Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2011 Proceedings - All Submissions

8-6-2011

The Role of Conflict Resolution in Designing and Implementing Information Security Policies: An Institutional Perspective

Sherly Abraham
University at Albany, abrahamsherly@gmail.com

Indushobha Chengalur-Smith
Department of Information Technology Management, School of Business, University at Albany, SUNY, shobha@albany.edu

Follow this and additional works at: http://aisel.aisnet.org/amcis2011_submissions

Recommended Citation

Abraham, Sherly and Chengalur-Smith, Indushobha, "The Role of Conflict Resolution in Designing and Implementing Information Security Policies: An Institutional Perspective" (2011). *AMCIS 2011 Proceedings - All Submissions*. 467.
http://aisel.aisnet.org/amcis2011_submissions/467

This material is brought to you by AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2011 Proceedings - All Submissions by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

The Role of Conflict Resolution in Designing and Implementing Information Security Policies: An Institutional Perspective

Sherly Abraham
College of Computing & Information
University at Albany
abrahamsherly@gmail.com

InduShobha Chengalur-Smith
School of Business
University at Albany
shobha@albany.edu

ABSTRACT

This paper examines the suitability of institutional theory in explaining the design and implementation of information security policies in organizations. We conduct a case study in a large governmental organization in the United States. We capture multiple perspectives among the different groups in the organization and examine how this affects the design and implementation of security policies. We find a high interdependence between the information security group and other groups in the organization resulting in task and process conflicts. These conflicts had both positive and negative outcomes. A combination of dominating and compromising conflict management styles are shown to produce positive results in resolving the conflicts. Our study highlights the importance for managers to balance security and usability and to ensure that the stringency of security policies do not override the business objectives of the organization.

Keywords: information security policy; institutional theory; conflicts; conflict management.

INTRODUCTION

Designing, implementing and enforcing security policies in organizations is a complex task, and requires making changes to existing technologies and procedures, and achieving a “buy-in” from all stakeholders in the organization. For example, a security policy might prevent certain users from installing programs or downloading files to their computers or require a project team to make changes to the software design to accommodate security requirements. Thus the organization has to be cognizant of existing work practices and processes as it rolls out new policies. Informational resources are distributed across several groups in organizations and implementing security policies could result in conflicts of values, goals, power and cultures between the various groups (Gagne et al., 2008). This can be partly attributed to the differing perceptions of the various stakeholders.

It is essential to understand how this multiplicity of views can impact the design and implementation of security policies. In order to successfully implement new security policies, management will have to negotiate between various constituents and overcome resistance to change. We know little about how the variations in perspectives and requirements among different stakeholders in an organization can create conflicts, and how this affects the design and implementation of security policies. In addition, various institutional factors inherent in an organization can influence the design and implementation of security policies. The present study aims to answer the following research questions:

How do institutional forces shape the design and implementation of information security policies?
How do interdependencies among organizational units and their differing perspectives on security create conflict?
Can such conflicts lead to positive results in terms of security policy design and implementation?

INSTITUTIONAL THEORY

A number of studies have examined the implementation of security policies in organizations (Baskerville, 1993; Dhillon and Backhouse, 2001; Walsham, 1993). Walsham (1993) emphasizes the social context in which information systems are designed, implemented and evaluated. Dhillon and Backhouse (2001) identify the dominance of technical and functionalist approaches in the information systems security literature, and call for studies to investigate other perspectives like interpretive, radical humanist, and radical structuralist paradigms. These studies highlight the need for a socio-organizational perspective in analyzing security policies and the challenges in implementing them in organizations. Drawing on this perspective, we propose that institutional theory is well suited to explain the design and implementation of security policies in organizations.

Institutional theory underpins the process by which social structures consisting of schemas, rules, norms and routines become guidelines for governing social behavior (Zucker, 1987). The theory is built on three major elements: coercive, mimetic and normative forces that shape the institutionalization of rules and norms within the social structure. Based on DiMaggio and Powell (1983) we define the three forces as follows:

Coercive – Associated with political pressures and the problem of legitimacy stemming from formal and informal pressures, e.g. government mandates and environmental regulations

Normative- Associated with professionalism as members of a profession define the conditions and methods of their work, e.g. industry standards and best practices

Mimetic- Associated with organizations attempting to model other organizations under uncertainty and goal ambiguity

While one view of institutional theory proposes that organizations achieve stability by the persistence of norms and beliefs, another view contends that institutionalization within organizations can cause resistance to change (Goodrick and Salancik, 1996). Institutional theory has also been applied in examining information systems. Given the habitual nature of human interaction with information systems (Gosain, 2004), the enactment of patterns of practice become institutionalized. Although such institutionalization could assist in creating stability, it could also lead to resistance to the changes that come with technological innovations and requirements.

