Association for Information Systems
AIS Electronic Library (AISeL)

ICIS 2007 Proceedings

International Conference on Information Systems (ICIS)

December 2007

Making Sense of Institutionalizing Information Systems Security Management in Organizations

Carol Hsu
City University of Hong Kong

MAKING SENSE OF INSTITUTIONALIZING INFORMATION SYSTEMS SECURITY MANAGEMENT IN ORGANIZATIONS

Carol W. Hsu
Department of Information Systems
City University of Hong Kong
ischsu@cityu.edu.hk

Abstract

Information Systems (IS) security management has gained renewed importance for the past few years resulting from the rising numbers of security incidences and compliance pressure. While majority of IS security research has been focusing on the technical value and the effectiveness of IS security implementation, studies on the organizational process of implementation is rather limited. This paper employs a socio-cognitive perspective to examine the sense-making process of IS security BS 7799 Part 2 certification among different stakeholder groups in the organization. Using a qualitative case study approach, the findings reveal different understandings on the strategy and consequence of IS security implementation. We argue that socio-cognitive perspective, in particular the concept of frames analysis, can act an analytical tool to interpret meanings and anticipate actions in managing IS security in organizations.

Keywords: IS security, technological frames, socio-cognitive perspective, institutionalization, qualitative research

Introduction

Today modern organizations are initiating information systems (IS) security management projects to tackle rising security incidents and to meet the requirements of regulatory compliance such as Sarbanes-Oxley Act of 2002 or the Data Protection Act (Department and PricewaterhouseCoopers, 2006, Gordon et al., 2006). In the IS security literature, we find a number of studies investigating issues regarding IS security management in organizations. Some focus on the impact of preventive and deterrent effort on security effectiveness (Straub, 1990, Kankanhalli et al., 2003), some concentrate on the design of IS security policy (Whitman et al., 2001, Siponen and Iivari, 2006), and others centre on the issue of management and employee awareness programs (Siponen, 2000, Straub and Welke, 1998). As an attempt to classify research paradigms in the IS security field, Dhillon and Backhouse (2001) applied the Burrell and Morgan framework and reveal the dominance of technical and functionalist approach among the existing security literature. Comparing to the mainstream IS scholarly work, they conclude that " a socio-organizational perspective is the way forward if security of information systems is to be achieved" (Dhillon and Backhouse, 2001, p.147). Put simply, security literature in the functionalist paradigm does not consider the social nature of the organizational problem of securing a system. The Barings Bank case exemplifies the disastrous consequence of ignoring socio-organizational issues when implementing IS security management (Willison, 2006). In line with this argument, the research reported in this paper adds to the body of knowledge concerning the socio-organizational perspective for understanding IS security management in the organization. In particular, the paper examines the organizational implementation process for achieving IS security management BS 7799 Part 2 certification.

BS 7799 stems from the publication of *A Code of Practice for Information Security Management* in 1993 and then of BS 7799 Part 1 in 1995 in the United Kingdom. The emphasis of this standard is on the development of an IS security management framework and policy, rather than of technical requirements. Although the great success of BS

7799 Part 1 quickly led to its transformation to an international standard ISO/IEC 17799 in 2000, BS 7799 Part 2 remains the associated certificate scheme which was only recently developed as ISO/IEC 27001 in December 2005. In the literature, Backhouse et al.(2006) have described the institutionalization process of BS 7799 at the industry and international level. We attempt to examine the people and organizational issues during the period of introducing, implementing and achieving BS 7799 Part 2 certification as a means to institutionalize IS security management practice in a financial institution.

The results of this research have implications for theoretical development and practice in IS security management. From a research standpoint, a focus on socio-cognitive approach adds value to the socio-organizational approaches found in some IS security management literature. The findings of this investigation also offer a theoretical explanation of how and why different organizational members behave differently towards IS security policies and procedures. From a managerial perspective, our empirical findings suggest that managers need to pay great attention to the behavioral aspect of IS security management as opposed to just enforcing stringent policies.

The paper is organized as follows. In the next section, we discuss the significance of social and organizational perspective in understanding IS security management. We follow this discussion with the introduction of socio-cognitive approach, in particular the concept of frames. We continue with the description of the research methodology deployed in this study and the narrative of the case, the Finance House. Discussion of the findings discloses two important themes concerning the process of institutionalizing IS security management practice in the Finance House. The concluding remarks are a reflection on the contributions and implications of our research.

Theoretical Framework

Many IS studies have demonstrated that implementations of the same technologies can result in different social consequences because of distinct and complex organizational structures and cultures in which information technologies are developed and adopted (Sahay et al., 1994, Orlikowski and Baroudi, 1991, Ciborra and Suetens, 1996, Avgerou, 2001, Ciborra and Lanzara, 1990). Others have shown that the social and political forces are salient in the institutionalization of an IS (Silva and Backhouse, 2003, Silva, 2007). Altogether these findings challenge any assumptions that information technology is an objective and independent artefact with known properties and lawful order, and that the way to understand technology is through a reductionist or functionalist approach. Rather, these findings suggest that information technology is part of a social system and actively interacting with other components such as politics, economics, social and legal norms and working practices. As a result, meanings of information technology are not directly derived from its technical features, but indirectly through the interpretations of human actors involved. That is, information technology is socially constructed and shaped (Bijker and Pinch, 1987). The approach of this paper broadly aligns with this sociological paradigm.

Social Construction and the Study of IS security

IS security researchers are increasingly paying attention to the relevance of context in studying IS security phenomenon although such theoretical approaches are "still at a theory-building stage" (Dhillon and Backhouse, 2001, p.148). Some have discussed the external forces on managing IS security while others have focused on the institutionalization process in the organization. For example, Hu et al. (2006) have examined the impact of institutional isomorphism on the adoption of IS security management practice. Siponen and Iivari (2006) argue that the stringent rule-based and context-free security policy is not applicable in today's turbulent and fast-changing business environment. They elaborate that to maintain competitive advantage, while coping with unforeseen business circumstances, employees of modern organizations might not have the patience to follow the formal compliance process for approval to information access. Their suggestion is that instead of enforcing IS security policies literally, the design of IS security policies requires the input of "application principles to solve such exceptional situations" (Siponen and Iivari, 2006, p. 448). In other similar studies, Willcocks and Margetts (1994) address the significance of contextualizm when undertaking the risk assessment in the organization. Backhouse and Dhillon (1996) propose the analytical tool of responsibility structure to examine the norms and patterns of behaviors of different actors in the organization.

