https://doi.org/10.48009/3_iis_2019_128-138

Issues in Information Systems
Volume 20, Issue 3, pp. 128-138, 2019

A CASE BASED ANALYSIS OF ORGANIZATIONAL SECURITY GOVERNANCE DIMENSIONS: USER INVOLVEMENT, PROCESS INTEGRITY, AND RESOURCE ALLOCATION

Sushma Mishra, Robert Morris University, mishra@rmu.edu

ABSTRACT

Incidents of cybersecurity breaches are widespread and on the rise. There is more and more evidence to believe that threats to information assets are better mitigated if security controls are reflective of specific organizational context. Organization security objectives are critical to a useful basis for strategic planning for comprehensive security. Based on a study, Mishra (2015) that identifies 23 objectives of organizational security governance (OSG), this study interprets the meaning of these objectives to operational, tactical and senior level executives in an organization. Based on the case study data, the result indicates that the importance of OSG objectives to different segments of employees is dependent on roles they play in organizations. A framework of underlying OSG dimensions: user involvement, process integrity, and resource allocation are proposed. Implications are drawn, and future research suggested.

Keywords: Organizational security governance (OSG) objectives, case study, resource allocation, user participation, business processes

INTRODUCTION

Organizational Security Governance (OSG) is a set of responsibilities and practices used by the management in an organization to provide direction to manage risks and use organizational resources appropriately (ISACA Manual, 2004). OSG offers a set of objectives that guide day-to-day operations of organizations that includes controls aims at reducing risks exposure of IT assets. Information security has traditionally been considered a technical issue, but with growing threats to IT, there has been more awareness about the role of security in boardrooms. Mishra (2015) argues that OSG objectives are critical in managing informational assets in an organization and proposes that these objectives should be reflective of employees' values about the context. The benefits of developing value-driven OSG objectives are that these objectives are contextualized and employees have a sense of ownership of controls arising from such objectives. This study provided 23 OSG objectives that are theoretically grounded and empirically validated. These objectives, however, have not been tested in a real organizational setting.

The purpose of this study is to conduct a case study and interpret the use of these objectives in a real setting. In a hierarchical organizational structure, people have different roles and responsibilities and changed perceptions about what is needed to be done in terms of security goals. This study is set out to address the following research questions:

RQ1: What OSG objectives are important to top management, middle management, and lower management level administrators based on their roles and perception of security?

RQ2: What are, if any, underlying dimensions of OSG objectives and its interrelationship?

The remaining paper is organized as follows. The next section presents a discussion of 23 OSG objectives and their meaning. After discussing the OSG objectives, a description of the case study presented. A discussion about newer insights is presented, followed by a conclusion.

OSG OBJECTIVES

Mishra (2015), using a value-focused approach, developed 23 OSG objectives (6 Fundamental and 17 Means Objectives) that are grounded in Value theory and empirically developed. The list of objectives is presented in tables 1 and 2. Fundamental objectives are the core of the OSG program, whereas means objectives support the fundamental objectives. For a more detailed understanding of these objectives, refer to Mishra (2015). These objectives form the basis of this study. A case study was performed at the organization Alpha to assess the meaning of these objectives to management at various levels. Along with the validity and interrelationships of these objectives at Alpha, the focus was to understand what objectives were important to three different levels of management workforce, namely operational, mid-managerial, and strategic level.

Table 1. Fundamental Objectives for Organizational Security Governance (Mishra 2015)

	Objective	Key Lessons
F1	Ensure Corporate Controls Strategy	Control strategy aligns the security governance and business objectives Antecedent to complete security and process integrity Provides the departments with control plans
F2	Encourage a Controls-Conscious Culture	Risk consciousness in employees creates a “prevention mentality.” Helps in minimizing intergroup rivalry over security governance initiatives Creates an environment where individuals “watch out” for each other
F3	Establish Clarity in Policies and Procedures	Ensure the proper use of the applications and technological solutions instituted Make policies easily accessible Reflect control requirements in the systems Develop visibility of fair policies
F4	Maximize Regulatory Compliance	Meet legal, regulatory and contractual obligations Use compliance as a driver to develop security governance initiatives
F5	Ensure Continuous Improvements in controls	Continuous and iterative control assessment improves the controls environment Understand the organizational context of particular controls Change in roles should be reflected in subsequent controls
F6	Enable Responsibility and Accountability in Roles	Provide clarity in roles and ownership of decisions Promote transparency in roles and avoid sudden changes in responsibility structures