Institutional theory is also useful in explaining the implementation of security initiatives. Bjork (2004) explains how the formal security structures in organizations can be influenced by institutional factors that stem from coercive, mimetic and normative forces, resulting in organizations with isomorphic security structures. Similarly, Hu et al., (2007) utilize neo-institutional theory to explain how factors internal and external to an organization shape information security initiatives. They show that while external institutional factors play a role in shaping the security efforts there are also strong internal factors that influence the process.

Information security is a highly regulated domain, and there are a number of governmental mandates such as Sarbanes Oxley and breach notification acts that require organizations to comply with laws pertaining to information security. Similarly, normative pressures exist in the form of National Institute of Standards and Technology (NIST) guidelines and ISO standards that provide guidelines for information security. Additionally, given the difficulty of predicting the direction of future technologies, organizations under uncertainty may also rely on mimetic forces in designing security policies. Thus we believe that institutional theory can assist in explaining the factors that govern the design of security policies stemming from the presence of coercive, normative and mimetic forces.

We propose the following:

Proposition 1: The design of security policies is influenced by environmental factors stemming from the presence of coercive, normative and mimetic forces

Design and implementation are two distinct phases of information security policy development (David, 2002). The design stage is when the information security group identifies the need for a new security policy or a change in existing policies. The need for the policy can result from governmental mandates, new security standards, security incidents and so on. During the implementation stage the security group will need to evaluate existing technologies and analyze the feasibility of implementing the policy in their organization. This stage may involve pilot testing and requires coordination among various stakeholders in the organization.

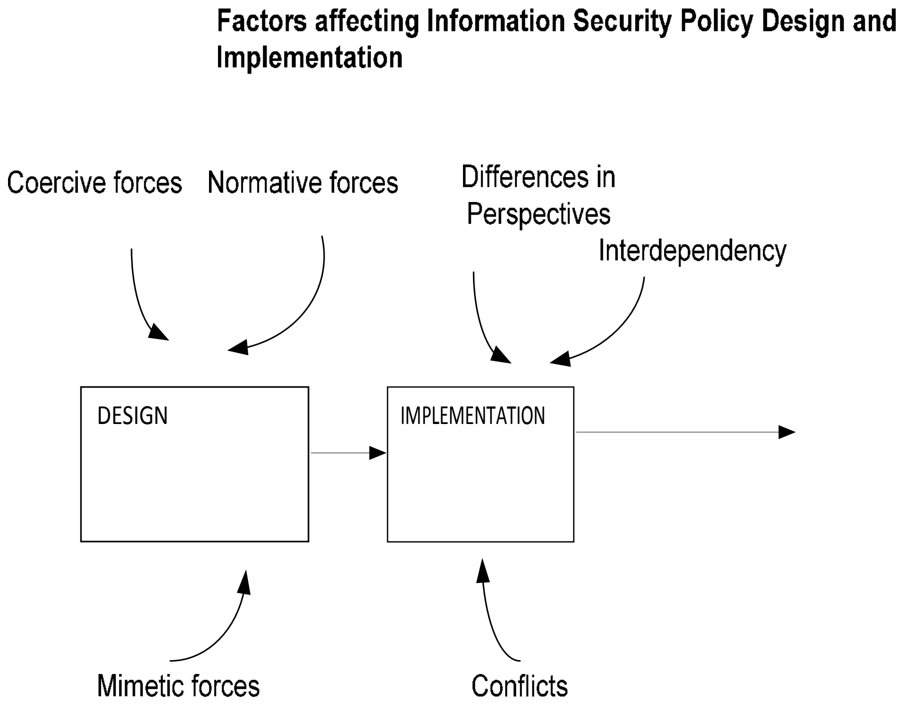

Factors affecting Information Security Policy Design and Implementation
Coercive forces
Normative forces
Differences in Perspectives
Interdependency
DESIGN
IMPLEMENTATION
Mimetic forces
Conflicts