Building on the premise of socio-cognitive research, other researchers have turned their attention to the importance of people's interpretation and understanding of IS security. Vroom and von Solms (2004) argue for the inclusion of

employee's awareness and security culture when evaluating the extent of IS security effectiveness in an organization. Dhillon and Torkzadeh (2006) propose the development of security objectives via a value-focused thinking approach. Their conceptual framework highlights that the process of structuring value allows a better understanding of what people really consider as the most relevant and important for maintaining IS security in the organization. In a similar sprit, this research focuses on the revealing the interpretations that shape the institutionalization process of IS security management via the implementation of BS 7799 Part 2 certification. Firms seeking certification against BS 7799 Part 2 are required to submit to an audit exercise by an accredited certification body. Certification bodies are third parties who examine the compliance with the standard. The certificate will normally be valid for 3 to 5 years and is available for renewal to ensure the continuous maintenance of a good management system. The costs of obtaining and maintaining a certificate can be significant. An organization seeking certification must commit itself to investing manpower and financial resources during the implementation and audit process. The audit process can take between 9 and 28 months (Anderson et al., 1999).

Concept of Frames

Minsky (1975) introduced the term 'frame' to represent "a data-structure representing a stereotyped situation" (p.212) and to be used in artificial intelligence applications. In addition to artificial intelligence, similar concepts or notions have also developed and applied in other fields such as cognitive psychology and linguistic study. There are many terms used to describe the formation and existence of such understanding: "schema", "cognitive maps", "mental models", "frames", "paradigms", "scripts" and "thought worlds"(Orlikowski and Gash, 1994). For this particular research, we choose the word frames. The socio-cognitive approach shares the same belief with social constructivism that knowledge cannot effectively construct meaning in isolation, and reality is a personal interpretation dependent on how individuals perceive their experiences. With these views of epistemology and ontology, socio-cognitive theorists maintain that action is subject to interpretation of the individual on the basis of his worldview and the surrounding environment, as Bandura (1986) argues "what people think, believe, and feel affect how they behave" (p.25).

Within the scope of organizational studies, a frame has several characteristics. First, a frame is a mechanism for an individual's sense-making. It allows people using it to reconcile their current knowledge with new information presented by the environment and to give meaning to their understanding of the world. An individual's frame is always situated in particular time and space context. Despite deploying the same frame as a reference, the context in which individuals are located might constrain and elaborate their interpretations of an object or event and therefore lead to different understandings and actions as a consequence. A frame is also a mechanism for an organizational sense-making. An organizational frame permits members of the organization to assign shared meanings to activities and events taking place. As a result, these interpretations direct members to behave accordingly (Lin and Conford, 2000). Although frames are held independently by individuals, there is the existence of shared frames. Socio-cognitive approach suggests that in the course of socialization, a certain group of people generate or share the same beliefs and assumptions towards some phenomena. Bijker and Pich (1987) refer to this as relevant social group within the context of organization. They argue that only when all or most relevant social groups are located, one can start defining the problems and hence tracing the common frames shared among members of relevant social groups. Different relevant social groups might define problems or share frames differently, and each group assign different meanings to the surrounding artefact, subsequently different actions. In other words, when misalignment of interpretation among different relevant social groups arises, there exists an incongruence of frames in the organization (Orlikowski and Gash, 1994).

Building upon the concept of frames, Orliskowski and her colleague (Orlikowski, 1993, Orlikowski and Gash, 1994) extended the applicability of frames analysis in organizational science and further develop it into the idea of technological frames, since they find that technology issues are not specifically addressed *per se* in socio-cognitive studies. They use the term 'technological frames' to address the mental models of how members of an organization assume, expect and interpret the technology they use in that particular organization. Technological frames not only include the nature and functionality of technology itself, but also embrace "the specific conditions, applications, and consequences of technology in particular context"(Orlikowski and Gash, 1994). Empirical studies have shown how technological frames analysis can be applied to reveal how different actors make sense of information technology and how they interact with the technology accordingly in the organization (Orlikowski, 1993, Orlikowski and Gash, 1994, Lin and Conford, 2000). Other studies have also referred to or implicitly adopted the idea of technological

frames in studying social and behavioral aspect of information systems (Sahay et al., 1994, Sahay, 1997, Barrett, 1999, McLoughlin et al., 2000).

In this research, the notion of frames is used to capture the assumptions and interpretations of various relevant social groups within the context of institutionalizing IS security management practice in a financial firm. The study includes a focus on how different groups of stakeholders in the organization made sense of the certification and consequently behave during the implementation process. Before discussing the findings, we describe the research method used and the narrative of the case.

Research Study

Research Site and Method

The research was conducted in a major financial institution in Taiwan, the Finance House (a pseudonym), which provides securities settlement and depository services to individual and institutional investors both domestic and foreign. The organization has over 400 employees spread among 11 departments. The firm has computer linkages with more 1000 institutional participants including securities firms, custodian banks and stock exchanges across the country. The business operations of the Finance House are tightly regulated by the national financial supervisory authority. In early 2004, the organization decided to undertake BS 7799 Part 2 certification as a means to develop enterprise-wise IS security management. The enterprise-wise certification was obtained in October 2005. This development is the period of this empirical research.

