions. Their work centers on personality traits rather than communication when throughout the study it is evident that one can identify a person's behavioral trait through the way they communicate whether verbally or non-verbally. Lowry et al. (2015) also espouse the need for studying why individuals react the way they do to organizational information security policies. They found that clearly communicated actions have the tendency to deter computer abuse in organizations. However, their study fails to explain the factors that influence communication within the organization such as the structure, traits of the individual and the nature of communication (Heracleous and Barrett, 2001) with regard to the organizational policies.

Burns et al. (2017) adopt the Psychological Capital framework in explaining and predicting approaches to securing information in organizations. They emphasize the role of employees (insiders) in securing information. Their study reveals that security goal setting, participation and contingency planning, among other strategies are required to enhance security in organizations. However, without an

understanding of communication, these strategies cannot be achieved (see Neves and Eisenberger, 2012).

This paper therefore advances arguments for an organizational communication approach to securing information.

Organizational Communication

Communication has been conceptualized diversely as verbal and non-verbal dialogue between a speaker and a listener (Nickolayev et al., 2015), as informing, entertaining, rousing and irritating (Wallace and Roberson, 2009), and as a movement of information from a source through a channel to a destination (Shannon, 1948). Hahn et al. (2001) also point to factors such as individuals and common set goals as playing vital roles in communication. Contextual factors such as deep structures, set goals and task satisfaction levels interplay in interactions between individuals (Goffman, 1982). Through interactions, Heracleous and Barrett (2001) suggest that organizational communication is influenced by relations which are not visible but observable. According to their Discourse Framework of Organizational Change (see figure 1), these relations are shaped by a combination of people's communicative actions, their interpretive schemes and the deep structures. As shown in figure one below, the theory assumes that discourse is a duality of communicative actions and deep structures which are mediated by interpretive schemes.

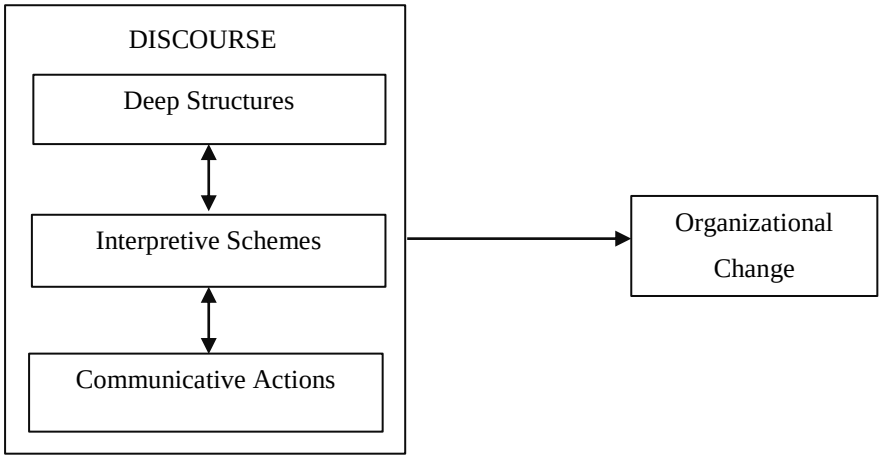

Figure 1: Organizational Change as Discourse [Adapted from Heracleous and Barrett (2001)]

Deep Structures

Organizational deep structures are categorized as structures of signification, legitimation, and domination (Giddens, 1984). These structures are considered to be abstract in nature and require a deeper understanding of what is seen (Jones and Karsten, 2008). They provide a subtle understanding of how and why things are done in society. For example, one is able to identify a soldier by the uniform he or she wears. Their choice of dressing is informed by structures of signification. Additionally, we can determine the role an employee plays in an organization by observing the tasks performed and the tools used. For instance, resolving information security issues is a preserve for employees with some knowledge in information security. The power that the management of an organization possesses that enables it to implement policies to guide the behavior of employees is an example of structures of domination. Safa & Von Solms (2016) emphasize that top management play a critical role in securing information through the development and execution of information security policies. When an employee goes against such policies, management can draw on structures of legitimation to contend with or apply sanctions to the culpable employee. However, Ahmad et al. (2014) postulate that giving

managers the right to sanction employees who do not comply with information security policies may have an adverse effect on securing organizational information resources (see also Herath and Rao, 2009).

In an organization, communication is affected by the structures of signification, legitimation, and domination (Heracleous and Barrett, 2001). Hage et al. (1971), in agreement with this assertion, explain that it is these structures that influence coordination and design of organization processes. Teixeira et al. (2012) also proffer that the structure of an organization informs the way individuals in an organization communicate, relate with one another and use their authority. Structures provide the rules and resources within which communication can be performed (Heracleous and Barrett, 2001). While Giddens explains that societal behavior is founded on the structures of signification, domination and legitimation, Heracleous and Barrett explain that communication occurs within the context of these structures. As such, it is not prudent to discuss information security policies and behavior in organizations without an understanding of these structures.

Communicative Actions

During organizational communication, what is communicated is as important as the factors that influenced the action performed after the communicative action (Searle, 1969). Searle describes what is communicated during an interaction as a Locutionary act. The goal of locutionary acts is to get things done. However, locutionary acts when uttered could result in more than one possible action. These possible actions are called illocutionary acts. Perlocutionary acts are the actions that are performed after an utterance (or a locutionary act) has been made. Collectively these make up the constructs of the Speech Act Theory (Searle, 1969).

Therefore, locutionary acts are the first stage of communication. Once a message is constructed and communicated, regardless of whether it has been received by the intended recipient or not, it can be classified as a locutionary act. This is because these words can be independently analyzed. Illocutionary acts are the intended meaning of the message that was constructed. That is the second stage. They are then followed by Perlocutionary acts. Perlocutionary acts are the actions performed after the constructed message was communicated. That is the third stage. We realize therefore that the messages constructed at the first stage (locutionary) lead to an action performed at the third stage (perlocutionary). These classifications are necessary because the theory espouses that locutionary acts do not always lead to perlocutionary acts. However, for a perlocutionary act to have been performed, there should have been an initial locutionary act. For example, Herath and Rao (2009) reveal that directives contained in information security policies in organizations are not always adhered to. This points to an inherent gap between "what is communicated" (locutionary) and "what is done" (perlocutionary). While Siponen et al. (2014) emphasize that compliance to organizational information security policies is essential to securing information, it is germane to understand the critical role of locutionary, illocutionary and perlocutionary acts contained in these organizational policies.