Figure 1. Factors affecting security policy design and implementation

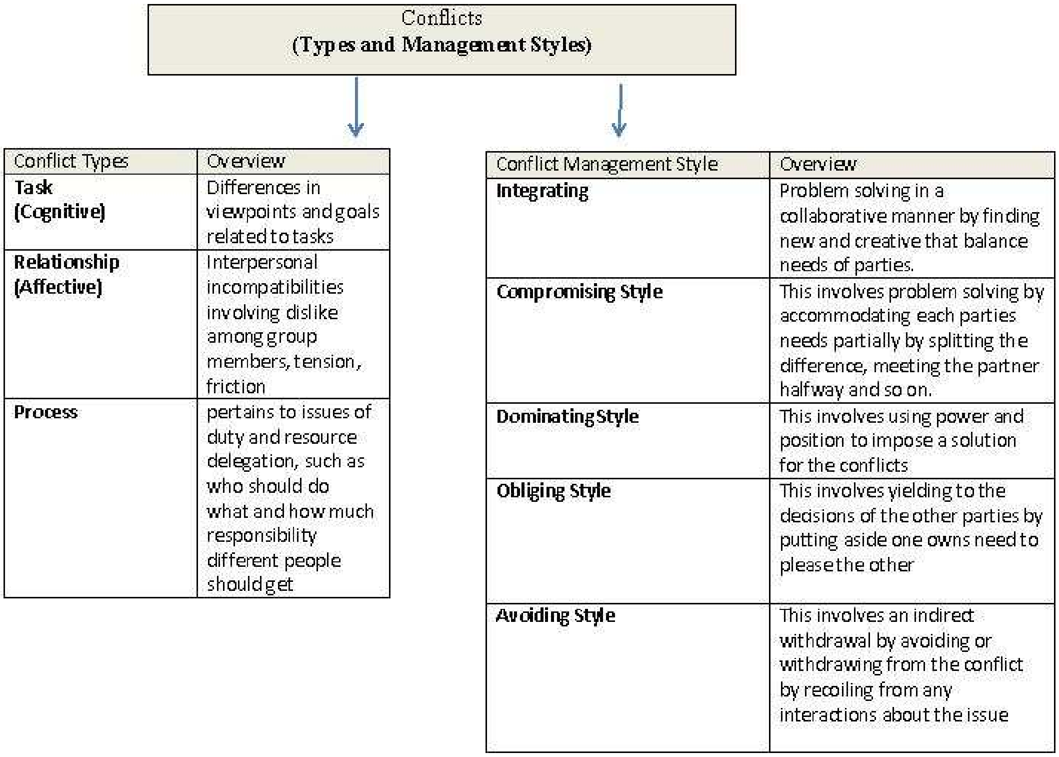
A notable consequence of institutionalization is resistance to change (Zucker, 1987). Security policies require implementing changes to institutionalized practices at the technological, organizational and human levels (Vrooms and Solms, 2004). Although the design stage might require the coordination of different actors in the organization, we expect a higher level of interdependence at the implementation stage of the policy. This interdependence combined with the inherent resistance to change in organizational units that have different perceptions of security risks can result in conflicts.

Although other studies (Hu et al., 2007) identify the presence of internal resistance forces, they do not analyze the variations in perspectives among different organizational groups and the accompanying conflicts. In order to capture the effects of multiple perspectives and the resulting conflicts, we turn to the conflict management literature.

Conflict Management

Conflicts occur among two or more parties and are defined as a "process in which one party perceives that its interests are being opposed or negatively affected by another party" (Wall and Callister, 1995). The organizational literature identifies three major properties of conflicts- interdependence, interference and disagreement (Barki and Hartwick, 2001; Meissonier and Houze, 2010; Putnan and Poole, 1987). Interdependencies exist when a group or individual relies on the actions of another group or individual. Interference occurs when the goals, interests, and objectives of the groups or individuals are misaligned. Finally, disagreement occurs when there are differences in interpretations in values and objectives.

Jehn and Mannix (2001) categorize conflicts in work groups into three levels: relationship, task and process conflict. In general, relationships conflicts have been shown to have negative impacts while task oriented and process conflicts can create learning opportunities and improve quality outcomes of teams (Liang, Jiang et al.,2010). Conflict is an integral part of information systems development (Smith and McKeen, 1992) and it is necessary to examine how conflicts are managed and their impact on the development of IS projects. Conflict management literature has identified five different types of conflict management styles and Table 1 summarizes the conflict types and conflict management styles based on Jehn and Mannix (2001) and Gross and Guerrero (2000).