The researcher was a manager at the international business affair division of the Finance House between July 2004 and December 2005. Data collection took place during this period and additional 5 formal follow-up interviews with top management, users and IT personnel were undertaken after the researcher left her position in the company. Data sources came from the observation notes, informal conversation with employees, internal security policies, meeting minutes of the certification working group, and organizational press releases. Observation notes mainly came from the researcher's attendance at 15 monthly management-level meetings chaired by the company chairman in which the certification progress was reported and discussed. Informal conversation data was gathered through the means of social networking and after-meeting discussion with other members of the firm. Because of the nature of the researcher's job, there was an abundant supply of opportunities to interact with other staff across the company's hierarchical levels and various departments. Social lunches and informal chats were valuable to capture people's personal views of the certification project. In addition, a total of 34 formal documents were used in this investigation ranged from monthly progress reports by the certification team, internal IS security training materials, internal IS security policies and procedures, meeting minutes, and organizational publications. The use of multiple sources of information helps to demonstrate the credibility and dependability of a qualitative case study research (Yin, 1994). The focus on the data collection centered on the identification of different relevant social groups within the context of this study and what different social groups understood as the strategy and value of BS 7799 Part 2 certification.

This research study uses a qualitative approach (Yin, 1994, Creswell, 1998). Walsham (1995) suggests that there are two types of research roles that can be exercised in the conduct of interpretive case studies: the outside observer and the involved researcher. The outside observer might have advantages of having participants express their opinions freely since participants see the researcher as an outsider, and hence consider no danger in revealing what they really think of various organizational issues. The problem with such a role is that the researcher might encounter difficulty of gaining initial entry, trust, and further access to some organizational documents or meetings because these might be classified as for 'the insider' only. Adopting the role of participant grants the researcher opportunities for being counted as a member of a group or organization and hence of getting an insider's view from other members of the organization. Given of the nature of the subject under investigation, access to information might have been difficult, especially so when the focus is on personal interpretations of security issues. In this situation, the personal contact with organizational actors proved invaluable. The familiarity with the researcher made the interviewees feel comfortable about discussing possibly sensitive or confidential issues.

However, we must also acknowledge that being an insider means that participants are more likely to perceive the existence of political interests between themselves and the researcher in the organization, and consequently will be more reserved with what they want the researcher to know. In this case study, the researcher developed the research

interests on this subject after becoming acquainted with some internal auditors and having informal conversations about the implementation process. The researcher did not participate in the certification decision-making process. Neither did the researcher work in the relevant departments such IT or audit department that was in charge of implementation. Therefore, this helped to reduce any potential political conflicts between the researcher and interviewees that might have endangered the data collection quality as well as to minimize the researcher's own bias that might jeopardize the validity of research findings.

The approach adopted for analyzing the data consisted of drawing on the concept of frames to structure the narrative of the case, thereby performing a dialogical process between data and theory (Klein and Myers, 1999). In this research, "hermeneutic circle" or "hermeneutic process" was deployed to aid the researcher to understand the correct interpretation (Lee, 1991, Rathswohl, 1991). Only if we can obtain and interpret fully the meanings that organizational actors ascribe to BS 7799 Part 2 certification and to guide their behaviours will we bee able to build a rich and complex picture of IS security management implementation. Our hermeneutic process started with our early understanding of certification implementation process as a whole, then through interviews with participants and observation of organizational activities, we were able to refine our understanding of the whole through the parts. Put differently, following the approach suggested by Orliskowski and Gash (1994), the initial understanding of the implementation process led us to identification of three distinct social relevant groups in this particular case. In each group, the interview data and field notes were then studied and organised into different themes. Through the recurring exercise of reading the field notes and interview materials, we refined the development of themes and ensured that the developed themes were dominant across different interest groups in the case. As we encountered conflicting or incomplete interpretations of a certain event or statement we went back to the participants and ask either informally or formally for clarification. This process continued and only stopped when we were fairly confident with our understanding of the IS security management implementation process under scrutiny.

The Case: the Finance House

In 2001, to respond to a request from the national financial supervisory authority, the Finance House commenced strong internal IT security compliance check and developed an IT security policy. In late 2003, resulting from a national security assessment exercise, the government made a decision to include three of the Finance House's main computer systems as the part of national critical infrastructure. Other similar systems included in the national critical infrastructure were the trading systems operated by the securities and futures exchange. The reason for the inclusion was that the failure to provide timely securities trading, clearing and settlement could lead to a major interruption to the capital market and hence cause undesirable panic in society. As a consequence of this government decision, in early 2004, the financial supervisory authority mandated that Finance House as well as the securities and futures exchanges were required to achieve good standard of IS security management. Explicitly, the authority named the BS 7799 Part 2 certification as the matching standard, and required these companies to complete the certification process within a reasonable time period.

Between late 2003 and October 2004, the company had rewritten its security policy and procedures to meet the certification requirements. It also held over 144 sessions of an internal security training program at the department level or organizational level. By October 2004, 22 of the company employees, mostly from internal audit and IT departments, were awarded posts as BS 7799 Leading Auditors. In July 2004, Finance House passed the first stage of certification audit, i.e. document review. Shortly after, the organization succeeded in a compliance audit for the second stage and obtained the certificates for three main operational systems in October 2004. To celebrate this achievement, the chairman of the company held a BS 7799 Part 2 certificate presentation ceremony with guests from the supervisory authority and securities exchanges. In 2005, the management group decided to expand the scope of certification to the rest of operational systems that were not classified as national critical infrastructure. As a result, the BS 7799 Part 2 certification were awarded to all other systems in October 2005.

Research Findings

During data analysis, we identified three relevant social groups related to the BS 7799 Part 2 certification process: Management Group; Certification Team; and Other Employees. The Management Group consists of members of

senior management and the chairman who initiated and approved the certification project. The Certification Team includes technologists in the IT department and auditors in the internal audit department. Other Employees here refer to the rest of staff from different hierarchical levels in the organization. We made a decision of not naming this particular group as a "user group", as is usually done in other similar studies in technological frames analysis. The reason was that there was no single technological artifact in use here.

Three domains of frames emerged from the analysis of interviews, observation notes and documentation. We see three distinct interest groups having different interpretations of why certification was introduced (certification strategy), how it was implemented throughout the organization (image of implementation process), and how it has impacted on the daily work practice after implementation (outcome of certification). In the following sessions, we present the analysis of the different assumptions and interpretations of each domain held by the three groups.

