AMCIS2015 Puerto Rico Paper Submission

Mismatched Understanding of IS Security Policy: A RepGrid Analysis

Full paper

Gurpreet Dhillon
Virginia Commonwealth University
gdhillon@vcu.edu

Ahlam Almusharraf
Virginia Commonwealth University
almusharrafa@vcu.edu

Spyridon Samonas
Virginia Commonwealth University
ssamonas@vcu.edu

Abstract

Professional and academic literature indicates that organizational stakeholders may hold different perceptions of security rules and policies. This discrepancy of perceptions may be rooted into a conflict between the compliance of stakeholders to organizational norms on the one hand, and security rules on the other. The paper argues that a mismatched understanding of security policy can have a devastating effect on the security of organizations, and should therefore be treated as a key reason for non-compliance to security policy. Using *Personal Construct Theory* and *Repertory Grids* we explore how different stakeholder groups within an organization can hold divergent views on the same security policies. Our findings have implications for the design of security policy training and awareness programs, as well as for the institution and internalization of good IS governance practices.

Keywords

Information security policy, Repertory Grid, norm-rule compliance, stakeholder perceptions.

Introduction

A study by Ernst & Young reported that in nearly half of the organizations surveyed information security was not very well integrated with the organizational business strategy. Lack of awareness and insufficient understanding of security requirements were cited as the common reasons (Ernst & Young, 2012). Indeed, various stakeholder groups hold different understanding and knowledge about information security, which is reflected, not only in the design of policies, but also in the practice of security (Vaast, 2007). Albrecthsen and Hovden (2009) suggest that users and managers practice IS security differently because they have different rationalities. Guo (2013) notes similar discrepancies in the understanding of security issues between end-users and IS people, which are essentially linked to a cost-benefit assessment of security policies in the workplace (Padayachee, 2012).

One of the key themes that emerges from research in IS governance and security is the gap in perceptions that exists amongst various stakeholders. Johnston and Hale (2009) articulate it as "discrepancy of perceptions" between information security governance implementers and non-implementers, and between business and information security functions. In terms of IS security and governance, different perceptions of what a security policy might be and what the security rules mean in a given situation can be attributed to various reasons. First, there is a general lack of awareness of the nature, scope and

significance of the security policy amongst the users (Straub and Welke, 1998). Despite extensive research that has led to notable improvements in policy compliance and security awareness in organizations, there is still a need for greater clarity of security policies (Hu et al., 2012; Myyry et al., 2009). Second, there is a need to align security rules with the rest of the business (Briggs and Edwards, 2006; Doherty and Fulford, 2006). Certain aspects of this alignment have been discussed in the literature, particularly in the context of the internalization of security goals and their link to work outcomes (Hu et al., 2012; Myyry et al., 2009; Padayachee, 2012).

User behavior and understanding of security issues is shaped by the interlocking of organizational, technological and individual factors (Albrechtsen, 2007). While awareness programs in organizations are certainly useful, they do not necessary change rationalities or break into what Boland and Tenkasi (1995) consider as 'communities of knowing'. Such communities seem to be very important in the context of security, since "social representations of different occupational communities frame individual beliefs and interpretation of IS security" (Vaast, 2007; pg. 133). However, organizational level factors that influence individual cognitive processes have long been ignored by the literature (Hu et al., 2012). As Tan and Hunter (2002) point out in their seminal paper on the RepGrid technique, an understanding of the values of stakeholders leads them to adjust their perceptions. Hence, the Repertory Grid technique gives us the potential to improve 1) our understanding of how stakeholders make sense of security policies influenced by their norms and 2) the alignment between norm and rule compliance, which can help in the mitigation of security breaches. Each stakeholder uses their own value to understand and interpret the security policies. These personal cognitions are called "personal constructs" (Kelly, 1955).