Table 2. Means Objectives for Organizational Security Governance (Mishra 2015)

	Objectives	Key Lessons
M1	Ensure Efficacy of Audit Processes	Have frequent internal and external audits Treat auditors as consultants to assess management’s adequacy
M2	Maximize Clarity in Business Processes	Efficiently designed mature business processes are better protected Provide an end-to-end view of the business process and manage changes
M3	Ensure Communication about Controls	Have frequent debates about controls Develop communications policy for constructive communication within and outside functional groups
M4	Ensure Alignment of Individual and Organizational Values	Promote values such as respect for others, privacy, integrity, self-pride in job and honesty Involve users in the development process to understand an individual’s attitudes and beliefs about security
M5	Ensure Data Criticality	Assess and classify data according to sensitivity Identify data owners to assign responsibilities according to information criticality Link data with authorizations for secure and reliable IT infrastructure
M6	Ensure Punitive Structures	Establish clear consequences and disciplinary actions against non-compliance with policies Explain the meanings of criminal acts and respond effectively in cases on non-compliance

M7	Ensure Clarity in Control Development Process	Develop a favorable perception and transparency of the controls Develop simple, flexible, timely and easy to use controls
M8	Ensure Formal Control Assessment Functionality	Develop formal entity for control assessment Differentiate between lines of business and industries before applying popular OSG frameworks Stakeholder’s viewpoints need to be reflected in the governance process Perform periodic cost-benefit analysis and IT architecture review for the correctness of design for the security controls
M9	Maximize Monitoring and Feedback Channels	Helps in achieving the performance standards set for the IT processes Assures “what is being claimed” is accomplished Incorporate the feedback into the controls
M10	Ensure Visible Executive Leadership	Fundamentally helps in improving the perception of security governance Lead by example and nurture the relationships with employees executive
M11	Maximize Group Cohesiveness	Group behavior influences and shapes individual’ perception of security controls Discourage favoritism and self-interest in groups and manage peer pressure
M12	Maximize Management Commitment	The reward for conformity with controls and encourage values such as dedication, determination, open-mindedness, and truthfulness Establish adequate controls as a “top priority.”
M13	Maximize Resource Allocation for controls	Groundwork before developing controls requires coordination of multidisciplinary functions Allocate appropriate resources in a politics-free environment
M14	Encourage Standardization of Controls	Create systemization in control development process and assess against mechanisms employed by others Benchmark security investments and governance practices to learn from others
M15	Maximize Training and Education	Awareness about social engineering issues can be provided with work-related examples Apply the knowledge in daily practice with focused training and education
M16	Ensure ethical and moral values	Propagate right ethical environment Leadership establishes the right tone of ethics in organizations
M17	Maximize trust building mechanisms	Develop a conducive environment for controls deployment Enhance trust with partners within and outside the organization

METHODLOGY

This research adopts an in-depth case study approach. This qualitative in-depth case study is performed to interpret the meanings of the objectives in an organizational context. Benbasat et al (1987) argue that a field case study helps in presenting a description of the phenomenon under study without disturbing the natural state of affairs. The relevance of the developed objectives needs to be studied in a real organizational setting to bring out their meaning fully. In a natural setting, events unfold in relation to the focus on contemporary issues and this makes a realistic picture of the relevance of the constructs under study emerge.