Table 1: Definition of Different Frames Domains

Frames Domain	**Definition**
Certification Strategy	- Understanding of external and internal organizational strategy in relation to BS 7799 Part 2 certification
Image of Implementation Process	- Understanding of implementation requirements and impact on day-to-day work during implementation process
Outcome of Certification	- Understanding of the consequence of having achieving BS 7799 Part 2 certification

Certification Strategy

The Management Group initiated the BS 7799 Part 2 certification project as a result the mandatory requirement from the national financial supervisory authority. Although the regulatory authority did not set an explicit deadline for completing this requirement, a management-level internal meeting was quickly held in the Finance House to discuss the certification issue. In the meeting, the senior management felt that to start with, the scope of certification should be limited to the three main operational systems. By focusing on these three systems, which already had good IT security controls in place, senior management believed that the company could get the certification without undertaking too many necessary adjustments in the existing security management. Timeline is important because speedy completion allowed the company to "quickly demonstrate to the authority about the performance of the firm," as indicated by one senior executive.

Besides meeting regulatory requirements, given the nature of the financial business, the chairman assumed that having the BS 77799 certificate would have a positive impact on the public confidence. He expressed this belief in a meeting,

> *"The certification can demonstrate to the public that we have secure back-office securities processing system. So, investors will have confidence when trusting us with securities settlement and computerized book-entry services we provided."*

With the instruction from the Management Group, the IT department and internal audit department came together and formed a task force for the project, referred to as the Certification Team. When asked about the reason for forming this team, while some members in the team had mentioned compliance, most provided a response of "taking orders" or "do as instructed by the boss".

A similar line of response was given by other employees in the organization. During numerous information conversations, the researcher asked other employees whether they were aware of this project and why the company decided to seek for BS 7799 Part 2 certification. Many expressed having no knowledge of this project. Observations

also indicated that people from other departments showed very little interest in knowing more about the security certification project or in continuing conversations on this topic during the informal discussions.

Image of Implementation Process

During the time of implementing the certification, the Management Group assumed that the process would be fairly straight forward since the organization had strong a IT security architecture. At the outset of the implementation process, the Management Group had learnt that the leading organization in their sector had successfully obtained the certification with highly complementary comments from the external auditor. Despite having confidence on their existing technical controls, the Management Group were concerned that unfamiliarity with specific certification requirements might slowdown the process and hinder external audit outcome, and to lose out to the leading organization in the same sector. This concern led to a decision to hire external consultants to assist on the project. The external consultant remarked on the Management Group's belief in scoring high marks in the audit exercise,

> *"I was told that the company wanted to be the best. And I knew after the first few meetings with the senior management that the goal is not only having certificates but also getting above 90 or even higher in the audit assessment."*

The project initiation came directly from the top of organizational structure and the Certification Team assumed that their main priority was having the certification accomplished within a very short time span as expected by the Management Group. One internal auditor recollected that,

> *"it was highly stressful. They [the Management Group] wanted to have the certificate as soon as possible and with the best results among other rival organizations. Therefore, we have pressure of becoming BS 7799 Lead Auditor. It was not required for BS 7799 certification, but was necessary for the management to show how good we [the company] were to the outsiders!"*

With a strong technological security already implemented, the Certification Team concentrated on the preparation of documents for the first stage of BS 7799 audit. Under BS 7799, the organization was required to have policies and procedures covering 10 control sections, 36 control objectives and 127 controls. Staff from the IT department were not very familiar with the process of formal policy writing, hence this task was done mostly by the internal audit department with the assistance of the external security consultants. At the same time, members of the Certification Team were all taking courses for the qualification of BS 7799 Lead Auditor. During the year 2004, 22 members were awarded qualifications BS 7799 Lead Auditors. This number was the highest among other compatible organizations. Members from the Certification Team also expressed the increase in knowledge about risk management and security management that resulted from the interaction with the external consultants and the training for becoming BS 7799 Lead Auditors.

Due to the time pressure for obtaining certification, the Certification Team consequently believe that they did not have sufficient resources or time allocated for appropriate employee education and awareness campaigns, and that such activity was important for establishing an organizational security culture. One employee commented on the compliance-centric attitude of the Certification Team,

> *"I was asked to fill in information on the risk assessment form circulated [by the Certification Team].I found the criteria were not suitable for the evaluation of our business activities in my department. I wanted to discuss this with them. But they told me to try to squeeze information in. I think that they do not really care about learning how risk might happen in my department!"*

The assumption of treating the process as an exercise of document production was also seen in other employees' interpretation. A number of staff in informal conversations thought of this process as the extension of ISO 9000 certification that the company just accomplished few years earlier. For example, one employee explained,

> *"BS 7799, something to do with ISO 9000, right? Does that mean even more papers and checks we need to do for the internal audit?"*

The lack of emphasis on employee empowerment and development of security culture was reflected in the organization of a 144 session security-related training program. This training program was delivered by the human resource department instead of the IT or internal audit department. We observed that most sessions were given by the external consultant and the materials were too generic to attract employees' interests in the subject matter. Employees viewed the attendance at this training program as not significantly different from other training program offered by the human resource department. They consider attending the session as just one way to fulfill the yearly required hours of training course attendance.

Outcome of Certification

With respect to the interpretation on the outcome of the certification, we observed that the Management Group held the views that the certification was a major milestone and a success in increasing the profile of the company. For publicity, in October 2004 the company had organized a proper BS 7799 certificate presentation ceremony with the attendance of large numbers of organizational employees and guests from the supervisory authority, stock exchanges and a representative from British Standard Institute. In the ceremony, the chairman made a remark that,

> *"The company had the second biggest national database on individual data information. The certification is a major milestone in demonstrating the company's commitment to information security management."*

The philosophy of informing the public on achieving BS 7799 Part 2 certification was reinforced through the publications of newsletter, monthly company journals and flyers to the individual/institutional investors.