Interpretive Schemes

Apart from deep structures and communicative actions, the interpretive schemes of people influence how they receive or react to communicative actions. These interpretive schemes are manifested by people's communication traits. Communication traits are described in terms of what is labeled as an individual's communication area (Beck, 1994; Brown and Harvey, 2011); namely, the open / free activity, blind, hidden, and unknown activity areas. The open area (FA) refers to the phenomenon where people's motivation and behavior are known to themselves and also to others through communication. The blind area (BA) is where others know more about us than we know about

ourselves through our interaction with them. The hidden area (HA) represents the experience where we know more about ourselves than others do about us through communication. The unknown activity (UA) area explains the occurrence where neither a person nor other people are aware of certain behaviors or motivation through communication or the lack of it. According to Beck (1994) the free activity area is characterized by a balanced giving and receiving feedback regularly. People with a dominant blind area are quick to express their views and rarely make room for receiving feedback. Receiving but not giving feedback during communication characterizes a dominant hidden area. People in this quadrant avoid decision-making and are quick to delegate powers to others. People with a dominant area of unknown activity are neither good feedback givers nor receivers. Unless the situation critically demands it, they rarely initiate a communication process. Hence, they are seldom able to receive feedback.

Boorom et al. (1998) explain that communication apprehension and interaction involvement are traits exhibited by people during the communication process. They emphasize that communication apprehension influences interaction involvement which ultimately affects the outcome of sales in an organization. Limon and La France (2005) also present another perspective of individual communication traits. They emphasize that communication is influenced by a person's willingness to communicate, interpersonal communication competence, and verbal aggressiveness. In addition to communication apprehension, Martin and Myers (2006) introduce additional traits namely; "talkaholicism," assertiveness, responsiveness, and flexibility. We find that the explanation given by Boorom et al., Limon and La France and Martin and Myers overlap one another, and are largely influenced by Beck's classification, although not explicitly stated by the authors. As such, we argue that communication apprehension, interaction involvement, competence, verbal aggressiveness are all influenced by a dominant open area, hidden area, unknown area or hidden area.

Sommestad et al. (2014) allude to the fact that not all employees adhere to organizational information security policies and directives. As such, it is necessary to understand the individual interpretive schemes that mediate these communicative actions performed by management who are the custodians of information security policies.

In summary, we adopt Heracleous and Barrett's theory to explain how organizational communication contributes to securing information within an organization. The framework views organizational communication as an iterative composition of deep structures and communicative actions, mediated by interpretive schemes. The framework posits that it is through communication that actions are performed in the organization. For instance, for a security breach to be resolved, it needs to be reported to the appropriate department. This report is made in the form of a communicative action and will eventually lead to the recovery of operations. Our adoption of the framework is founded on the apparent gap in literature regarding the explanation of information security from an organizational communication perspective. We therefore perceive information security as one of the organizational realities presented in the organizational communication framework by Heracleous and Barrett (2001).

METHODOLOGY

This research is informed by an interpretivist philosophy (Venkatesh et al., 2016; Sobh and Perry, 2006). Interpretivist research is founded on the principle that people are intelligent enough to create and infer their own meanings from their interaction with the world around them (Orlikowski and Baroudi, 1991). The ontology of interpretivism is that reality is socially constructed, subjective, may change, and is multiple in nature. Leeds-Hurwitz (2009) explains that, central to social construction are two underlying assumptions: people rationalize their experience by developing a model of the world and how it works; and through language, people construct reality. Also, the epistemological dimension for interpretivism points to the explanation of social phenomena through subjective

meanings (Sobh and Perry, 2006). Our choice of philosophy is based on our understanding that organizational communication is an interaction between people influenced by external factors, hence, it requires an explanation of findings based on intelligence and reason.

The strategy employed for this research was case study. This was informed by the authors' choice of organizational communication and information security as the variables for this study. Baxter (2006) suggests that a case study is required when the focus of the study is to answer "how" and "why" questions; when the researcher cannot influence the behavior of the subjects of the study; when the research seeks to be conducted in a specific context; and/or when there is no clear-cut boundary between the phenomena under study and its context. This research satisfies at least the first three conditions. It addresses the question of how organizational communication affects information security; the researcher has no stake in the organization that will make respondents feel obliged to heed to his instructions or commands and the context for this study is organizations that create, store and share digital and non-digital information.

The methods used to collect data were interviews, questionnaires, observation and document studies. Data collection was done between the periods of January 2015 to March 2015 by the authors of this study. Interviews were required to provide an understanding of responses given in questionnaires and observed phenomena. These methods were combined to ensure that responses given were as close to the truth as possible. For instance, if an employee was said to have a dominant UA area, there had to be some form of interaction between the researcher and the employee to confirm the case. Data were collected over a period of ninety days. A total of twenty-one respondents were covered in the data collection process. This covered all employees of the organization used as the case study. Interviews elapsed an average of thirty minutes whereas the administration of questionnaires took a mean duration of twenty minutes per respondent. It was necessary to conduct interviews after respondents completed questionnaires to gain a deeper understanding of some of the responses given. Also, three meeting sessions were observed on three different days to assist in establishing inter-departmental collaboration efforts. Data collected sought to group employees of the organization according to Beck's (1994) classification, identify the prevailing organizational structure, collect data on information security breaches, and observe processes and interactions between employees while executing their duties, among others. After explaining the attributes of each communication area to respondents, they were asked to choose which of the areas they belonged to. To confirm the results, employees were observed during the period of the data collection to ensure that responses given were accurate. The interviews conducted also sought to facilitate discussions on organizational information security policies.