Organizational Context

The Alpha organization is a state agency responsible for planning, implementation, and maintenance of information technology needs of a large city in Northeast of USA. The organization is in the process of developing security governance program to provide more secure services to its clients, people of the city and also preparing compliance reports for several state and federal regulations. The Chief Information Officer (CIO) is proactive about developing security policies and control structure, working the state internal audit division. Alpha has defined its organizational goals to work with customers and to align business and technology objectives. Organizational security governance (OSG) is identified as a strategic area of improvement by the agency. The security architecture at Alpha is focused in five areas: applications, authentication, networking & infrastructure, physical, and process. The management emphasizes that improving security controls will drive efficiency and effectiveness across the city. The organization's CIO has implemented a new approach to create business technology plans. The strategic plan of the organization is to establish a standard framework and processes that deliver IT services for each agency and establish an enterprise view. Such planning intends to build more enterprise-level targets and evolve from agency-focused goals. The benefits of such an approach are manifold. An enterprise approach by the agency reduces the costs of maintenance and helps manage enterprise level risks. Building standard services leverages the resources and establishes effective partnerships between Alpha and other agencies.

The organizational structure includes the CIO as the head of the agency. Five managers directly report to the CIO. The applications development manager is responsible for all in-house development work. End-user services manager is in charge of operations and support facilities. The infrastructure services manager is responsible for enterprise systems and database administrators. The manager in charge of administration is responsible for training and administrative support functionalities. The newly added project management manager looks after the software development projects in the organization. The organization overall has more than 100 employees at the time the case study was conducted, with several positions open for recruitment, as well as some consultants. The security planning process is tightly integrated and requires an investment of resources from agencies and Alpha. Being the service IT provider for the entire state, Alpha has the additional responsibility of keeping the data and services protected. To provide excellent infrastructure, the organization approaches every agency individually and assesses the agency's information needs and the current state of technology utilization. The management at Alpha considers OSG as a strategic driver for ensuring effective service delivery to the other agencies under the City. The organization is in the process of redefining its OSG objectives and program. The desired changes in the security governance objectives in the new program are reflective of the managements' dedication to developing a critical IT infrastructure free from vulnerabilities. The proposed OSG initiatives were discussed at length with the representatives from the top level, middle level, and operational management in the organization. Depending on the nature of their roles, respondents from each level of the management identified with unique requirements from the proposed OSG program. The interaction with Alpha personnel resulted in three different perspectives on the use and importance of the OSG program. Each of these perspectives is discussed in the next three subsections.

RESULTS

RQ1: What OSG objectives are important to top management, middle management, and lower management level administrators based on their roles and perception of security?

Top management perspective about OSG

The senior management is responsible for defining the strategic direction, providing leadership and resources for the security governance program. By definition, the role of top management is about strategizing and allocating resources for planning purposes (Ansoff, 1985). The CIO emphasized the need for a controls strategy and establishing an ethical environment for the success of any governance initiative (Mishra and Dhillon, 2006). The top management at Alpha believes in commitment to security governance initiatives and how essential it is for the success of the governance program. Establishing separate controls assessment functionality could only help the cause of healthy controls in the organization. As explained by the chief security officer:

> He [CIO] is supportive of our actions. The hard part is getting to his colleagues, the other directors, who need to approve it but have no clue about it. But we depend on the CIO to get the things done. He helps in getting them [other directors in the city council] on board.

The directors at Alpha could identify better with the objectives with leadership and strategic aspects of security governance. The directors believe that security governance at Alpha is about emphasizing the importance of resource allocation for making sense of the controls program. This perspective emphasizes the importance of resource allocation in attaining a robust security governance program. Resources in the form of finances, people and technology are essential for effective security governance. As one participant pointed out:

> A strategy for good governance is good, but we do need the resources, may it be in the form of money, people, or infrastructure.