Furthermore, one senior executive believed that having completed the process, the organization had enhanced its internal compliance procedure. In one of interviews published in an IS security magazine, this executive reiterated his belief in the value of certification and the expected positive outcome,

> *"In a strong IS security management and strict compliance environment, there is no allowance for 'more or less about right' attitude towards security. I believe that my organization has top-class security management supported by frequent internal audit and departmental self-assessment check-list exercises."*

Their view on a strict compliance environment was consistent with the continuous developments in the organization: 1) the requirements of at least two employees receiving relevant information systems auditor certification each year; 2) the installation of full-scale intrusion and detection systems (IDS) as well as intrusion and prevention systems (IPS); 3) the installation of an Internet monitoring system.

The Certification Team, in particular members from the internal audit department, shared this understanding with the Management Group that the outcome of certification meant the establishment of more formal compliance procedures within the company. When asked how they would assess the success of IS security management resulting from certification, both IT staff and internal auditors cited the reduction in technical and operational errors in the compliance report, rather than commenting on the change of other employees' knowledge or behaviors.

Some members in the Certification Team had slightly different interpretation on the consequence of the certification. They believed that maintaining the good result in the ongoing external audit and minimizing the operational errors would rely on their capability in performing more frequent internal audits, rather than trusting employee's self-awareness and ability in ensuring good security management practices. One internal auditor amused us with the story of the use of instant messenger, which was not allowed in accordance with the organizational IS security policy,

> *"After the first round of the internal audit, users know that MSN was not allowed. I asked them to remove it. However, they move to web MSN which can be detected by our Internet monitoring software. They again were notified, and then they behave. But their good*

> *behaviors only happened for a short period of time either before or after my audit to the department. This pattern keeps going as a cycle."*

Other Employees had different views regarding the outcome of the certification. During a number of informal conversations, some staff expressed that the increase in compliance resulting from the certification project brought more inconvenience than benefits. The perception of inconvenience and strict compliance had prompted some employees to get around the formal security procedures. For example, according to the new IS security policy written up during the certification process, employees are not permitted to use portable devices such as USB memory sticks or portable hard disks unless receiving a written approval from the management. We observed that employees tend to violate this rule because of the sudden outside-company meeting or traveling reasons. One employee made similar remarks on the inflexibility and inconvenience,

> *"My job required extensive traveling abroad. However, they [IT department] said for strict security reason, they can not implement or enable a web-based e-mail solution. At the end, every time I travel, I ask my colleague to access my e-mail and forward to my yahoo account and I use yahoo to reply to my client. But this is so troublesome and unprofessional."*

Table 2: Summary of Frames Analysis for ISMS Implementation

	Management Group	Certification Team	Other Employees
Certification Strategy	Compliance; Speed; Good for public reputation.	Top management decision; Compliance	Do not know; Top management decision
Image of Implementation Process	Straight forward; Achieving high score of certification result; Good qualifications for internal auditors.	Meet management's expectation; Focus on word-to-word compliance; Knowledge improvement.	Same as ISO 9000 certification; Paper work; Responsibility of IT and internal audit department
Outcome of Certification	Success; High recognition; Strict security management	Reduction in technical and operational errors; Heavy work-load on compliance check.	Inconvenience; A lot of rules.

Discussion

The above section has presented findings of the frames held by three relevant social groups in the organization during the time of BS 7799 Part 2 certification. These different interpretations offer valuable insights to explain the issues and unanticipated organizational consequences in the institutionalization process of information systems security management in Finance House. We organize our discussion under two themes: institutional isomorphism on certification adoption and strategies for legitimating IS security management practice.

Institutional Isomorphism on Certification Adoption

In this study, the Management Group see that compliance with government requirements and potentially for good publicity are the primary driver for seeking BS 7799 Part 2 certification. This view reflects the institutional approach to the adoption of organizational practices. Similar to the theoretical assumption of socio-cognitive theories, institutionalists believe that the individuals or organizations shape, at the same time are shaped by, the social rules

and normative regulations, which consequently impact on individuals' behavior or organizations' decision-making process. In IS field, many researchers have examined the role of institutional isomorphism in influencing organizations' decision for the adoption or assimilation of technological innovations (Chatterjee et al., 2002, Iacono et al., 1995, Teo et al., 2003). In this study, the assumptions about certification held by the Management Group demonstrate the influence of institutional isomorphism on the Finance House's decision-making process. For example, from the institutional economics perspective, Akerlof (1970) suggests that the institutional arrangement of third-party certification can help to resolve the information asymmetry in the market, normally known as "lemons problem". Here one motivation held by the Management Group was to establish a signaling method to inform the general public with respect to the sound security management practices in the Finance House. The assumption of signaling strategy was reflected in the public statements by the Management Group. Through the leverage of BS 7799 Part 2 certification, they believe that they company can as a result reinforce the consumer confidences in the current financial services provided, and perhaps in future services that could be developed.

Institutional researchers in the organizational field also argue that practices travel from one organization to another because of the operationalization of different mechanisms of isomorphism in a social system (Scott, 1995). Institutional researchers indicate that there exist three different mechanisms of institutional forces: *coercive, normative and mimetic* (DiMaggio and Powell, 1983, Scott, 2001, Meyer and Rowan, 1991). In this study, we see these forces shape the context in which the Finance House was located, hence constraining the Management Group's interpretation of IS security management. Orlikowski and Gash (1994) argue that " this sense-making process, they (people) develop particular assumptions, expectations and knowledge of the technology, which then serve to shape sequent actions toward it" (p.175). The research findings here indicate that coercive forces and mimetic forces constitute the social reality of the environment in which the Finance House operates. The institutional isomorphism acts as a powerful force that affects on how decision-makers in the Finance House make sense of BS 7799 Part 2 certification.

Starting with assumptions on the certification strategy, the Management Group viewed certification as a means to meet the regulatory requirements and demonstrate to the authority the performance of the firm. These interpretations lead to the subsequent actions of initiating the BS 7799 Part 2 certification. Furthermore, the regulatory authority also plays a significant influence in the Management Group's expectations on the scope of information systems up for BS 7799 Part 2 certification. In other words, the coercive force shapes the management's understanding of the value of BS 7799 Part 2 certification, which led to the decision of limiting it to three main operational systems.