To help analyze the data collected, this paper adopts a semiotic (Fiol, 1989) mode of analysis. Semiotic analysis identifies rules that regulate the activities of an organization with regards to how signs are interpreted. Myers (1997) proffers that semiotic analysis emphasizes the conceptualization of words and signs that can be grouped into categories. However, these categories must be related to the theory that guided the arguments advanced in the research. Hence, relevant data collected were grouped according to our theoretical framework adopted from Heracleous and Barrett (2001). There are three types of semiotic analysis: content analysis (Hsieh and Shannon, 2005), conversation analysis (Wooffitt, 2005) and discourse analysis (Dijk, 2011). According to Hsieh and Shannon (2005), content analysis is used to interpret data from texts. The task of the researcher is to find structures and patterns in text and present their meanings based on regularities. Wooffitt (2005) establishes that, conversation analysis is concerned with interpreting verbal interactions. Conversation analysis assumes that interpretations can be draw from exchanges between people. Van Dijk (2011) proffers that discourse analysis is a combination of both content and conversational analysis. The processes of content, conversation and discourse analysis started by first using data collection methods that supported the collection of data on text, verbal, and non-verbal communication between employees of Cadabra. For instance, the study used observation as one of the methods to monitor and record conversation between

respondents. The data was then coded into themes under deep structures, communicative actions, interpretive schemes, information security issues, information security prevention, and information security response. This was done by going through the data repeatedly and categorizing them according to their relevance to the research topic. Inferences were then drawn to highlight facts, patterns and knowledge that helped to explain the role organizational communication plays in securing information.

RESULTS

Cadabra Recruitment (pseudonym), the selected organization for the case study, is a Ghanaian Human Resource Company with twenty-one (21) employees. The organization works with three (3) key target client groups, namely, employers, job seekers and micro, small and medium scale entrepreneurs. It was also discovered that the dominant communication area at Cadabra was UA (38%), followed by HA (29%), and BA(19%) and then FA(14%). We arrived at this by asking respondents to determine which area they belonged to after explaining the four different traits to them. They were also asked to identify the areas in which other employees in the organization belonged to. We then proceeded to confirm the results through observation and interviews. For the purpose of this study, we replace the names of employees with pseudonyms. The Chief Executive Officer is the CEO, the Chief Operating Officer is the COO, AA is the head of the Information Technology (IT) department or the IT Manager. Pseudonyms starting with A work in the IT department. BB is the head of Finance and Administration or the Finance Manager, hence all initials starting with B work in the Finance and Administration Department. CC is the head of Recruitment or the Recruitment Manager, therefore all initials starting with C belong to the Recruitment department. DD is the head of Training and Development or the Training Manager, as such, all pseudonyms starting with D work in the Training and Development department. The table in the Appendix summarizes the results regarding the four communication traits and the frequency of communication.

At Cadabra, data pertaining to transactions include new business volumes (that is, the number of new customers who request for services), number of vacant positions filled for customers (pertaining to recruitment), total revenue, total expenditure, available jobs, website traffic, and total number of registered users. According to them, the listed transactions recorded information that was meant to be kept secure. These are stored on Cadabra's online server with restricted access and designated roles for each user. The server hosts Cadabra's website and the software that is responsible for capturing the information presented in the previous section. These are hosted on an online Linux Database. The website is open to the public and serves as a portal 1) for jobseekers to create profiles which are eventually stored in the database, 2) for employers to create profiles and advertise vacant positions, and 3) for recruiters to post new jobs. All employees have access to the software based on their individual roles.

In addition to the online server, Cadabra makes use of Google Servers to store important digital documents. These are stored on Google's online Google drive. Documents stored on Google drive include customer agreements, sample of employee contracts, monthly reports prepared from information retrieved from the TPS, employee manual, standard operating procedures, company profile, and service policy. This server also stores a list of all employee tasks. Access to all of these technologies and systems require internet connection. Cadabra does not have an elaborate information security policy or framework. However, organizational documents contain information security components which are discussed in this section. Upon recruitment, new employees are presented with some official Cadabra Recruitment documents. The documents are 1) employee manual 2) standard operating procedure and 3) employee contract. It was discovered that 67 percent of employees were aware of information security policies; and 23 per cent of employees were not aware of documented policies. We went beyond the responses given to find out if employees who claimed to be aware had

indeed read them. It was discovered that employees with UA communication characteristics formed a greater proportion of those who were aware of the policies. Below is an extract from the employee contract:

"No Cadabra team member shall share or divert information from the Cadabra clients' database of both jobseekers and employers to 'self' or any third party for any use that is not authorized by Cadabra. Any such action will be treated as illegal and result in prosecution."

"Cadabra team members will respect and adhere to all Non-Disclosure Agreements (NDAs) signed by the individual, and by other team members who represent the company as a whole, in business transactions for internal Cadabra purposes, or with external clients. The employee agrees not to use or disclose to any person or entity, any confidential information or materials of Cadabra or any other Cadabra clients and its partners, except as directed by Cadabra in the performance of Cadabra-related duties. The employee agrees not to use or disclose to any person or entity any confidential information on Cadabra or any other Cadabra clients – including, but not limited to vendors and other third party clients."

"The employee agrees not to use or disclose to any person or entity, any confidential information or materials of Cadabra Human Capital Ltd. and its partners, except as directed by Cadabra in the performance of Cadabra-related duties. The employee agrees not to use or disclose to any person or entity any confidential information on Cadabra clients – including, but not limited to jobseekers, employers and vendors".

Cadabra's monthly reports included information security breaches that had occurred over the years. However, only those of January to March 2015 were made available for the study. Within this period, Cadabra's reports recorded four (4) security breaches. Aside these security breaches, three (3) other breaches were recorded in February and March during data collection through observation. These three (3) security breaches were caused by the disruption of Cadabra's internet services. Hence, employees could not access information on the server.

Below is the interaction that ensued during a security breach that occurred on February 09, 2015. C6 was the first to discover that the internet was not working, however, it was D2 who reported it first by going to A2's office. The conversation that ensued were between A2 (UA trait), AA (HA trait) and D2 (BA trait).

D2 to A2: "A2, please the internet is down again!"

A2 to D2: "Ok, I'll work on it."

After about thirty minutes, AA walks into A2's office with the same issue.

AA to A2: "Hey, the internet isn't working. Have you restarted the broadband?"

A2 to AA: "Yes, I have"

AA to A2: "Have you called, Momo Internet Services (pseudonym)?"

A2 to AA: "No, I haven't"

AA to A2: "Please do".

A2 proceeds to call Momo Internet Services. After another thirty minutes, the internet is restored. A2 receives a call from Momo.

A2 to Momo representative: "Yes it's working now. Thank you."