The CSO explained that the most critical aspect of a good security governance program is creating a punitive structure that ensures that people understand the consequences of the actions. The existing research literature in this area recognizes the importance of the objectives relevant to the top management at Alpha. The need for controls strategy has been articulated in the research literature even though not explicitly. In the literature, there have been clear calls that information security should be integrated into an organization's overall management plan (Perry, 1982; Lane, 1985; Smith, 1989). Perry (1982) argues that computer security and control strategy establishes a climate and need for control. Since strategy is such an integral part of control design, it must be understood and formulated before designing the controls. The organizational strategy establishes the managements' intent, concern, and means to achieve the control objectives (Perry, 1982). Management needs to convey the expectations about the controls to employees. Thompson and von Solms (2008) argue that it is a part of the governance duties of the executive management to encourage employees to adhere to the behavior expected to contribute towards the successful protection of information assets. The executive leadership should espouse that controls are essential and be consistent in response to convey what is advocated is real (Drennan, 1992). The consistency in what is being said is same as what is being done should ultimately lead to the shared tacit assumptions of employees becoming aligned with these espoused values of the organization, thus progressing towards an Information Security Obedient Culture (Thomson and von Solms, 2008). The management has to be proactive and work towards changing the corporate culture, and the resulting employee behavior (Drennan, 1992). Employee behavior can be controlled by establishing punitive structures which allow policing and safeguarding organizational resources within the organization.

Middle management perspective about OSG

Establishing process integrity through efficient auditing practices, standardization efforts, and superior technical competencies come together as critical aspects of information security governance for the middle-level managers at Alpha. The middle management perspective is in emphasizing the due process in achieving process integrity for information security governance. The objectives that emerged as the important ones to the middle-level managers at Alpha are *Ensure Efficacy of Audit Processes, Ensure data criticality and clarity in control development process.* The middle-level managers believe that an audit should be done frequently. The control development process should have clarity, and data criticality should be strived for through adequate access controls and authorization mechanisms. As senior audit manager explained:

> If you don't understand that HR may be the one place you go to. I [an employee] don't understand what it [policies and procedures] means, ask this upfront. Having to own the policies, it [the management] should be responsible for the procedure for this procedure, be responsible for answering those questions. Clarifying the concepts helps people in believe in the governance program in the management.

Also, the objectives *Encourage Standardization of Controls and Maximize trust building mechanisms* were deemed significantly crucial by this group of people. The middle-level managers strived for developing benchmarking standards in controls development. The managers also believed that trust within the organization and with the stakeholders outside the organization is crucial for the success of the organizational security governance program.
Research literature acknowledges the importance of the objectives identified by the middle-level managers at Alpha. Data criticality is essential, and if organizations do not ensure that all employees understand their information security roles and responsibilities, it may become challenging to protect the confidentiality, integrity, and availability of information assets (NIST Special Publication 800-16, 1998, p 12). For governance purposes, it is crucial to understand the business system and the dynamics of business processes within the systems for good security (Savola et al., 2007). It is vital to recognize linkages of information security with business processes and have the abilities to create and distribute new knowledge horizontally and vertically in organizations by using regular business interactions (Savola et al., 2007). This perspective of OSG acknowledges the importance of developing and maintaining process integrity for security governance. Management should be concerned about creation, protection, and distribution of knowledge in the organization as it is a source of competitive advantage (von Krogh, 1998). A controls strategy fits into the overall organizational strategy for business growth, and security is viewed as a strategic governance issue (Lane, 1985, Smith, 1989). All the above measures require trusting people

in an organization to do the right thing at the right time in the right way. Trust measures work within the organization to coordinate and improves the controls initiatives and outside the organization to enhance the perception of security governance efforts of the management.

Lower management perspective about OSG

The operational management respondents comprise security officers, auditing officers, and help desk people. The functional people are the ones who are responsible for the operational efficiency of the business. The staff works with the controls daily, yet their representation in the development process of the control is minimal. This group of respondents identified themselves with the objectives that emphasized the importance of individual user involvement in the success of security governance. There was a unanimous agreement in the group about the importance of having a control conscious culture in the organization. The operational people felt that the culture would guide them in times of confusion.