Using *Personal Construct Theory* and *Repertory Grids* we explore how different stakeholder groups within an organization can hold divergent views on the same security policies. Our findings have implications for the design of security policy training and awareness programs, as well as for the institution and internalization of good IS governance practices.

Theory and Methodology

The Personal Construct Theory

Kelly in the 1950s developed the Personal Construct Theory, which focuses on the personality and cognition of individuals. Kelly (1955) argued that people interpret events around them, and that their behavior needs to be understood in terms of personally constructed ideas and explanations of how the world works. People's interpretations of the world are always subject to revision and alternative reconstruction. Kelly defined human construct as measures by which people make sense of the world they live in. People use a construct system to interpret present events and to predict what will happen in the future. Kelly emphasizes that constructs are bipolar (dichotomous) in nature, which means each construct has a corresponding contrast construct. For example, the construct "good communication" has a corresponding contrasting construct of "poor communication." Using the bipolar labels helps in enhancing our understanding and interpretation (Kreber, et al., 2003; Tan and Hunter, 2002). Kelly (1955) argued that values mean nothing without opposites. The notion of a construct is considered different than what would typically be referred to as a concept. The formation of a construct is founded on similarity and differences in events, i.e. some events are similar in features while others are different. This conception is captured in the dichotomy postulated by Kelly, and differs from our normal thinking. Humans usually think of concepts in terms of absolute categorization where events are ordered along a specific (or a specified) dimension.

The dichotomous nature of the constructs has been central to Kelly's assertions since it emphasizes the distinctions between the contrasts, e.g. warm - cold as opposed to irrelevant contrasts such as warm - flexible. This conception is very similar to what has in the literature been termed as "universe of discourse" (as noted in Boole's studies in logic and probability from 1854). Following decades of research in the literature it has been well established that construct-based, rather than proposition-based, are now the basic cognitive units (see empirical research undertaken by Millis and Neimeyer, 2007).

The Personal Construct Theory makes an important distinction between values and beliefs and how values are situated with a construct. Horley (2012) notes that in Personal Construct Theory values are the core constructs and ordinary beliefs are peripheral constructs. This is an important distinction since values "govern a person's maintenance processes". In the context of IS research, there is common understanding that an appreciation of norms, expectations, values, and beliefs can result in more successful information systems (see Tan and Hunter, 2002).

Repertory Grid (RepGrid)

RepGrid is a technique that was introduced by Kelly (1955) and it is grounded on his Personal Construct Theory. It is used to define 'personal construct systems.' RepGrid is a two-dimensional matrix that captures a construct system with regard to a specific field of experience. It represents the understandings and differences in the constructs of individuals or groups through generating cognitive maps. RepGrid has three components: elements, constructs and links. Elements are the objects of interest within the area under study. For example, the elements can be student and faculty. Constructs represent how the individuals interpret the elements. Example of constructs is "strict access restrictions – no access restrictions." Links are connecting the elements and constructs. The links show how individuals interpret the similarities and differences between the elements and constructs (Kreber, et al., 2003; Tan and Hunter, 2002).

Data Collection and Analysis

Data Collection

This study was undertaken as a case study at a large public sector university in the US. The university was mandated by the state to comply, not only with the Department of Education policies, but also with the NIST and HIPAA guidelines. Compliance of this sort is a federal requirement. The study was conducted over a period of one year. We worked very closely with the university's Technology Services Department. In our study, nine people from the university were selected to participate in this study to reflect different groups of end-users within the University. The participants were divided into three stakeholder groups: students, staff and faculty (three participants from each group). Students participants were used in this study because they are using an assortment of the university's IT resources and services, such as email, VPNs, WiFi and Ethernet networks, on a regular basis and to a great extent throughout the academic year. In this respect, our study treats students as organizational insiders who have access to the university's networks and should conform to any relevant security policies.

It should be noted that small sample size is not unusual in the application of Repertory Grid; small sample size between six and ten participants has been used before (Dillon and McKnight, 1990; Hassenzhal and Trautmann, 2001). However, there are studies where the sample size was even smaller. For instance, Botterill (1989) used a sample of one subject, whereas Phythian and King (1992) used a sample of two managers.