A2 sends a Skype message to employees.

A2 to all staff: "The internet is working now everybody"

In another instance, the availability of information was compromised. In the data gathered below, we describe what ensued at Cadabra. C4 successfully entered her username and password in Cadabra's online system and then the following interaction proceeded:

C4 to C5: "Barona Survey is the only client to be registered?"

C5 to C4: "Yes, that is the only new client"

At this moment C4 completes the form and proceeds to confirm the entry but an error is displayed. The interaction continues below.

C4 to C5: "unable to register client" That's what the form is saying! Please help!"

C5 then tries to register the new client herself but also fails. The interaction continues.

C5 to C4: "Yup. True true. Hold on"

C5 to CC: "Hi CC. Please the system is not allowing C4 to register Barona. Can you please talk to A2?"

CC to C5: "Ah again? Sure will do".

All the above conversations were done through instant messaging. C5 then went to A2's (IT Manager's) office but he was not present. She proceeded to send him an email.

CC to A2: "A2, I asked C4 and C5 to register Rabona Survey but they are having challenges with the system again. Can you please check and sort us out? Please, CC."

A2 to CC: "I'm out of the office. I will check it out tomorrow when I come to work."

The above ended interactions for day one of trying to register a new client. The following day, A2 perceived that Rabona had already been registered so he decides to confirm this.

A2 to DD: "Has anyone in your department registered Rabona Survey?"

DD to A2: "Yes we did that yesterday. Why?"

A2 to DD: "C4 tried to register them again but never mind."

A2 to C4: "Hey, Rabona has already been registered by the Training and Development department."

C4 to A2: "Aha, ok, merci beaucoup."

Again, another instance of security breach occurred when an employee (D3 from the Training and Development Department) received a warning from an antivirus software that Cadabra's website contained malicious content. This incident was neither reported to the IT department nor to superiors. Throughout the data collection period, this warning was observed once and only on D3's computer. The warning however disappeared the following day. Further interaction with the A2, the IT Assistant revealed that he had ran a server virus scan the following day. According to him (A2), this was routinely done to ensure security of Cadabra's online data resource. A separate interaction with D3 revealed that he was not aware of this organizational effort (ie. the server scan) to secure information.

In the next section, we analyze how these interactions affected information security at Cadabra using the Discourse as Organizational Change framework.

ORGANIZATIONAL COMMUNICATION AND INFORMATION SECURITY

In this section we present analysis of the data, explaining how and why organizational communication influences securing information. The analysis that follows is twofold: how and why prevention of and response to breaches are achieved by organizational communication. In each argumentation, we

explain how deep structures and individual communication traits bear on communication actions to enable the achievement of information security.

Organizational Communication and Prevention of Security Breaches

Cadabra's communication for the prevention of security breaches is the use of text contained in their employee manual, contract and Standard Operating Procedures (SOPs) as revealed in the previous section. These texts signify locutionary acts as they were given to make employees aware of security risks and sanctions. Adams and Sasse (1999) and Straub and Welke (1998) suggest that awareness of security policies contributes to prevention and deterrence. The locutionary acts contained in the organizational documents were in the form of written directives. A close look at the written policy shows that it has a lot of statements with the words '*agrees not to use or disclose,*' signifying that inaction was a significant perlocutionary act. Awareness of policies was the overall reality the organization hoped to achieve.

However, complying with these policies is largely dependent on the dominant communication area of the employee. It was found from the empirical study that a greater proportion (seven out of eight) of employees with a dominant UA communication trait were aware of the contents of the organizational information security policy texts. People with this trait rarely initiate a communicative action unless the situation critically demands it, signifying that they are more reserved than others. Thus, the intended perlocutionary act of preventing security breaches through the use of organizational written communication was more favorable to such people with UA communication traits than others. Other communication traits give and/or receive feedback either because they find it more difficult to interpret communication or are more likely to challenge messages in a communication. This is not the character of employees with UA communication traits. They neither give nor receive feedback because they either interpret messages more easily or are more likely to accept and comply with them. Prevention of information security breaches is therefore attributable to inaction of employees with a UA communication trait.

The content of organizational policies was evident of structures of domination and legitimation. This is because the policies contained directives and sanctions that were developed by management. However, the nature of domination (because policies were given to subordinates by superiors) and legitimation (because policies were developed and issued by management) were not enough to compel all employees to familiarize themselves with security policies. This played a role in the observation that 67 per cent of employees were familiar with the content of organizational information security policies in the employee manual and contract. Since employees with UA communication traits generally were found to have the highest awareness rate in comparison to other traits, we infer that employees with UA traits abide by policies based on the fact that the documents were passed on from people with a higher authority in the organization. They do this to avoid any form of confrontation or query that might follow their inaction. Hence, structures of domination play an influential role in inducing employees with UA communication traits to gain awareness of organizational communications that are aimed at prevention of information security breaches.

In sum, prevention of security breaches is achieved by structures of domination and clarity in communicative action mediated by a reserved communication trait. Figure 2 below provides a graphical perspective of this assertion.