The objective *Maximize clarity in business processes* was considered very important by this group because it is directly related to their domain knowledge, expertise, and work. Transparency in business processes is crucial to develop controls that do not allow vulnerabilities to seep in the business. *Ensure Communication about Controls* objective advocates well-established communication policies about open discussions on controls between the management and the employees. Communicating was considered crucial by the operational people since it is essential for them to understand the scope and intent of the controls clearly. *Maximize monitoring and feedback* objective is also vital to this group as it provides an opportunity actually to change the controls that hinder the work process. The objective *Maximize Group Cohesiveness* was rated as very important by this group. The respondents felt that peer pressure and behavior of other group members played an essential role in the acceptance of the controls. *Ensure Alignment of Individual and Organizational Values* signifies the importance of individuals' value system aligned with the management's philosophy and organizational values. The respondents felt it was imperative to understand if the corporate values were in line with their value system. The objective *Maximize Training and Education* implied continuous training and education of the end users and members of the operational group felt that unless adequate training is provided to them about the controls, no governance initiative will sustain in the long run. As mentioned by a security officer:

> They [users] need to be educated about the initial controls as well as the reasons for the change. Communicate clearly and effectively about the changes in controls because things change, business needs change, and so do controls. Business processes should be well understood for this.

The operational management people could identify more with the objectives that represent an underlying theme of the importance of individual participation for the success of security governance. The research supports this conjecture in information security governance area. Conscientious and diligent employees can become the most reliable link in an organization's information security infrastructure (Henry, 2004). Pointing out the importance of individual participation in governance efforts, Thomson and von Solms (2008) argue that the environment within the organization has the most influence on employees' beliefs and attitudes. If there is a misalignment between individual and organizational values, the employees might move in the wrong direction and against the expectation of the management (Kilmann et al., 1985). Such an environment can be detrimental to security governance in the organization and may lead to miscommunication, lack of cooperation from the employees, and complacency in performance (Sathe, 1983).

RQ2: What are, if any, underlying dimensions of OSG objectives and its interrelationship?

Based on the emphasis of three levels of employees in the organization about OSG objectives, the initial 23 objectives were clustered in 3 different dimensions and labeled based on the underlying idea they represented. The three perspectives at various management levels at Alpha suggest three new dimensions of organizational security governance: user involvement, process integrity, and resource allocation. A synthesis of the three perspectives indicates the relevance of all the proposed objectives for Alpha. The emergent perspectives are the conceptualizations of security governance that is reflective of the nature of the work an individual does and the kind of organization the person belongs to. The perspectives from the three levels of management are not something unique to Alpha. Research literature in management and information systems suggests similar dimensions of managerial decision making. Weill and Ross (2004) and Peterson (2004) suggest dimensions or perspectives in organizational governance and claim that actions of decision makers across business units in the organization require three coordination mechanisms namely process based, structural and relational. Process-based mechanisms are the formalization and institutionalization of strategic IT decision making or IT monitoring procedures (Peterson, 2004). This dimension is similar to the middle-level managers' perspective on the importance of process integrity for security governance at Alpha.

The structural mechanisms are formal positions, roles, teams, and committees established to coordinate decision making in business and IT (Peterson, 2004). This dimension is similar to the top level management perspective about strategy and resources at Alpha. It is not surprising that the development of controls strategy and allocating resources for controls emerged as the most important objectives for the top management. The relational mechanisms foster voluntary and collaborative relationships among corporate executives, IT management, and business management (Peterson, 2004) to help in clarifying differences and finding creative solutions to problems. Self-control can be helpful in this environment (Kirsch, 1996). IT staffers often demonstrate a sense of "belonging to the IT team" because of their collective expertise and training. If managers implement clan controls (Ouchi, 1979), self-interested behaviors can be reduced. This dimension is similar to the operational level managers' perspective on the importance of the individual in the success of controls.