Besides coercive pressure, our data also shows that structural equivalence in the institutional environment led to competitive mimicry between the Finance House and other companies in the interorganizational network. Mimetic isomorphism represents the imitation of one organization perceived by others as successful or legitimate in an organizational field. Institutional mimicry is more likely to occur for competitive reasons or as a strategy to address uncertainty and ambiguity (DiMaggio and Powell, 1983, Guler et al., 2002, Tingling and Parent, 2002). In the context of the financial sector, Ang and Cummings (1997) point out that in the hypercompetitive financial environment, "peer banks exert considerable influence on each other because of tight professional networks formalized by memberships in regional and national bank association" (p.237). In this study, our findings find the evidence of similar strong rivalry and competitive pressure in the financial sector but also tight links. Peer influence on the adoption of BS 7799 Part 2 certification was seen in the expression of concerns over the external audit score by the Management Group. The concerns on whether the company can achieve the best score among the rival organizations indicate that the company did not want to be disadvantaged in the marketplace. This competitive mimicry also led to the Management Group's interpretation of the time pressure towards certification as the company did not want to become late adopter and loss out competitive edge in this process.

The frames of the Certification Team and Other Employees on certification strategy reveal an interesting finding that at the early stage of the organizational decision-making process, the impact of institutional pressure on changing people's perceptions seems to be limited to the power-holders in the organization. Both relevant social groups showed shared interpretations of the reasons of undertaking certification. Their explanation and actions indicate the internal structural influences rather than the external institutional forces.

Strategies for Legitimating IS Security Management Practice

While the frames of certification strategy shed some lights on the institutional pressure for certification, the other two frames help us to reveal how different groups of stakeholders view the implementation process and take action during the time of seeking certification. Through tracing the assumptions, this helps us to have a fuller understanding of the extent that IS security management practices were institutionalized or became legitimate. In this empirical study, although certification was interpreted as a successful project, the incongruence of the management group's expectations and those of other employees indicate perhaps a variance in the degree of acceptance of legitimacy of the new IS security management practice.

We draw here on the concept of legitimacy management to explain this. Suchman (1995) argues that institutionalization of an organizational practice can be achieved via three forms of legitimacy: pragmatic legitimacy, moral legitimacy, and cognitive legitimacy. These resemble the three pillars, including regulative, normative and cultural-cognitive, of institutions put forward by Scott (2001). Each type of legitimacy is associated with different episodic disposition and involves different maneuver strategies. In brief, pragmatic legitimacy refers to conveying a new practice's value or worth through causal power, or an influence strategy such as regulation or mass-media communication. Moral legitimacy links a practice to the notion of whether the activity is "the right thing to do", and the power holders often need to match their actions with the normative structure embedded in the organization. Cognitive legitimacy is the "deepest level" (Scott, 2001, p.61) since it means that an activity or product has become "some take-for-granted cultural account' (Suchman, 1995). Suchman also argues that the persistence of legitimacy simultaneously stabilises and strengthens as the focus moves from pragmatism to morality to cognition. The institutionalization of an organizational practice will require a certain degree of cognitive legitimacy where people no long consciously considering alternatives or resist the practice.

In formulating its legitimacy strategy, Finance House's management group placed a strong emphasis on pragmatic legitimacy management by exercising causal power. Causal power refers to the exercise of power when actor A makes actor B do something the latter would otherwise not do (Silva and Backhouse, 2003). When asked about the image of the implementation process, the certification team interpreted this project as following the instruction of the management group, and other employees viewed their involvement as complying with the management expectation. In other words, staff from internal audit and IT departments would not have sought to become qualified BS 7799 Lead Auditor or written up the formal security policy if this had been not requested by the management group.

As the implementation of certification proceeded, within the certification team, we see the meanings ascribed to certification change from merely obeying the management decision to supporting the contribution of the certification process in minimizing security risks. This was consistent with the findings of Orlikowski (1993) that the extent to which people will change their technological frames depending on the availability and types of training programs they receive. Having undertaken courses on BS 7799 Lead Auditors, members of the Certification Team had acquired more skills in designing compliance checks for IS security. The interpretations of the outcome of certification indicate that certification had acquired certain degree of moral legitimacy among members in the certification team- become the right thing to do.

We also discover some extent of moral legitimacy among Other Employees. However, their interpretations of the "right thing to do" appear to draw from their past experience with ISO 9000. Bandura (1986) suggests that a frame permits people to "select and process sensory information, rather than simply react to whatever impinges on their sense organs" (p.198). This implies that if people face situations which are similar to ones that have occurred in the past, they are most likely to react in accordance with experiences and knowledge obtained from the past and to anticipate similar outcomes. Here, our findings indicate that some employees perceived the BS 7799 certification as the extension of ISO 9000 certification. As a result, they treat this certification as an exercise of document production similar to what they have done during ISO 9000 certification.

Overall, the research findings indicate that the perception and acceptance of certification among most employees remained at the level of compliance with structural order in the organization, rather than embracing and embedding the security practices into their daily routines. The latter was important for producing "cognitive inertia" (Orlikowski and Gash, 1994, p.33), and hence for the establishment of cognitive legitimacy. In the case of the Finance House, employees' behavior in the use of instant messenger and portable hard disks illustrate that users may take actions that were consistent with their particular frames, i.e. certification caused disruption to work routines and inconvenience. One explanation is that the Management Group assumed that because certification was about writing

up formal procedures, the certification team should focus on the development of compliance procedure, instead of educating and enhancing employees' security awareness. Following the line of reasoning on changing frames, the lack of awareness training program led to no modification in employees' understandings on the significance of certification. Therefore, their actions showed no interest in the certification process or even violated the compliance requirements after the implementation. Put bluntly, IS security management was not fully embedded in the organizational practice and routines.