The participants constitute the elements of our RepGrid. Structured, face-to-face interviews were conducted to see how each participant understands security policies. Separate meetings were conducted with each participant. During the interviews, the participants were encouraged to explain how they perceive and understand the university's Information Security function. They were asked how to behave in certain situations based on their understanding of the security policies.

Constructs
1. Complexity of Compliance Requirements for third party
2. Acceptance of Multiple Roles assigned to a single person
3. Necessity of ISO designation
4. Necessity of Separate Organization Structure for security function
5. Requirement of Adequate resource allocation
6. Availability of Awareness Training
7. Classification of data based on sensitivity
8. Enforcement of Compliance maintenance
9. Strictness of Access Restriction
10. Awareness on data protection requirements
11. Importance of Breach Notification
12. Accountability of Non-compliant individuals and units
13. Consequences of Violations of policies
14. Reporting structure of Violations
15. Documentation of Violation
16. Necessity of Business impact analysis
17. System owner involvement in Data handled by the system
18. Restriction on Posting of sensitive info on public site
19. Documentation of Sensitive IT system classification
20. Necessity of Risk Assessment
21. Necessity of Annual Self-Assessment
22. Risk Assessment reports
23. Necessity of IT System Security Audit
24. Identification of Separate plan for each system
25. Necessity of Documentation is
26. Importance of Mitigation
27. Importance of Baselines
28. Vulnerability assessment by scanning the systems
29. Coordination between System Owner and Data Owner
30. Incorporation of Information Security Requirements in system development process
31. Importance of Retention of Data handled by IT system
32. Importance of Disposal of hardware and software verification
33. Importance of Account Management Practices
34. Importance of Selecting and implementing encryption controls
35. Necessity of Physical Security to protect IT systems

36. Necessity of Non-Disclosure and Security Agreements
37. Use of Email for sensitive data
38. Necessity of Role based Information Security Training
39. Necessity of Inventory Management practices for IT Assets
40. Use of Keystroke logging

Table 1. List of the Constructs

The constructs of our RepGrid were elicited from the Information Security policies and standards of the university. A total of 40 constructs were derived. Table 1 includes a list of the constructs that were elicited from the Security Policies and Standards. The responses from the interviews were used to weight the constructs for each element. The weight ranges from 1 to 5; 1 represents the construct and 5 represents the contrasting construct. Figure 1 shows a completed RepGrid. It represents the 40 constructs that were elicited from the Security Policies and Standards of the university. The 9 elements represent the values of the participants. Each construct was weighted based on the answers of the participants.

Rep 5 software, which is grounded on Kelly's Personal Construct Theory, was used to analyze the data and construct cognitive maps. This resulted in cluster analysis, principal components analysis and PrintGrid plots.

Cluster Analysis

The results of cluster analysis help to recognize patterns and main combinations of constructs and elements. RepGrid uses the FOCUS technique (i.e. hierarchical cluster analysis). Figure 1 shows the clusters generated by RepGrid for the elements and constructs. All of the elements have been reordered, so the similar constructs were placed close to each other and the similar elements were placed close to each other. As noted previously, a bipolar construct helps in grasping a superior understanding for the constructs. Thus, the participants can give a clearer interpretation for each construct. Seven constructs have been reversed (27, 29, 17, 24, 2, 7, 38) to highlight the patterns of the constructs. Reversing the constructs was based on the loading on each construct on the first component of the Principle Components Analysis. If a construct has a negative loading, it will be revised to better represent its correlation with other constructs.

By examining the shape of the dendrogram of the elements, we could recognize two main structures: staff1, staff2, staff3, student3 in one, and the rest in another. Examining the constructs' dendrogram resulted in two structures: one distinct (construct 27), and another contains the rest of the constructs. We measured the similarities among the same stakeholders (i.e. measuring the similarities among the members of the same stakeholder group) through analyzing the dendrogram and calculating the percentage of match among the same stakeholders.