The dimensions proposed by Weil and Ross (2004) are in the context of effective IT governance in an organization. Being a subset of the overall IT governance in the organization, information security governance domain can theoretically extend the concepts. All of the three perspectives need to be integrated for designing comprehensive security governance at Alpha. All objectives fall into one or more of these perspectives and are incredibly relevant for the organization. An organizational security governance program needs to be designed along the lines of these underlying objectives such that the benefits from such a program are maximized. Based on the discussion about the emergent themes from the three perspectives, the relationship between the dimensions is shown in figure 1 below.

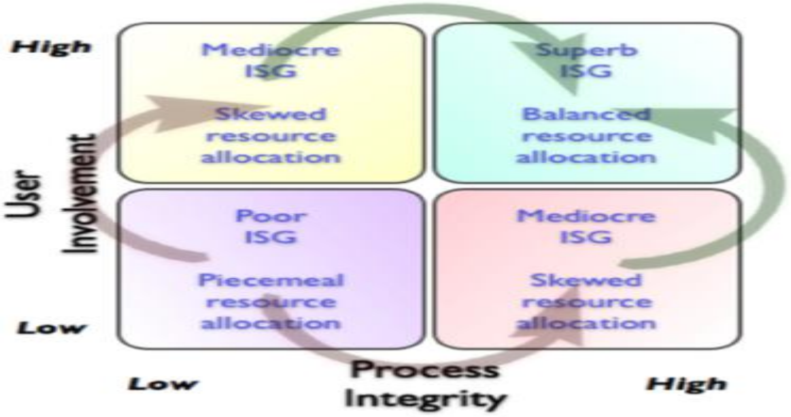
High
Mediocre ISG
Skewed resource allocation
Superb ISG
Balanced resource allocation
User Involvement
Poor ISG
Piecemeal resource allocation
Mediocre ISG
Skewed resource allocation
Low
Low
Process Integrity
High

Figure 1. The User-Process-Resource (UPR) matrix for organizational security governance

The proposed User-Process-Resource (UPR) matrix shows the interdependence of the three dimensions of OSG. In the above matrix, the intersection of the two dimensions, user involvement, and process integrity results in four stages of OSG, dependent on the resource allocation dimension. The lower quadrant on the left side represents low process integrity and low user involvement with piecemeal resource allocation for controls. The result is poor OSG practices for organizations in this quadrant. Moving away from this quadrant in the clockwise or anti-clockwise direction (it would be challenging to move directly in the diagonally opposite quadrant) an organization can either increase process integrity or user involvement. The resources allocation in these quadrants would be skewed in either direction (depending on which quadrant the organization is) resulting in mediocre OSG practices. For example, if an organization is in the top left quadrant, the resources are skewed towards more user involvement and less process integrity initiatives.

Similarly, if an organization is in the bottom quadrant at right, the resources are skewed towards increasing process integrity, and user involvement is neglected. To reach in the ideal state, i.e. the quadrant at the top on the right, where there are high user involvement and high process integrity, requires balanced resource allocation for both the dimensions. Organizations in this quadrant would have superb OSG practices, and this is the desired state to be in.

This matrix explicitly establishes the relationships between user involvement, process integrity, and resource allocation for maximizing OSG in an organization.

DISCUSSIONS

All 23 objectives are considered necessary by the organization and, to some extent, each is being realized by the management through various measures. The data from Alpha supported all of the objectives. A careful evaluation of each objective was performed based on the evidence from the data to corroborate the claim of an Alpha meeting that objective. A critical review of observations, interviews, and artifacts suggests all objectives are essential to Alpha and are in use in some form. However, there were some additional insights, apparent contradictions, noticed in what the management claimed versus what it did. These are discussed below.

Regulatory compliance issues

The first issue that emerged is about the organization's stand on regulatory compliance issue. Explaining the benefits of regulatory compliance, the manager of internal audit division said,

> Regulations are beneficial. It gives you guidelines like there is a blueprint that you are comparing with a real operation to see whether there is a match. If the operation matches the blueprint, that is great. If not, where are the differences? Why are those differences here to begin with? It is very important to have such guidance

Some managers agreed that regulations were a big driver for the organization to revisit its internal controls objectives. With the top management supportive of the compliance efforts, the organization would be able to utilize the opportunity to make a lot of changes it wished for. Some of the members of the management felt that compliance is reactive and take things backward. Any organization that takes its internal controls program back or starts its controls development process looking at the regulations would have difficulty in succeeding good security. People felt that compliance was the job best left to the auditors. The employees have to participate at the minimum, providing what the auditors need to let them off the hook.