Conflicts
(Types and Management Styles)

Conflict Types	Overview
Task **(Cognitive)**	Differences in viewpoints and goals related to tasks
Relationship **(Affective)**	Interpersonal incompatibilities involving dislike among group members, tension, friction
Process	pertains to issues of duty and resource delegation, such as who should do what and how much responsibility different people should get

Conflict Management Style	Overview
Integrating	Problem solving in a collaborative manner by finding new and creative that balance needs of parties.
Compromising Style	This involves problem solving by accommodating each parties needs partially by splitting the difference, meeting the partner halfway and so on.
Dominating Style	This involves using power and position to impose a solution for the conflicts
Obliging Style	This involves yielding to the decisions of the other parties by putting aside one owns need to please the other
Avoiding Style	This involves an indirect withdrawal by avoiding or withdrawing from the conflict by recoiling from any interactions about the issue

Table 1. Conflicts and Conflict Management Styles

Information security is inclusive of all the processes in the organizations, and requires the coordination of various stakeholders in the organization in order to translate the policies into action (Werlinger et al., 2009b). Most studies analyze responses from security administrators (e.g. Kraemer and Carayon, 2007) or managers (e.g. Kankanhalli et al., 2003) but do not capture multiple perspectives within different groups in the organization. The difference in goals and priorities among the various groups in the organizations adds to the complexity in implementing policies. Goodhue and Straub (1991) suggest that if security is not part of an individual's job they could have little appreciation for either the potential dangers or actions that could prevent security incidents.

The need for security could get in the way of meeting the business objectives of the organization. Stringent security requirements could turn off users and have been noted to be a hindrance in completing tasks (Post and Kagan, 2007), hence it is necessary to find the right balance between security and usability (Lorrie and Garfinkel, 2005). Conflict can have positive project outcomes (Baron, 1991) and the task and process conflicts that arise during the implementation of security policies could assist in balancing security and usability and ensuring that security policies are in line with the business objectives of the organization.

Although relationship conflicts can be prevalent in the implementation of security policies, in this study we focus on task oriented and process conflicts. Most studies consider conflict management styles individually, but there is evidence that a combination of conflict management styles is more common (Falbe and Yukl, 1992). In essence, conflicts can be handled more effectively using a combination of conflict management styles rather than using a single mode of conflict handling (Van de Vliert et al., 1995).

Although the dominating conflict management style has been shown to be effective (Gross and Guerrero, 2000), others have criticized it for not considering the opinions of other parties, and tending to force a decision (Montoya-Weiss et al., 2001). Users prefer collaborative conflict management styles over dominating management styles (Ives and Olson, 1984; Robey and Taggart, 1981), but the nature of information security requires management to sometimes undertake assertive decisions to shut down systems or suspend authorization rights of users. However studies have shown that dominating conflict management styles could lead to negative outcomes (Barki and Hartwick, 2001). A combination of compromising and dominating conflict management styles could alleviate these negative outcomes.

The above reasoning leads to the following set of propositions in the context of information security conflicts:

Proposition 2: The high interdependence between the information security group and the other groups in the organization may result in conflicts that could have positive and negative outcomes

Proposition 3: Task and process conflicts may assist in the process of balancing security and usability

Proposition 4: A combination of dominating and compromising conflict management styles may produce positive results in information security policy implementations

RESEARCH METHOD

Given the paucity of prior research on the application of institutional theory to the design and implementation of security policies, we adopted an exploratory approach for our analysis. Specifically, we relied on the case study method and collected data using interviews, focus groups and document analysis. We chose a large government organization that we refer to as Company ABC, as the context for our study. ABC has approximately 4000 employees and the company has a hierarchical organization structure. Information technology is a key component of ABC's outreach services to the public. ABC has a large number of web-based forms that are available to the general public and can be filed online to obtain the services of ABC. Figure 2 is an organizational chart of ABC.