Faculty1 and faculty3 had highest similarity among the constructs (84%), and staff1 and staff3 had 80% similarity among the constructs. Similarly, we measured the similarities in how the participants see the construct among the different stakeholders. Our findings indicate that each group of two participants who have high match percentage may have more in common. Thus, even with the high percentage of match between the stakeholders, we still have non-trivial percentage of non-match in stakeholders' values. This reveals the gap amongst the stakeholders' perceptions, which might result from the absence of security awareness. When the stakeholders do not have sufficient knowledge regarding the security policies, they depend on their own values to develop an understanding for the policies, and they, then, behave according to that understanding (Straub and Welke, 1998).

Figure 1: RepGrid FOCUS technique

On the other hand, we measured the similarities among the constructs; we found 100% similarity between constructs 10 and 32, 10 and 25, 10 and 35, 25 and 35, 32 and 35, 35 (see Table 1). According to these results, the interviewees treat the constructs "the physical security is required to protect IT systems," "disposal of hardware and software verification is very important," "documentation is extremely required" and "the awareness on data protection is required" as the same. This indicates a misunderstanding or misinterpretation of the security policies. Such misunderstanding can lead to inappropriate behavior in response to security incidents. Stakeholders tend to behave based on their rationalities or values they hold; and the differences in their rationalities with regard to security policies can be translated into different security practices (Albrecthsen and Hovden, 2009; Vaast, 2007).

Principal Components Analysis (PCA)

Principle Components Analysis looks at the variability (i.e. variance) in the ratings of constructs. It identifies the extent to which the ratings of each construct are similar to one another. First, we measured the correlation among the elicited constructs through PCA, which was required to measure content and structure of an individual's perceptions. The analysis of the constructs' correlations indicated high correlations between some constructs. For instance, the construct "strict access restriction" is highly correlated with the construct "violation should be documented" (0.94). Similarly, the construct "compliance requirements for third party should be complex" is highly correlated with the construct "multiple roles assigned to a single person is not acceptable" (0.81), and with the construct "data classified based on sensitivity" (-0.84). However, the constructs "awareness on data protection requirements," "documentation is extremely required," "disposal of hardware and software verification is very important," and "physical Security required to protect IT systems" had no relation with any other construct and among them (correlation coefficient = 0). Figure 2 shows the PrinGrid plot that has resulted from the principal components analysis of the data.

PCA helps in breaking down the RepGrid into fundamental structures. Here, PCA generates 8 components. Bell (1990) mentioned that most of Repertory Grids could retain two or three factors. By looking at the variance of each component of PCA, we found that five components explained more than 80% of the variance. However, we decided to retain two components (which explain 51% of the variance) because of the big drop between the variance of the second (variance = 22.5%) and third components (variance = 13.9%). As we see in Figure 2, the constructs were distributed evenly around the plot.

The grid has been treated as if the elements were plotted in a 40-dimensional space (based on the constructs). The center of the axes was the means of the elements. With PCA, the dimensions were reduced to 8 dimensions (components). Then, rotation of the components took place to spread the elements in a 2-dimensional plot (see Figure 2). Kelly (1969) called this output as "geometry of psychological space." The PrintGrid plot gives a better understanding of the relationships among the elements, among the constructs, and between the elements and the constructs. We analyzed the PrintGrid plots (one for the same stakeholders and another for different stakeholders). The plots used two principal components to display the cognitive maps of the elements. The nine elements were shown on the map and highlighted in red. Each construct was plotted as straight line. The distance between each construct and the center of the plot represents the variance in the ratings among constructs, i.e. the overall weightage of a certain construct based on ratings each element gave for this construct. Most of the constructs have high variance, whereas only few of them have small variance. That reflects the high variation in stakeholders' perceptions in general.