Internal auditing issues

The second issue that emerged was about the state of internal auditing in the organization. Almost all of the respondents felt that auditing was crucial to establish the importance of organizational security governance objectives. The CIO believed that auditing added to the deterrence efforts and created a consciousness about the controls. The senior manager added:

> Auditing is no different to that [as a mechanism to inventory in the military]. They [auditors] come in, and they check and look at best practices. We add time to this so that we can follow up on it so that we are compliant with the direction that we agreed to move on it. They [auditors] need to follow up again based on dates that we customers told them to check if we would meet their recommendations.

The management felt that there were several benefits of performing regular audits within the organization. The auditors, who have industry experience, are in an excellent position to assess the performance of the management on security governance issues and provide an independent their party perspective about the state of affairs. The independent assessment assures other stakeholders such as regulators and investors and helps in building the organization's goodwill. Also, the auditors provide a benchmark assessment about the controls and give a direction for the future governance initiatives.

Given the sentiments of employees, it appeared that the organization was frequently audited and took the feedback from the auditors to improve the security governance process. On the contrary, there were very few audits in the organization, and the perception about auditing was not very favorable among the employees. Through observations and informal conversations with employees and managers, it was inferred that at this state agency, auditing, over the years, has been used as a tool to punish agencies that create trouble for the top management. Thus, if a particular department was not following the orders or doing things in a manner which is not appreciated by the bosses higher up, that department or agency was subjected to an immediate audit. This way, the trouble-making department was answerable to the bosses 'higher up' for the findings by the audit team.

Segregation of duties issues
The third issue that emerged from data alludes to the organization's position on segregation of duties. The interview data suggest that, for the most part, management felt that segregation of duties as control was significant for the organization. As shared by the manager, infrastructure services:

> How do you deal with this [internal fraud or security breaches]? Design proper controls. Ensure responsibility and accountability, have multiple layers of controls, segregate duties, have audited. Segregation of work is essential, make sure people in a group just keep doing what they are doing and never cross the line. They should not know about how others do their work.

The security team felt that segregation of roles was a significant control for security governance. It is as vital as designing correct access controls and authorization mechanism for the systems because the inadequate separation of function would provide unauthorized access to people who have no reason to get access to certain things. Observations at Alpha leads to believe that separation of the roles is not done all the times. There have been instances where people have had inadequate accesses in the name of cross-training in the organization. Sometimes, in the name of cross-training, the staff at helpdesk performs the job of assessing the adequacy of their work. There is a helpdesk team (say primary) that takes request from the city users, and there is a team (say secondary) that supports their functions as back up. There is another team (say surveillance) that performs frequent and random checks on the work requests to ensure that all work orders are being addressed adequately. There have been times when the person doing the primary work of support checks his job the next day in the surveillance team.

In Alpha, these discrepancies in "what is being said" and "what is being done" provide an interesting insight into OSG practices. The reasons or motivations for this apparent contradictions warrant a study of its own and is beyond the scope of the current study. There are several contributions to this study. The OSG objectives developed in another study were empirically validated in this case study. The three underlying dimensions of OSG are contributions to theory and practice in security governance domain. It is a contribution to the body of knowledge in this area and can fuel further studies about dimensions of OSG. For practitioners, it provides a tool to assess the effectiveness of their OSG programs and employ measures to improve in all dimensions. Many studies can fuel from these results. It could lead to the development of an OSG assessment tool for organizations scoring preparedness in all 23 areas. The main limitation is that it is a single case study. The results are generalizable to theory but not so much to the population. More studies are required that use other quantitative and qualitative methods to study this topic.