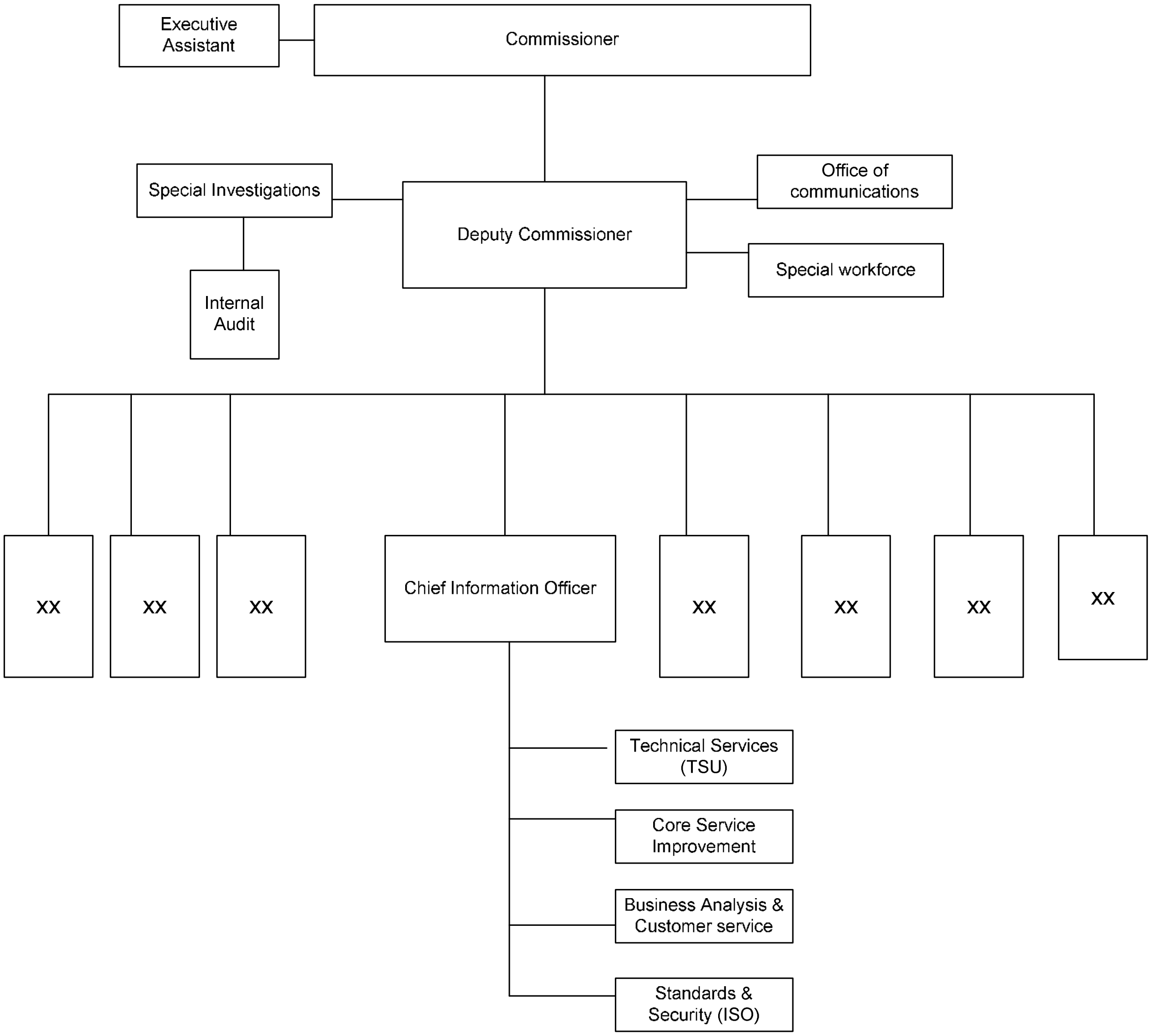


Figure 2. Organization Chart

Approximately 13 percent of the workforce in ABC are information technology staff. The Chief Information Officer oversees four major units, two of which are the Technical Services unit (TSU) and the Standards & Security office (ISO). TSU is responsible for the core IT services ranging from applications development to network services, whereas the ISO is responsible for designing, implementing and enforcing information security policies. We conducted interviews and focus groups with the chief information officer, and employees from the ISO and TSU. In addition we had access to the organization's policies, current technology projects and strategic planning documents. The information technology portfolio at ABC includes an assortment of legacy, commercial and open source applications.

ANALYSIS

The technology infrastructure at ABC is controlled by a centralized technology agency that we refer to as OFC, and it governs all the technology operations in the state. Hence the security policies of ABC were designed to fit the requirements of OFC. Although, OFC provides guidelines, the individual agencies are responsible for setting their local security policies and implementing the policies within their respective agencies. The analysis of our interview data revealed that the security policies at ABC are also shaped by governmental mandates such as the

Federal Information Security Management Act (FISMA). FISMA focuses on the protection of the nation's critical infrastructure, and the role of ABC as a government entity requires them to be FISMA compliant. Other examples of coercive forces that shape ABC's security policies are the state specific security and breach notification act, the public officer's law, and the USA Patriot Act.

The ISO staff are also members of a forum for state information security officers, where best practices and guidelines are shared. In addition, NIST guidelines are used to understand the professional standards and requirements for security. This is evidence that normative forces influence the design of information security policies.