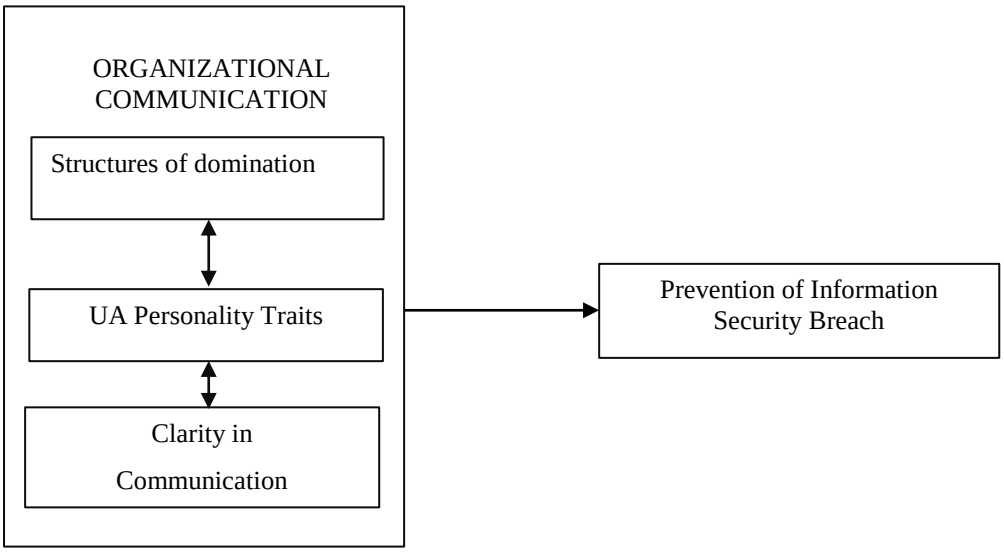

Figure 2: Organizational Communication and Prevention

Organizational Communication and Response to Security Breaches

In the empirical study, it was found that D2 (Training Assistant), whose dominant area is BA (which is characterized by the frequent voicing out of opinions with little opportunity for receiving feedback) initiated the conversation with A2 (IT Assistant) to get the Internet restored (see previous section). We can reason that the Training Assistant's condition for satisfaction was not met because the IT Assistant could not get the Internet fixed at the Training Assistant's request. We deduce that this was the direct result of the Training Assistant belonging to a different department. As such, the Training Assistant did not have knowledge regarding all the possible options that could lead to the resolution of the pertaining security breach. Had this been the case, the Training Assistant would not have stopped at reporting the security breach at the locutionary stage. She would have included what she expected the IT Assistant to do, which is, sharing with him the intended perlocutionary action she expected from reporting the breach to the IT Assistant. Another reason why the IT Assistant refused to try other alternatives to resolve the breach was the fact that the request was made by his colleague and not a superior. Hence, there was no influence by structures of domination.

Although the Training Assistant did not see the process of resolving the security breach to the end, she initiated it. This is key in responding to security breaches. Once discovered, incidents need to be reported (Schwartz and Janger, 2007). The Training Assistant's dominant communication trait is BA, which is characterized by the tendency to give feedback regularly without receiving. Hence, employees who are outspoken, are key to responding to security breaches. This is because they are naturally inclined to speaking out first about issues. Also, we can deduce that the Training Assistant did not inquire about the progress of resolving the breach due to the nature of BAs which prevents them from willingly receiving feedback. Had the Training Assistant followed up on the initial request, other alternatives could have been executed by the IT Assistant.

The IT Assistant who was already aware of the security breach did not take any action. He perceived that the Internet Service Provider (ISP) was already aware of the problem which was not the case. His conclusion on this matter was as a result of his communication trait (UA) which is characterized by

avoiding interaction. Although he could have called the ISP after his first action (restarting the router) did not work, his communication trait (UA), which is characterized by avoiding giving and receiving feedback, influenced his decision not to call the ISP. This trait led to the prolonged resolution of the security breach. We can therefore conclude that interpretive schemes, during security breaches, influence the identification and resolution of threats. Although BA traits contribute positively to resolving security breaches, it falls short with regards to following up on reported security breaches.

AA (IT Manager), a superior of the IT Assistant, initiated a locutionary act (reporting the breach) that began the process of restoring the internet service. While the IT Manager performed a locutionary act, he subsequently followed it with the intended perlocutionary action. His ability to follow his locutionary act with the intended perlocutionary is attributed to his role as the Manager of the IT Department. His headship of the department gives him the privilege of invariably knowing more about the organization than his subordinates. Headship also gives him the privilege to receive more departmental communications than subordinates to increase his knowledge. Additionally, his communication trait affords him the ability to receive feedback and not to give out information. Since more knowledge is gained by listening than speaking (Sticht, 1972), it can be said that his listening had enabled him to know more about the range of possible actions that could address the security problem through interaction with others in the organization. In fulfilment of this expectation, the IT Manager demonstrated a more superior knowledge in IT issues than the Training Assistant. The role of an IT Manager signifies a structure of legitimation. The IT manages role as the head of the IT department is also a structure of signification. Therefore, in responding to security breaches, structures of legitimation and signification are important factors to consider. Again, the Training Assistant's request was left at the locutionary level which occasioned the IT Assistant's interpretation. However, the IT Manager who urged his assistant (A2) to contact the ISP, showed that locutionary acts that are not backed by the intended perlocutionary act left the receiver of the message to decide what to do based on the number of illocutionary options. This is evident in the fact that, while the training assistant did not provide options on how to tackle the pertaining breach, the IT Manager did.

In the third incident observed during the data collection period, D3 from the Training and Development Department, whose dominant area is FA (characterized by the constant voicing out of opinions while leaving little or no room for feedback), failed to reported a security breach to his managers or superiors. We can induce that D3's tendency to give little or no room for feedback influenced his decision not to pay attention to the feedback he was receiving from his computer at the time. Hence, the message that was communicated was mediated by D3's interpretive scheme which supports the constant voicing out of opinions without allowing others to provide feedback. Again, the message that was communicated by the anti-virus was also left at the locutionary stage. The message exposed the threat but did not provide any information on what to do next. This also contributed to D3's inaction since the intended perlocutionary act was not communicated. The lack of interdepartmental collaboration also contributed to D3's inaction. It seems that D3 was not aware of the severity of the security message. He would have paid more attention to security promptings had he belonged to the IT department.

In summary of the arguments advanced in this section, we posit that organizational response to security breaches can be achieved by structures of signification and legitimation, inter-departmental collaboration, and knowledge-rich communication mediated by an outspoken communication trait. A graphical perspective is provided in figure 3 below.