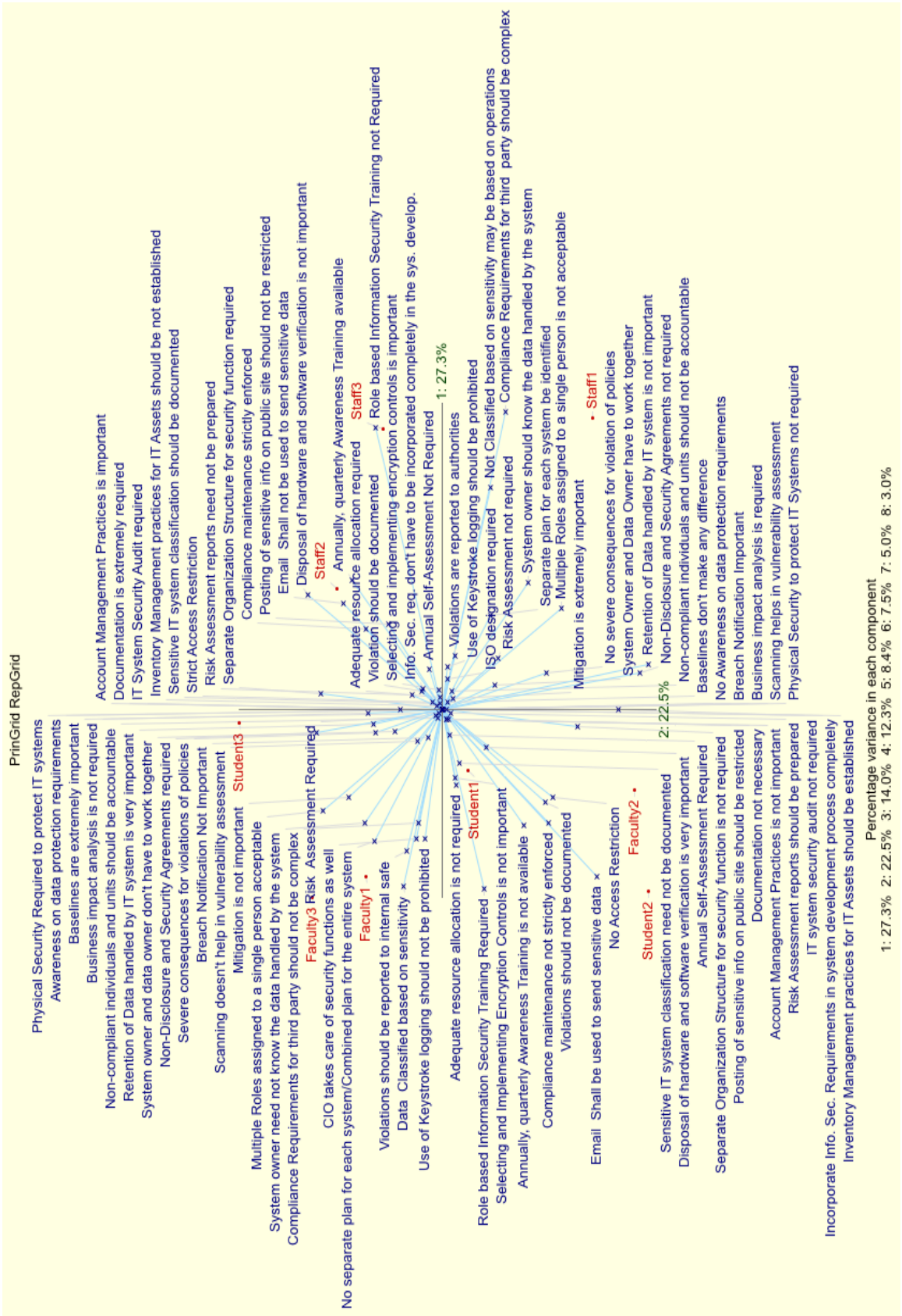

Figure 2: RepGrid PrinGrid plot

The angle between two constructs' lines represents the variance between two ratings (i.e. the correlation between the constructs). That is, the smaller the angle, the similar the ratings and the higher correlation between two constructs. As we see in Figure 2, and from the correlation results between the constructs, only few constructs were rated similarly due to the different perceptions that the stakeholders hold. As we found in the plot, some of the constructs were highly correlated (as we mentioned above), whereas the others had some correlation that range from medium to low correlation. Constructs "awareness on data protection requirements," "documentation is extremely required," "disposal of hardware and software verification is very important," and "physical security required to protect IT systems" had correlation coefficient equal to zero, i.e. the correlation does not exist. These constructs got the same ratings from the stakeholders, which means they share the same understanding for these policies.

On the other hand, the distance between two elements represents the ratings of each element on the constructs. Two elements would be plotted close to each other if both have similar ratings on each construct. In contrast, two elements would be plotted far apart if both have different ratings. Faculty1, faculty 3 and student 1 were plotted close to each other, which reflect some similarities among the constructs those participants held. Similarly, student 2 and faculty 2 were plotted close to each other. Staff2 and staff 3 were plotted close to each other. This result is consistent with the results of the percentage of similarities between the elements, which emphasize that there is a gap in the perceptions that the stakeholders held.

Discussion

Our analysis indicates that the values of stakeholders significantly influence compliance behavior. And there seems to be more to individual value based compliance and governance than the traditional attitudinal and behavioral research. Repertory grids have the explanatory power to highlight how perceptions among key stakeholders differ in a given context. An understanding of the user perceptions helps in the design of good governance practices for managing security.

Awareness and Compliance

One of the critical issues emerging from our analysis of RepGrids is the relationship between awareness and compliance. Clearly, there was mismatch amongst stakeholders in terms of four important aspects that have often been considered critical for good governance:

- Awareness of data protection requirement
- Need for physical security to protect IT systems
- Need for proper documentation
- Importance of disposal of hardware and software verification