Finally, if the ISO is not able to obtain specific guidelines from OFC or the security officers' forum, they research security policies in other corporations or peer agencies. ABC is required to comply with Information Classification requirements as specified by Federal Information Processing Standards (FIPS) publication 199 that states: *"ISO staff will also reach out to staff in other agencies to learn of their classification efforts."* This is evidence of the presence of mimetic forces that mold the security policies at ABC. Overall, our analysis attests to the influence of environmental factors, specifically, coercive, normative and mimetic forces on the design of security policies, supporting Proposition 1.

The data gathered though our focus group and interviews suggested that the design and implementation of the security policy varied depending on the coverage and technological requirements of the policy. For instance, some of the security policies that required changes to work practices were first tested out in pilot groups prior to being implemented to obtain feedback on the accessibility and applicability of the policies. This feedback is used to further alter the policies and once the ISO is satisfied with the policy, it goes to the CIO and then to the communications officer for comments. The ISO team often works through several iterations before the policy is formalized. Once it has been approved, the policy goes into the general administration manual of the organization. The entire process of putting a security policy in place can take 2-6 months minimally.

A major challenge the ISO group identified is the delays that occur due to the different levels of approval required in the process before the policy is formalized. Delays could be due to the fact that the existing technologies might not support the implementation and enforcement of the policy. For instance, a current project to mask the social security numbers of users in the ABC database system so that only the last 4 digits are displayed is constrained by technological issues. Specifically, the ability to generate a unique key in the absence of the SSN would require major changes to the existing technological infrastructure. This is one example of the conflicts that arise between different groups due to their differing perspectives. The CIO is the ultimate arbiter between the demands of the various stakeholders.

The ISO is highly dependent on other units such as the CIO, communications office, TSU and other core service units in the organization in order to implement security policies. Hence they face a number of challenges in convincing other groups of the importance of the policy and obtaining their buy-in. For instance, the ISO group had proposed implementing an IDS/IPS (intrusion detection and prevention) system in one of their private networks but could not convince the TSU to implement it. The TSU director considered the risk to be very low. Referring to the IDS/IPS project, the director mentioned that the risk of a breach was very low. He commented: "*This is a private network for internal people, the worst that could happen was that devices on that network would get infected; but there are only a small number of devices, and they could be easily cleaned. Resources to implement an IDS/IPS could sideline other projects, so we resisted working on it"*. This is an example of a task conflict between the ISO and the TSU. Eventually the ISO had the CIO advocate for the project in order to get the TSU to implement the IDS/IPS, illustrating a dominating style of conflict resolution by the CIO.

We noted differences in the perspectives about the importance of security. For the ISO, the top priority is preventing a security breach from happening and hence they want to ensure their organization is as secure as possible. Although security is important, it is equally important to ensure that services are available to customers and employees. The TSU director stated: "*There is always a certain amount of risk in making services available on the web but in today's world people want to access the services of ABC from home. If we need 100% security we can have the user come to our office and show their passport but this is not feasible*". According to the CIO: "*No access is the best security but that does not align with the business goal of the organization of serving the public. A security breach can happen anytime, and if it does happen what is the process we have in place? An incident response* *approach is the top priority."* The CIO insisted that it was important to have a process along with the policy. An example that he provided was that although password protection is required, ABC also needs a procedure in place to help legitimate users if they forget their password, even if it is outside of regular working hours. "*We need to provide the support or have the technology in place to meet this need*." This is an instance where task and process conflicts eventually led to a balance of security and usability through a compromising style of conflict management.

The CIO mentioned that often the ISO recommendations need to be reevaluated to balance usability and the business objectives of the organization. For example, ABC was required to be PCI (Payment Card Industry) compliant in accepting credit card payments from customers. However due to delays by the external vendor, ABC was not able to attain PCI compliance. The ISO recommended that all credit card payments were to be stopped until they were PCI compliant, however the CIO evaluated the situation from a business perspective. "*The customers would be unhappy if we all of a sudden stop accepting credit card payments*". In order to balance both objectives, the CIO requested the audit body for an extension in the PCI compliance requirement, and notified the external vendor that ABC would consider breaking the contract and use a different vendor if they were not PCI compliant within a specified deadline. This is evidence of a compromising style of conflict management.

A major challenge for the ISO group was their exclusion from many IT project kick-off meetings. Although a team member from the ISO group was supposed to be involved in every IT project meeting, they were often not notified about the project or else brought in at later stages of development. For instance, although the ISO group had notified an application development team of the minimum encryption standards this was not implemented in the project. When the ISO questioned the development team about the minimum encryption requirement they were blamed for delaying the project and bringing issues to the table "very late in the game". Through the intervention of the CIO, the ISO and the development team were able to reach a compromise solution. Due to this conflict the ISO is now invited to participate in project development at an early stage. ABC has also developed an Intranet web portal that the ISO group can access to view the current IT projects and assign an ISO member to a development team as required. These are examples of positive outcomes of conflict.