CONCLUSION

The case study at Alpha provided interesting insights into organizational security governance objectives and practices in a real organization. The management in the organization is dedicated to the cause of developing robust OSG practices and thinks proactively about all the aspects of a proper controls program. All the objectives established in Mishra (2015) are reexamined in this case study. All of the objectives are being used in this organization. These objectives are based on theory, grounded in the values of organizational stakeholders and empirically examined through a case study. Implications are drawn.

REFERENCES

Benbasat, I, Goldstein, D. & Mead, M. (1987). The Case Research Strategy in Studies of Information Systems. *MIS Quarterly, 11*, 369-386.

Berk, J., (2006). Change Champions, *The Internal Auditor; 63*(2), 64-69.

Campbell, R., Al-Muhtadi, J., Naldurg, P., Sampemane, G. & Mickunas, M. D. (2002). *Towards Security and Privacy for Pervasive Computing*. In Theories and Systems, Next-NSF-JSPS International Symposium, ISSS 2002, Tokyo, Japan, 2002.

Dhillon, *G. (2001).* Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns. *Computers & Security 20(2), 165-172.*

Flowerday, S & Solms, R. (2005). Real-time information integrity = system integrity+ data integrity +continuous assurances. *Computers & Security, 24, 604-613.*

Goel, S., Pon, D., & Menzies, J. (2006). Managing information security: Demystifying the audit process for security officers. *Journal of Information System Security, 2*(2), 25-45.

Kanter, H., McEnroe, J., & Kyes, M. (1990). Developing and Installing an Audit Risk Model, *The Internal Auditor*, *47*(6), 51-55.

Karydaa, M., Kiountouzisa, E., Kokolakisb, S. *(2005).* Information systems security policies: a contextual perspective*. Computers & Security.24, 246-260.*

Lindup, *K.* (1996). The Role of Information Security in Corporate Governance. *Computers & Security, 15, 477-485*

Mishra, S. (2015). Organizational objectives for information security governance: a value-focused assessment. *Information & Computer Security, 23*(2), 122-144.

Mishra, S. & Dhillion G. (2006). *Information Systems Security Governance Research: A Behavioral Perspective*, 9th Annual NYS Cyber Security Conference and Annual Symposium on Information Assurance, June 14-15 Albany, NY

Rezmierski, V.E., Seese, M.R, & St. Clair II, N. *(2002*). University systems security logging: who is doing it and how far can they go? *Computers & Security, 21*(6), 557-564.

The Institute of Internal Auditors (IIA) (2006), The Role of Auditing in Public Sector Governance, retrieved on 121906 http://www.theiia.org/index.cfm?bhcp=1

Thomson, K., & Solms, R. (2005). Information security obedience: a definition. *Computers & Security. 24*, 69-75.

Melancon, D. (2006). Reaching Compliance Through Foundational IT Controls, IT Audit, Volume 9, December, retrieved on 12/19/06 http://www.theiia.org/itaudit/index.cfm?catid=21&iid=509

Moulton, R., & Coles, R.S. (2003). Applying information Security Governance. *Computers & Security, 22*(7), 580-584.

Roth, J. (2003). How do internal auditors add value? *The Internal Auditor, 60*(1), 33-37.

Swanson, M. & Guttman, B. (1996). *Generally Accepted Principles for Securing Information Technology Systems*. National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce.

Trček, D. (2003). An integral framework for information systems security management. *Computer & Security, 22*(4), 337-360.

Wagner, J. K. (2000). Leading the Way. *The Internal Auditor, 57*(4), 34-39.

Ward, P., & Smith, C. (2002). The Development of Access Control Policies for Information Technology Systems. *Computers & Security, 21*(4), 356-371.

Whitley, J. (2005). IIA Issues IS Audit Guidance. *The Internal Auditor;* 62(3), 24.

Whitman, M. (2003). Enemy at the Gate: Threats to Information Security. *Communications of the ACM, 46*(8), *91-95.*