Our RepGrid analysis found these four aspects to have the least correlation amongst stakeholders. A common thread that runs through the four issues is that of *awareness*. Over the years awareness of data protection has become a hygiene factor. Organization cannot afford to lack in the security awareness of their staff. Past research has also positively linked awareness to attitude and outcome beliefs for compliance (see Bulgurcu et al., 2010). One of the reasons for the lack of awareness can be attributed to the scope of awareness programs that currently exist. Hence, we looked into the range of awareness programs that existed at the university. Surprisingly enough, there were several programs – ranging from pamphlets to webinars and mini conferences. However, a closer look at these programs suggested that the message presented in the awareness programs was not very clear and often got diluted. Several approaches to security awareness have been put forward in the literature, which include 1) establishing a process for delivering the message 2) identifying responsible individuals 3) developing competence to determine sensitive and critical information 4) identifying business reasons for security 5) involving senior managers (see Peltier, 2005). In our case study organization, nothing of this sort was ever advocated.

Failure to have a well established awareness program is intricately linked to aspects of compliance. As Bulgurcu et al., (2010) note, awareness is linked to a belief that compliance should take place. Unfortunately this relationship is a little more complex than simply stating that increased awareness will lead to higher compliance. It is perhaps more appropriate to argue that increased awareness, along the dimensions identified by Peltier (2005) or Siponen (2001), among others, will lead to better compliance.

Governance Structures

Interestingly there was similarity and agreement amongst stakeholders on several issues. These included:

- Inherent complexity in vendor relationships
- Clarity of ownership, roles and responsibilities
- Data classification
- Non-disclosure and security agreements

If we are to compare these, with issues where there was limited agreement, it is clear that the stakeholders were aware of the importance of suitable governance procedures. Allocation of appropriate authority and responsibility, clarification of ownership issues and having necessary security agreements in place are important aspects that any corporate governance plan should have in place. Complexity and security have been well thought through the literature. As Ho et al. (2003) note, at the heart of any decision task is some sort of an optimization problem. And as systems become complex, so does management of security, aptly referred to as the *no free lunch theorem*. Ho et al (2003) note:

> "*As the complexity of a system increases without bound, the chance that the system will encounter an unplanned for situation also increases, and when an unplanned for situation occurs, the system's resulting performance in dealing with that situation is just as likely to be good as it is to be bad* (p. 788)."