DISCUSSION

We undertook a case study of a large government organization in order to examine the factors that impact the design and implementation of security policies. We found that the design of security policies at ABC was highly governed by the presence of coercive, normative and mimetic forces, confirming the presence of institutional elements. These findings are consistent with other information systems implementations (Gosain, 2004) and security initiatives (Bjork, 2004; Hu et al, 2007).

We also examined the conflicts that occur among the information security group and other units in the organizations and how these conflicts are resolved. We found differences in the perceptions of risk evaluation and security goals among groups. For the CIO reacting to a security incident was the top priority, for the ISO team the priority was to prevent a security incident from happening, and the priority for the TSU director was maximum availability to services. Some of the security projects that the ISO rated as high priority was considered a low risk by the TSU director. This is in line with the findings of Goodhue and Straub (1991).

As observed in other studies (e.g. Werlinger et al., 2009a), we noted that the ISO team was highly dependent on other units in the organization in order to implement their projects. For the formalization of security policies, they were dependent on the CIO and the communications office. If a policy required changes to application programming or networking infrastructure they were highly dependent on the TSU. This dependency and difference in security risk perception was a major cause of the conflicts identified among the groups in the organization. We confirmed the presence of task and process conflicts in implementing security policies.

The CIO played a key role in negotiating conflicts and finding a balance between security and usability. We observed that a compromising conflict management style was adopted by the CIO and this had positive outcomes. We also observed dominating conflict management approaches. An example was in completely shutting down an application that the ISO had discovered to have vulnerabilities. This meant that the application was not accessible to customers and disrupted the service provided by the TSU. Such a dominating conflict management style was necessary in order to take immediate action in an emergency situation.

We note that the inherent nature of information security calls for a mixed approach to resolving conflicts that includes both compromising and dominating. We observed that the ISO and the TSU were content with the approach undertaken by the CIO and seemed to welcome his intervention. Hence the combination of compromising and dominating conflict management style had positive outcomes. Similarly we note that conflicts present in implementing security policies had both positive and negative outcomes. Some of the negative results of the conflicts were the delays in completing the projects due to the various layers of approval. However this also had benefits in terms of helping to refine the security policies and making it comprehensible by all users in the organizations. The communications group reviewing the security policy assisted ABC in achieving this layer of review. Similarly, the task and process conflicts assisted in creating an optimum balance of security and usability. Our analysis of this case study leads us to conclude that conflict and the appropriate management of conflict can help an organization walk the fine line between security and usability.

CONCLUSION

Our study analyzed the design and implementation of security policies and the inherent conflicts that arise in the process. Our results confirm that institutional theory is well suited to explain the design of information security policies. We bring to light the interdependencies of the information security group with other units in the organizations, and the differences in perspectives of risks and goals among the different groups. Our findings confirm the presence of task and process related conflicts in implementing security policies. We also show how conflicts can have both positive and negative outcomes in implementing security policies. While conflicts are shown to delay the implementation of information security policies, it assists in balancing security and usability, and aligning the security policies with the business objectives of the organization. A combination of compromising and dominating conflict management styles is shown to produce positive outcomes.

REFERENCES

Barki, H and Hartwick,J.(2001) Interpersonal Conflict and its management in information system development. *MIS Quarterly* 25(2), 195-228.

Baron, R. (1991). Positive Effects of Conflict: A Cognitive Perspective. *Employee Responsiblities and Rights Journal*. 4(1), pp 25-36.

Baskerville, R. (1993) Information Systems Security Design Methods: Implications for Information Systems Development. *Computing Surveys*, 25 (4), pp. 375-414.

Björk, F. (2004) Institutional theory: A new perspective for research into IS/IT security in organizations. *Proceedings of the 37th Hawaii International Conference on System Sciences*, pp 1-5.

David, J. (2002) “Policy enforcement in the workplace”, *Computers & Security*, Vol. 21 No. pp. 506-13.

Dhillon, G., and Backhouse, J. (2001) Current directions in IS security research: towards socio-organizational perspectives, *Information Systems Journal*, 11 pp. 127-153.

DiMaggio, P.J. andPowell, W.W. (1983) The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48, pp. 147-160.

Falbe, C. M. andYukl, G. (1992) Consequences for managers of using single influence tactics and combinations of tactics. *Academy of Management Journal*, 35, pp. 638-652.