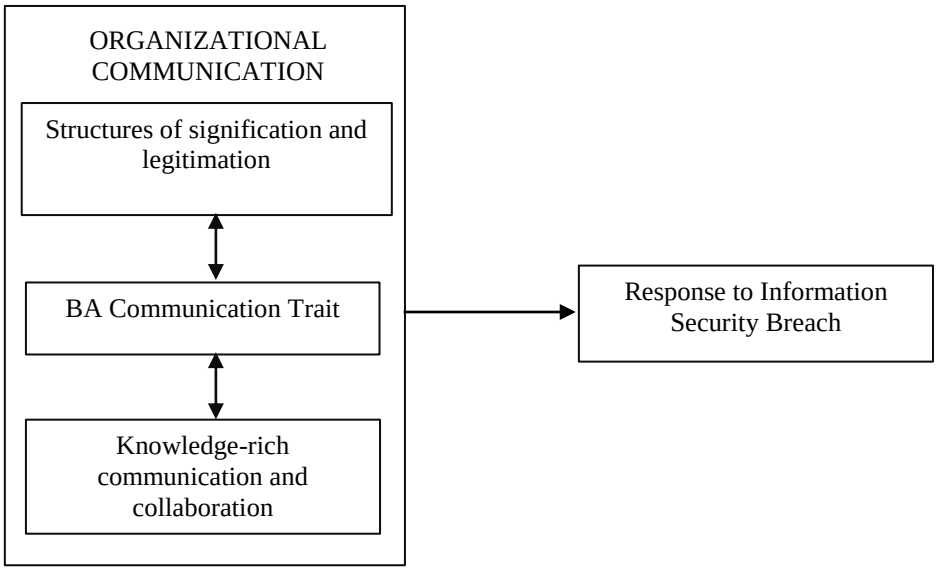

Figure 3: Organizational Communication and Response

Summary of Analysis

Based on the arguments advanced so far, we conclude this section by emphasizing that structures of domination, combined with clarity in communicative action, mediated by a reserved communication trait, supports information security prevention efforts in organizations. In addition, organizational response to security breaches can be achieved by structures of signification and legitimation, inter-departmental collaboration, and knowledge-rich communication mediated by an outspoken communication trait. Figure 4 below shows a synthesized framework from the analysis.

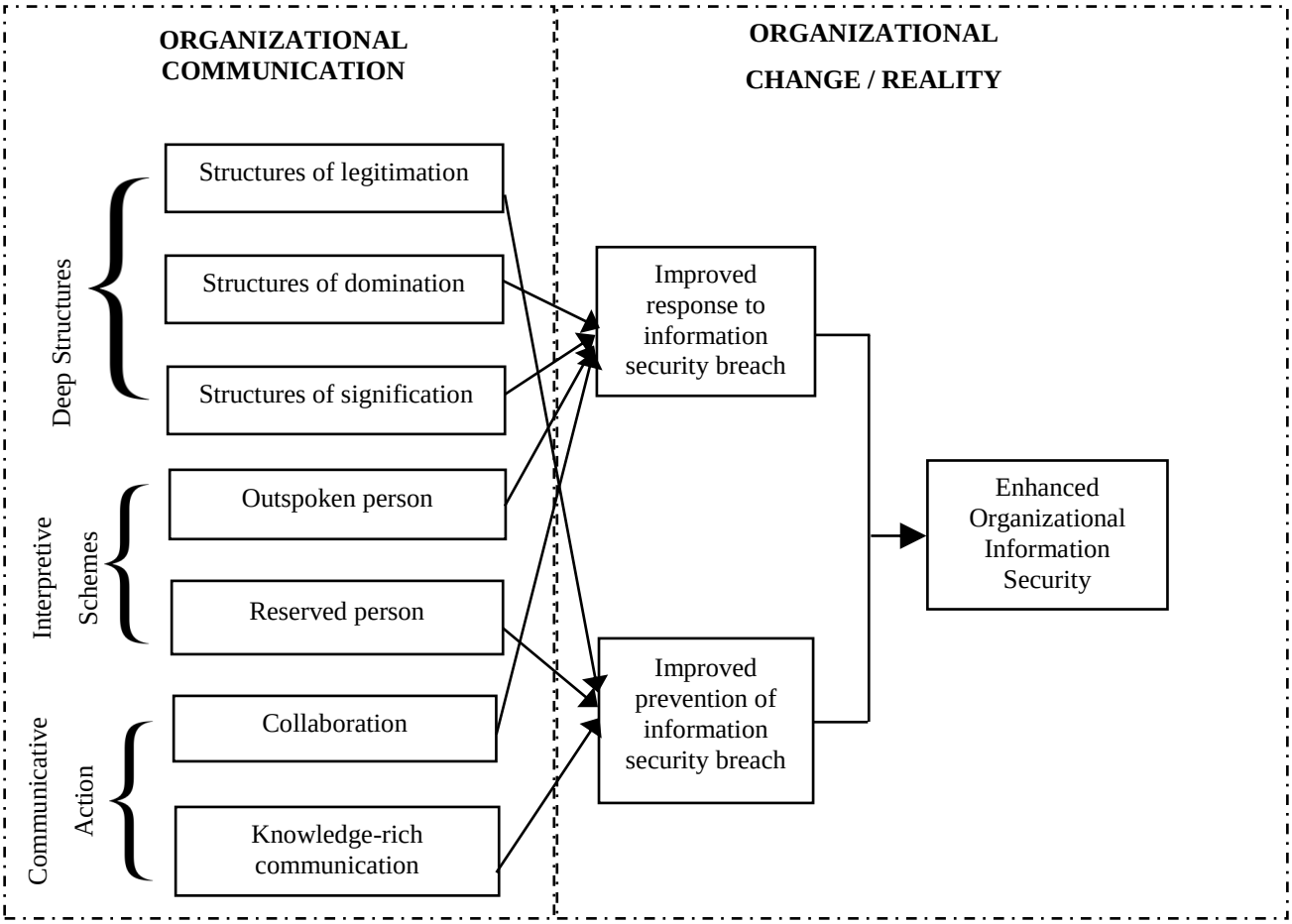

Figure 4: Organizational Communication and Information Security

Figure 4 emphasizes that no single variable leads to organizational reality but rather a combination of at least one variable of communicative action, interpretive schemes and deep structures. The figure also emphasizes the point that improved prevention and response to security breaches are combined to result in enhanced organizational information security.

DISCUSSION

The arguments presented in the previous section suggest that organizational communication cannot be overlooked in developing organizational information security strategies. The structure of the organization, which informs the way communication is done, and the individual communication traits of people are critical factors that need to be considered. Previous research on non-technical measures of securing information in organizations, to a large extent, failed to demonstrate how and why the constructs of organizational communication contribute to organizational realities in the manner in which they do (Baskerville et al., 2014).