Associated with inherent complexity is the notion of ownership and responsibility. The need for structures of responsibility was first highlighted by Backhouse and Dhillon (1996). Structures of responsibility help identify and establish various ownership and accountability aspects for security. Findings from our study suggest that while there was consensus amongst stakeholders that there is a need to bring clarity in ownership, this was not necessarily what was happening at the case study organization.

Managing Change

The mismatch in the perceptions of stakeholders reiterates the need for understanding security policies to reduce or eliminate divergence in stakeholders' perceptions. This can be achieved by educating the stakeholders through security awareness and training programs that 'sufficiently' inform stakeholders about potential security breaches and the effects of such breaches. Such programs help to ensure that various non-compliance behaviors or attitudes are addressed at the pre-deterrence stage (Willison and Warkentin, 2013).

However, awareness and training programs may not change the stakeholders understanding and interpretation of security policies. With the aid of Repertory Grid, organizations can take into account the mismatch in the perceptions of stakeholders regarding security policies, and thus design appropriate awareness and training programs that can positively change the values of stakeholders. In this way, more fine-grained change management actions that will reduce potential security policy compromises can be identified. Designing change management programs for security can be done through aligning security policies and standards with the business goals, so that business and security can work together effectively to achieve business goals with limited risk. Aligning security to business can also add value to the business itself. It optimizes security and risk management, and mitigates the overall business risk. Security should not be operating in response to security breaches only; rather, it should respond to all issues that influence organizations and the complexities associated with their daily business activities. Thus, security policies should be flexible to adapt to the changing nature of the business.

This study has theoretical and practical contributions. From a theoretical perspective, the study successfully uses Repertory Grid technique, which is grounded on Personal Construct theory, in the context of Information Systems to evaluate the conceptions of stakeholders regarding security policies. The Repertory Grid technique is rarely used in the Information Systems literature to study human values. The results of this study add to this body of knowledge and open up questions regarding human values and their relevance to different Information Systems issues.

From a practice perspective, this paper highlighted the importance of identifying the differences in the perceptions of stakeholders regarding security policies. Organizations can use the Repertory Grid technique to refine the alignment of norm and rule compliance. This involves 1) the identification of differences in the stakeholder perceptions of security policies, and 2) an assessment of how far these perceptions are from the actual meaning of the rules and policies.

Conclusion

In this study, we analyzed how different stakeholders within the same organization perceive the same security policies. The findings show that each stakeholder understands and interprets the security policies differently, based on their own perceptions. The mismatched understanding of security policies reflects on the practice of security governance, and this may, in turn, lead to non-compliance and devastating consequences for organizations. The alignment between norm and rule compliance implies a harmonization in the perception, attitude and behavior of staff towards security, and in this respect, it can help in the mitigation of security breaches. Finally, another benefit of the RepGrid analysis is that it provides us with valuable insights on how to initiate necessary changes that will foster the organizational commitment for security.

REFERENCES

Albrechtsen E. 2009. “A qualitative study of users' view on information security.” *Computers & Security* (26:4), pp. 276-289.

Albrechtsen, E., and Hovden, J. 2009. “The information security digital divides between information security managers and users.” *Computers & Security* (28:6), pp. 476-490.

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

Bell, R.C. 1990, "Analytical issues in the use of repertory grid technique." *Advances in Personal Construct Psychology* (2), pp. 25-48.

Boland, R.J., and Tenkasi, A.V., 1995. "Perspective making and perspective taking in communities of knowing." *Organization Science* (6:4), pp. 350–372.