Gagne, A., Muldner, K. and Beznosov, K. (2008) Identifying differences between security and other IT professionals: a qualitative analysis. In: *HAISA’08: Human Aspects of Information Security and Assurance*. Plymouth, England, July 8-9 2008, pp. 69-80.

Goodhue, D. L., and Straub, W. D. (1991) Security Concerns of System Users: A Study of Perceptions of the Adequacy of Security. *Information & Management* (20:1), 1991, pp. 13 – 27.

Goodrick, E. and Salancik, G. R. 1996. Organizational discretion in responding to institutional practices: Hospitals and Cesarean births. *Administrative Science Quarterly*, 41: 1-28

Gosain, S (2004) Enterprise information systems as objects and carriers of institutional forces: the new iron cage? *Journal of the Association for Information Systems* 5(4).

Gross, M. A., and Guerrero, L. K.., (2000) Managing Conflict Appropriately & Effectively: An Application of the Competence Model to Rahim's Organizational Conflict Styles. *International Journal of Conflict Management*, Volume 11, Issue 3.

Hu, Q., Hart, P. and Cooke, D. (2007) The role of external and internal influences on information systems security – a neo-institutional perspective. *The Journal of Strategic Information Systems*, 16 (2) pp. 153-172.

Ives, B. and Olson M. H. (1984) User Involvement and MIS Success: a review of research. *Management Science* 30(5), pp. 586-603.

Jehn, K A. and Mannix, E. A. (2001) The dynamic nature of conflict: a longtitudinal study of intragroup conflict and group performance. *Academy of Management Journal* 44(2), pp. 256-282.

Kankanhalli, A., Teo, H.-H., Tan, B.C.Y., and Wei, K.-K. (2003) An integrative study of information systems security effectiveness, *International Journal of Information Management*, 23, 2, 139-139.

Kraemer, S., and Carayon, P. (2007) Human errors and violations in computer and information security:the viewpoint of network administrators and security specialists. *Applied Ergonomics,* 38, pp. 143-154.

Liang, T., Jiang, J., Klein, G.S, Liu, J.Y., and Nat,S. (2010). Software Quality as Influenced by Informational Diversity, Task Conflict, and Learning in Project Teams. *IEEE Transactions on Engineering Management*, 57 (3), pp. 477-487.

Lorrie C., and Garfinkel, S. (2005) *Security and Usability*. O'Reilly and Associates.

Meissonier, R.and Houze, E. (2010) Toward an 'IT Conflict-Resistance Theory: action research during IT pre-implementation.

Montoya-Weiss, M., Massey, A.P.and Song, M. (2001) Getting it together: Temporal coordination and conflict management in global virtual teams. *Academy of Management Journal, 44*(6) , pp 1251-1262

Post, G., and Kagan, A., (2007) Evaluating information security tradeoffs: Restricting access can interfere with user tasks *Computers & Security*, 26(3), pp. 229-237.

Putnam, L. L.and Poole, M. S. (1987). Conflict and negotiation. In F. M. Jablin (Ed.), Handbook of organizational communication. Newbury Park, CA: Sage.

Robey, D. andTaggart, W. (1981). Measuring manager's minds: the assessment of the style in human information processing. *Academy of Management Review* 6 (3), pp. 375-383.

Smith, H.A. and McKeen, J.D. (1992) Computerization and Management: A Study of Conflict and Change. *Information & Management*, Vol. 22, No. 4, pp. 53-64.

Van de Vliert, E., Euwema, M. C. and Huismans, S. E. (1995). Managing conflict with a subordinate or a superior: Effectiveness of conglomerated behavior. *Journal of Applied Psychology,* 80, 271-281

Vroom, C. and von Solms, R. (2004) Towards information security behavioural compliance. *Computers & Security*, 23:3, pp. 191-198.

Wall, J. and Callister, R. (1995). Conflict and its management. *Journal of Management*, 21(3), pp. 515-558.

Walsham, G. (1993) *Interpreting Information Systems in Organizations*, Wiley, Chichester, UK.

Werlinger, R., Hawkey, K., and Beznosov, K. (2009a). An Integrated View of Human, Organizational, and Technological Challenges of IT Security Management. *Journal of Information Management & Computer Security*. 17(1), pp.4-19.

Werlinger, R., Hawkey, K., Botta, D.and Beznosov, K., (2009b). Security Practitioners in context: Their activities and interactions with other stakeholders within organizations. *International Journal of Human-Computer Studies*, 67, pp. 584-606.

Zucker, L. (1987). Institutional Theories of Organization. *Annual Review of Sociology*, 13, pp. 443-464.