Some researchers have focused on the significance of managerial issues in information security compliance (Johnston and Warkentin, 2010). Aside the fact that most of them focus on prevention

only, they present an inadequate explanation of what influences different employees to react differently to the same policies. The study however, provides a deeper understanding on what, how and why employees react or respond to security-related issues in organizations. We emphasize the relevance of frequent collaboration in the analysis. Although this may seem rudimentary, the aim was to represent its significance with regards to information security. The findings revealed that without this, both information security prevention and response strategies will undoubtedly fail to achieve the desired outcome. In addition to frequent collaboration, policies and strategies must be clearly stated and communicated backed by the desired actions. For instance, it is not enough to say that *"all employees must act in a manner that does not compromise the security of the organization"* Additional information on what constitutes insecure actions should be provided.

Crossler et al. (2013) assert that one of the challenges for behavioral research on information security has been improving information security compliance in organizations. Their study is only one of several papers that emphasize that, for a security breach to occur, the individual might have done something wrong, whether intentionally or unintentionally. However, we have presented another dimension of individual behaviors demonstrating that an individual in exhibiting their natural characteristics within an organizational setting also has the tendency to contribute positively or negatively to information security. These naturally characteristics cannot be termed as misbehavior or deviant behavior.

This paper contributes immensely to research in this direction as we have explained why one employee may be compliant while another may not be without any malicious intention. We have explained that it is due to the person's communication trait, the pertaining organizational structure and the type of communicative action received. We asserted that the components of structure, communication traits and communicative actions cannot be overlooked in defining organizational communication. This is due to the critical role these components play in discourse. These three components have not been combined and explained critically as we have sought to do in this paper. Although we adopted Heracleous and Barrett's (2001) framework, we explained further their generalizations. For instance, their framework mentions deep structures but we discussed the different types of deep structures that exist in organizations. The same was done for interpretive schemes and communicative actions. However, we also revealed that one of the shortfalls of their framework was to view discourse as a duality of deep structures and communicative actions mediated by interpretive schemes. We found that interpretive schemes are not always the mediator.

Although organizations may have existing technical and non-technical strategies for securing information, our study provides an additional layer of security to bolster information security. This is because the study provides an understanding of how and why employee response to communicated directives and tendency to react to security threats differ from person to person. We have explained that these differences are as a result of an interplay between deep structures, interpretive schemes and communicative actions. These exposes can form the foundation for information security efforts in organizations. The theoretical contribution of this paper cannot be over-emphasized. The study contributes a theory for explaining (see Gregor, 2006) information security through an organizational communication perspective. This paper therefore contributes to theory building in Information Systems research through explanation; specifically, non-technical information security research.

This study was subject to some limitations. First, the organization used for the data collection is an SME. However, the constructs used in advancing arguments in this paper were not SME-specific. For instance, deep structures, interpretive schemes and communicative actions exist in large organizations too. It is therefore expected that any research conducted using the same constructs should validate the knowledge shared in this study. Secondly, claims were not tested due to the scope of this paper. The focus of the paper was to explain information security through an organizational communication perspective. For further research, we advocate for a positivist study aimed at testing the arguments

advanced herein. Hypotheses can be developed and data collected to contribute to the discourse on securing information through the lens of organizational communication. Also, since the study used data from an SME, we advocate for a separate research using a larger organization to verify the objectivity of the findings and discussions provided in this study.

CONCLUSION

This study sought to provide an organizational communication explanation of information security prevention and response in organizations. Previous studies on non-technical measures for securing information have to a large extent relegated the discourse to the background. The analysis above suggests that clearly written, knowledge-rich, intra-departmental collaboration, reserved and outspoken personalities are the means to achieve information security prevention and response. In view of this paper's deliberations, it is necessary to ensure that communication, whether through organizational documents or any other channels, are supported with the desired result. Findings from the study also show the need for frequent communication within departments to provide a shared platform for interactions between employees. In a department where frequent communication is encouraged, employees who naturally would not communicate with others are presented with the opportunity to do so. From the study, we discovered that to be able to prevent and respond to information security breaches, collaboration allows for the acquisition of knowledge that would have taken, for instance, a catastrophe to be aware of. These ideas are important for an organization is to achieve the security of its information.

REFERENCES

Ab Rahman, N. H., & Choo, K. K. R. (2015). A survey of information security incident handling in the cloud. *Computers & Security*, *49*, 45-69.

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, 42(12), 40-46.

Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing*, 25(2), 357-370.

Ahmad, A., Maynard, S. B., & Shanks, G. (2015). A case analysis of information systems and security incident responses. *International Journal of Information Management*, *35*(6), 717-723.

Anderson, B. B., Vance, A., Jenkins, J. L., Kirwan, C. B., & Bjornn, D. (2017). It all blurs together: how the effects of habituation generalize across system notifications and security warnings. *Information Systems & Neuroscience* (pp. 43-49).

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management*, *51*(1), 138-151.

Backhouse, J. & Dhillon, G. (1996). Structures of responsibility and security of information systems. *European Journal of Information Systems*, 5 (1), pp. 2-9.

Baxter, J. (2006). A case study of intra-community conflict as facility impact. *Journal of Environmental Planning and Management*, 49(3), 337-360.

Beck, C. E. (1994). Perspectives on the self in communication: the cognition continuum and the Johari window. *Technical Communication*, 41 (4), pp. 753-756.

Boorom, M. L., Goolsby, J. R., & Ramsey, R. P. (1998). Relational communication traits and their effect on adaptiveness and sales performance. *Journal of the Academy of Marketing Science*, *26*(1), 16-30.

Brown, D. R., & Harvey, D. (2011). An experiential approach to organization development. Prentice Hall, New Jersey.

Burns, A. J., Posey, C., Roberts, T. L., & Lowry, P. B. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior*, *68*, 190-209.

Cezar, A., Cavusoglu, H., & Raghunathan, S. (2013). Outsourcing information security: Contracting issues and security implications. *Management Science*, *60*(3), 638-657.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. C*omputers & Security*, *32*, 90-101.

Dhillon, G., Syed, R., & de Sá-Soares, F. (2017). Information security concerns in IT outsourcing: Identifying (in) congruence between clients and vendors. *Information & Management*, 54(4), 452-464.

Farahmand, F., Navathe, S. B., Sharp, G. P., & Enslow, P. H. (2004). Evaluating damages caused by information systems security incidents. *Economics of Information Security* (pp. 85-94).

Fiol, C. M. (1989). A semiotic analysis of corporate language: Organizational boundaries and joint venturing. *Administrative Science Quarterly*, 277-303.