The frames analysis shows that the persistence of legitimacy of security certification appears to remain of the form of pragmatic legitimacy and some moral legitimacy. In accordance with Suchman's legitimacy management, we argue that because the weak persistence of such legitimacy, Finance House might have a major challenge ahead in the light of unpredictable security threats and employees might not have the sufficient knowledge or enough level of awareness to identify potential risks and manage the risks.

Implication of Frames Analysis

In this paper we have applied the concept of frames analysis to investigate the process of institutionalizing an IS security management practice in an organization, and argue that this approach can offer an analytical tool to unfold the perceptions and consequent behaviors of different relevant social groups as new IS security management practices arrive in the organization. In this section, we present a synopsis of the main research and practical contributions of our study.

Research Contributions

The research contribution here is twofold: to the institutional research literature and to IS security management literature. First, our study reconfirms Orlikowski and Gash's argument (Orlikowski and Gash, 1994) on the contribution of frames analysis to other forms of social construction approaches such as power and legitimation. They suggest that "social cognitions connect to institutional analyses, which are concerned with shared, taken-for-granted systems of social rules and conventions" (Orlikowski and Gash, 1994). The concept of frames allows researchers to have a deeper understanding on how and why people behave towards the introduction of a new organizational practice. For example, the institutional environment shapes the assumption of the management group on the certification strategy and implementation process. By applying the frames analysis, we provide a lens through which to understand the interpretive schemas for human action during the legitimation process. Meanings that other employees ascribe to the certification implementation offer some explanations as to the forms of legitimacy achieved within the organization. These explanations would be lacking if the analysis had solely focused on the structural properties of the organization and causal power.

Second, this research makes a contribution to the literature in the field of IS security management. As mentioned before, socio-organizational approaches to the study of IS security phenomena are still at the early stage of theory development. In this study, a focus on the socio-cognitive nature of security management practices allows us to investigate in detail how people make sense of and hence enact the interpretations of their experiences and of the world around them. The research findings reveal that having strict compliance procedures does not guarantee perfect security. For example, the management group failed to take into account information sharing and communication flexibility, which was perceived by other employees as important in their work practice. As a result, employees did not change their assumptions and interpretations of the relevance of security management and continued to use instant messengers or portable devices seen as convenient to them. Furthermore, most security research from socio-organizational perspective have focused on the design or measurement stage of security management (Dhillon and Torkzadeh, 2006, Backhouse and Dhillon, 1996, Siponen and Iivari, 2006, Baskerville, 1993). Differing from these, this research provides an explanation of the process of, and anticipate the outcome of, institutionalizing IS security management.

Practical Contributions

Similar to implications of technological frames analysis, this research here demonstrates how different groups of stakeholders in the same organization have diverse understandings on the nature and implementation process of a newly introduced IS security management practice. As shown in the analysis, variance in assumptions and meanings

has a great impact on the legitimacy of a new management practice. Early identifications of these inconsistencies and efforts to reconstruct meanings of employees on this subject may help reshape their understandings of IS security, consequently, can strengthen the persistence of its legitimacy in the organization. In the case study, the BS 7799 Lead Auditor education exemplifies the impact of relevant training program on changing frames of the certification team.

The frames analysis first requires the identification of different relevant social groups in the organization (Bijker and Pinch, 1987). One relevant social group in an organization tends to define problems in a different manner from another social relevant group, and hence each group assigns different meanings to the surrounding artefact or technology, subsequently different actions. Having an appropriate understanding can add great value to the design and institutionalization process of security policy. In other words, instead of embracing fully the formal model, incorporating soft approach of meanings and interpretations help to increase employees' security awareness and hence their ability to make a sound judgement and risk assessment when "exceptional situations" arise (Siponen and Iivari, 2006). As a result, the overall security management effectiveness will increase as employees learn to accept and incorporate the concept of security principles into their work practices, i.e. the establishment of cognitive legitimacy.

Conclusion

In this paper, we employed the analytical framework of frames which refers to people's assumptions, interpretations, expectations and knowledge about the nature and role of a technological artefact or organizational practice. This study reveals that with the references of frames in a specific context, different relevant social groups in the organization assign different meanings to IS security management practice and use these meanings to make decisions on how to enact it. These findings reject the dominant functionalist and objective approach to IS security management practice, and the way to understand such a practice is through a reductionist or quantitative approach. Rather, the research results in this study illustrate that IS security practice is part of a social system and actively interacting with other components such as politics, economics, social and legal norms and working practices. Through the lens of frames analysis, it helps organizations have early diagnosis of any inconsistencies of understandings, hence, design appropriate strategic approaches accordingly in achieving an effective security management in practice.

References

Akerlof, G. "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism." *Quarterly Journal of Economics*, 89(3) 1970,pp 488-500

Anderson, S., Daly, D., and Johnson, M. "Why Firms Seek ISO 9000 Certification: Regulatory Compliance or Competitive Advantage?," *Production and Operation Management* (8:1) 1999, pp 28-42.

Ang, S., and Cummings, L. "Strategic Response to Institutional Influences on Information Systems Outsourcing," *Organization Science* (8:3) 1997, pp 235-256.

Avgerou, C. "The Significance of Context in Information Systems and Organizational Change," *Information Systems Journal,* (11:1) 2001, pp 43-63.

Backhouse, J., and Dhillon, G. "Structures of Responsibility and Security of Information Security," *European Journal of Information Systems* (5:1) 1996, pp 2-9.

Backhouse, J., Hsu, C., and Silva, L. "Circuits of Power in Creating De Jure Standards: Shaping an International Information Systems Security Standard," *MIS Quarterly* (30:Special issue) 2006, pp 413-438.

Bandura, A. *Social Foundations of Thought and Action: A Socio-cognitive Theory*, Prentice-Hall, Englewood Cliffs, NJ, 1986

Barrett, M. "Challenges of EDI adoption for electronic training in the London Insurance Market," *European Journal of Information Systems* (8:1) 1999, pp 1-15.