Botterill, T. D. 1989. “Humanistic tourism? Personal constructions of a tourist: Sam visits Japan.” *Leisure Studies* (8:3), pp. 281-293.

Briggs, R., and Edwards, C. 2006. *The Business of Resilience*. Demos, London. Brooks, G.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. 2010. "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness." *MIS quarterly* (34:3).

Doherty, N. F., and Fulford, H. 2006. “Aligning the information security policy with the strategic information systems plan.” *Computers & Security* (25:1), pp. 55-63.

Dillon, A., and McKnight, C. 1990. “Towards a classification of text types: a repertory grid approach.” *International Journal of Man-Machine Studies* (33:6), pp. 623-636.

Ernst & Young, 2012. “Fighting to close the gap.” *Ernst & Young’s Global Information Security Survey*.

Guo, K. H. 2013. Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security* (32), pp. 242-251.

Harnesk, D., and Lindström, J. 2011. “Shaping security behaviour through discipline and agility: Implications for information security management.” *Information Management & Computer Security* (19:4), pp. 262-276.

Hassenzahl, M., and Trautmann, T. 2001. “Analysis of web sites with the repertory grid technique.” *In CHI'01 extended abstracts on Human factors in computing systems* pp. 167-168. ACM.

Ho, Y. C., Zhao, Q. C., and Pepyne, D. L. 2003. "The no free lunch theorems: Complexity and security." *Automatic Control, IEEE Transactions on*, (48:5), pp. 783-793.

Horley, J. 2012. "Personal Construct Theory and Human Values." *Journal of Human Values* (18:2), pp. 161-171.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. 2012. Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture, *Decision Sciences*, (43:4), pp. 615-660

Johnston, A. C., and Hale, R. 2009. "Improved security through information security governance." *Communications of the ACM* (52:1), pp. 126-129.

Kelly, G. A. 1955. *The psychology of personal constructs*. Volume 1: A theory of personality. WW Norton and Company.

Kreber, C., Castleden, H., Erfani, N., Lim, J., and Wright, T. 2003. "Exploring the usefulness of Kelly's personal construct theory in assessing student learning in science courses." *Teaching in Higher Education* (8:3), pp. 431-445.

Millis, K. K., and Neimeyer, R. A. 2007. "A Test of the Dichotomy Corollary: Propositions Versus Constructs as Basic Cognitive Units." *International Journal of Personal Construct Psychology* (3:2), pp 167-181.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., & Vance, A. 2009. What levels of moral reasoning and values explain adherence to information security rules; an empirical study. *European Journal of Information Systems*, (18:2), pp. 126-139.

Padayachee, K. 2012. Taxonomy of compliant information security behavior. *Computers & security*, (31:5), pp. 673-680.

Peltier, T. R. 2005. "Implementing an Information Security Awareness Program." *Information Systems Security*, (14:2), pp. 37-49.

Phythian, G. J., and King, M. 1992. "Developing an expert support system for tender enquiry evaluation: a case study." *European Journal of Operational Research* (56:1), pp. 15-29.

Siponen, M. 2001. "Five dimensions of information security awareness." *Computers and Society*, (31:2), pp. 24-29.

Straub, D.W. and Welke, R.J. 1998, "Coping with systems risk: security planning models for management decision making." *MIS Quarterly* (22:4), pp. 441-64.

Tan, F. B., and Hunter, M. G. 2002. "The repertory grid technique: A method for the study of cognition in information systems." *MIS Quarterly* pp. 39-57.

Vaast, E. 2007. "Danger is in the eye of the beholders: Social representations of Information Systems security in healthcare." *The Journal of Strategic Information Systems* (16:2), pp. 130-152.

Willison, R. and Warkentin, M. 2013. "Beyond Deterrence: An Expanded View of Employee Computer Abuse," *MIS Quarterly,* (37:1), pp. 1–20