Giddens, A. (1984). The constitution of society: outline of the theory of structure. University of California Press, Berkeley, CA.

Goffman, E. (1982). The interaction order. *American Sociological Review*, 48 (1), pp. 1-17.

Gregor, S. (2006). The nature of theory in information systems. *MIS Quarterly*, 611-642.

Hage, J., Aiken, M., & Marrett, C. B. (1971). Organization Structure and Communications. *American. Sociological Review*, 860-871.

Hahn, L., L. Lippert & S. Paynton (2001). Organizational communication. Saylor Foundation, Virginia, USA.

Heracleous, L., & Barrett, M. (2001). Organizational change as discourse: Communicative actions and deep structures in the context of information technology implementation. *Academy of Management Journal*, *44*(4), 755-778.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), 154-165.

Hoof, B. V. D., Ridder, J. D., & Aukema, E. (2004). The eagerness to share: Knowledge sharing, ICT and social capital. Working Paper, Amsterdam School of Communication Research, University of Amsterdam, the Netherlands.

Hsieh, H. F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research*, 15(9), 1277-1288.

Jones, M. R., & Karsten, H. (2008). Giddens's structuration theory and information systems research. *MIS Quarterly*, 32(1), 127-157.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly*, 549-566.

Karanges, E., Johnston, K., Beatson, A., & Lings, I. (2015). The influence of internal communication on employee engagement: A pilot study. *Public Relations Review*, *41*(1), 129-131.

Kolkowska, E., & Dhillon, G. (2013). Organizational power and information security rule compliance. *Computers & Security*, *33*, 3-11.

Leeds-Hurwitz, W. (2009). Social Construction of Reality. *Encyclopedia of Communication Theory*, 892-895.

Limon, M. S., & La France, B. H. (2005). Communication traits and leadership emergence: examining the impact of argumentativeness, communication apprehension, and verbal aggressiveness in work groups. *Southern Journal of Communication*, *70*(2), 123-133.

Lowry, P. B., Posey, C., Bennett, R. B. J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organizational information security policies: An empirical study of the influence of counterfactual reasoning and organizational trust. *Information Systems Journal*, 25(3), 193-273.

Martin, M. M., & Myers, S. A. (2006). Students' communication traits and their out-of-class communication with their instructors. *Communication Research Reports, 23(4), 283-289.*

Myers, M. D. (1997). Qualitative research in information systems. *MIS Quarterly*, 21(2), 241-242.

Neves, P., & Eisenberger, R. (2012). Management communication and employee performance: The contribution of perceived organizational support. *Human Performance*, *25*(5), 452-464.

Nickolayev, V. P., Svintorzhitskaja, I. A., Bondar, I. A., & Ermakova, L. I. (2015). On subtle distinctions between lingual communication and interlingual miscommunication. *European Journal of Science and Theology*, *11*(4), 159-168.

Ning, H., Liu, H., & Yang, L. T. (2013). Cyberentity security in the internet of things. *Computer*, (4), 46-53.

Orlikowski, W. J., & Baroudi, J. J. (1991). "Studying information technology in organizations: Research approaches and assumptions" *Information Systems Research*, *2*(1), 1-28.

Orlikowski, W. J., & Robey, D. (1991). Information technology and the structuring of organizations. *Information Systems Research*, *2*(2), 143-169.

Pattinson, M. R. & Anderson, G. (2007). How Well Are Information Risks Being Communicated To Your Computer End-Users? *Information Management and Computer Security*, 15(5) 362 – 371

Richmond, V. P., McCroskey, J. C., & McCroskey, L. L. (2001). Organizational communication for survival: making work, work. 3rd edition. Allyn and Bacon, Boston, MA.

Schwartz, P. M., & Janger, E. J. (2007). Notification of data security breaches. *Michigan Law Review*, 105, 913.

Searle, J. R. (1969). Speech Acts: An Essay in the Philosophy of Language. Cambridge University Press.

Shannon, C. E. (1948). A mathematical theory of communication. Bell System Technical Journal, 27(3), 379-423.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management*, 51(2), 217-224.

Sobh, R., & Perry, C. (2006). "Research design and data analysis in realism research" *European Journal of Marketing*, 40(11/12), 1194-1209.

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security*, 22(1), 42-75.

Stavrou, V., Kandias, M., Karoulas, G., & Gritzalis, D. (2014). Business Process Modeling for Insider threat monitoring and handling. In *International Conference on Trust, Privacy and Security in Digital Business* (pp. 119-131). Springer, Cham.

Sticht, T. G. (1972). "Learning by Listening" in Frele, R. O. and Carroll, J. B. (eds) Language Comprehension and the Acquisition of Knowledge, Winston, Hillsdale, NJ pp. 285-314.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. *MIS Quarterly*, 441-469.

Sumra, I. A., Hasbullah, H. B., & AbManan, J. L. B. (2015). Attacks on security goals (confidentiality, integrity, availability) in VANET: a survey. In *Vehicular Ad-Hoc Networks for Smart Cities* (pp. 51-61). Springer, Singapore.

Teixeira, R., Koufteros, X., & Peng, X.D. (2012). Organizational structure, integration, and manufacturing performance: a conceptual model and propositions. *Journal of Operations and Supply Chain Management*, 5(1), 70.

Thomson, K., & van Niekerk, J. (2012). Combating information security apathy by encouraging prosocial organizational behaviour. *Information Management & Computer Security*, *20*(1), 39-46.

Uffen, J., Guhr, N., & Breitner, M. H. (2012). Personality Traits and Information Security Management: An Empirical Study of Information Security Executives. *Proceedings from the International Conference on Information Systems, 2012.*

Van Dijk, T. A. (Ed.). (2011). *Discourse studies: A multidisciplinary introduction*. Sage.

Venkatesh, V., Brown, S. A., & Sullivan, Y. W. (2016). Guidelines for conducting mixed-methods research: An extension and illustration. *Journal of the Association for Information Systems*, *17*(7), 435.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97-102.

Wallace, H. & C. Roberson (2009). Written and interpersonal communication: methods for law enforcement. Prentice Hall, New Jersey.

Wooffitt, R. (2005). Conversation analysis and discourse analysis: A comparative and critical introduction. Sage.