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

Bijker, W.E., and Pinch, T.J. "The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociological of Technology Might Benefit Each Other," in: *The Social Construction of Technology Systems,* W.E. Bijker and T.J. Pinch (eds.), MIT Press, Cambridge, MA, 1987, pp. 17-50.

Chatterjee, D., Grewal, R., and Sambamurthy, V. "Shaping Up For E-Commerce: Institutional Enables of The Organizational Assimilation Web Technologies," *MIS Quarterly* (26:2) 2002, pp 65-89.

Ciborra, C., and Lanzara, G.F. "Designing Dynamic Artifacts: Computer Systems as Formative Contexts," in: *Symbols and Artifacts: View of the Corporate Landscape,* P. Gagliardi (ed.), De Gruyter, Berlin, 1990, pp. 147-165.

Ciborra, C., and Suetens, N. "Groupware for an Emerging Virtual Organisations," in: *Groupware and Teamwork,* C. Ciborra (ed.), John Wiley & Son Ltds, London, 1996.

Creswell, J.W. *Qualitative inquiry and research design: Choosing among five traditions* SAGE Publications, Thousand Oaks, 1998.

Department of Trade and Industry, and PricewaterhouseCoopers, "Information Security Breaches Survey 2006 - Technical Report," p. 36.

Dhillon, G., and Backhouse, J. "Current Directions in IS Security Research: Towards Socio-Organizational Perspectives," *Information Systems Journal* (11) 2001, pp 127-153.

Dhillon, G., and Torkzadeh, G. "Value-focused Assessment of Information System Security in Organizations," *Information Systems Journal* (16) 2006, pp 293-314.

DiMaggio, P.J., and Powell, W.W. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields," *American Sociological Review* (48:2) 1983, pp 147-160.

Gordon, L., Loeb, M., Lucyshyn, W., and Richardson, R. *2006 CSI/FBI Computer Crime and Security Survey* Computer Security Institute, 2006, p. 29.

Guler, I., Guillen, M., and Macpherson, J. "Global Competition Institutions, and the Diffusion of Organizational Practices: The International Spread of ISO 9000 Quality Certificates," *Administrative Science Quarterly* (47:2) 2002, pp 207-223.

Hu, Q., Hart, P., and Cooke, D. "The Role of External Influences on Organizational Information Security Practices: an institutional perspective," 39th Hawaii International Conference on System Sciences, Hawaii, 2006, pp. 1-10.

Iacono, C., Benbasat, I., and Dexter, A. "Electronic Data Interchange and Small Organisation: Adoption and Impact of Technology," *MIS Quarterly* (19:4) 1995, pp 465-485.

Kankanhalli, A., Teo, H.H., and Wei, K.K. "An Integrative Study of Information Systems Security Effectiveness," *International Journal of Information Management* (23:2) 2003, pp 139-154.

Klein, H., and Myers, M. "A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems," *MIS Quarterly* (23:1) 1999, pp 67-94.

Lee, A.S. "Integrating Positivist and Interpretive Approaches to Organizational Research," *Organization Science* (2:4) 1991, pp p342-365.

Lin, A. and T. Conford. "Framing Implementation Management," International Conference on Information Systems, Brisbane, Australia, 2000

McLoughlin, I., Badham, R., and Couchman, P. "Rethinking Political Process in Technological Change: Socio-technical Configurations and Frames," *Technology Analysis & Strategic Management* (12:17-37) 2000.

Meyer, J., and Rowan, B. "Institutionalized Organizations: Formal Structure as Myth and Ceremony," in: *The New Institutionalism in Organizational Analysis,* P.J. DiMaggio and W.W. Powell (eds.), The University Press of Chicago, London, 1991, pp. 41-62.

Minsky, M. "A framework for representing knowledge," in: *The Psychology of Computer Vision,* P. Winston (ed.), McGraw-Hill, New York, 1975, pp. 211-277.

Orlikowski, W. "Learning from Notes: Organizational Issues in Groupware Implementation," *Information Society* (9:3) 1993, pp 237-250.

Orlikowski, W., and Gash, D. "Technological Frames: Making Sense of Information Technology in Organizations," *ACM Transactions on Information Systems* (12:1) 1994, pp 174-207.

Orlikowski, W.J., and Baroudi, J. "Studying Information Technology in Organizations: Research Approaches and Assumptions," *Information Systems Research* (2:1) 1991, pp 1-28.

Rathswohl, E.J. "Appling Don Idhe's Phenomenology of Instrumentation as a Framework for Designing Research in Information Systems," in: *The Information Systems Research Arena of the 90s, Challenges, Perceptions and Alternative Approaches,* H.-E. Nissen (ed.), North Holland, Amsterdam, 1991.

Sahay, S. "Implementation of Information Technology: A Time-Space Perspective," *Organisation Studies* (18:2) 1997, pp 229-260.

Sahay, S., Palit, M., and Robey, D. "A Relativist Approach to Studying the Social Construction of Information Technology," *European Journal of Information Systems* (3:4) 1994, pp 248-258.

Scott, W.R. *Institutions and Organizations* Sage Publications, London, 2001

Silva, L. "Epistemological and theoretical Challenges for Studying Power and Politics in Information Systems," *Information Systems Journal* (17) 2007, pp 165-183.

Silva, L., and Backhouse, J. "The Circuit Of Power Framework For Studying Power in Institutionalization of Information Systems," *Journal of Associations for Information Systems*, 2003.

Siponen, M. "A Conceptual Foundation for Organizational Information Security Awareness," *Information Management & Computer Security* (8:1) 2000, pp 31-41.

Siponen, M., and Iivari, J. "Six Design Theories for IS Security Policies and Guidelines," *Journal of Associations for Information Systems* (7:7) 2006, pp 445-472.

Straub, D. "Effective IS Security: An Empirical Study," *Information Systems Research* (1:3) 1990, pp 255-276.

Straub, D., and Welke, R.J. "Coping with Systems Risk: Security Planning Models for Management Decision-Making," *MIS Quarterly* (22:4) 1998, pp 441-469.

Suchman, M. "Managing Legitimacy: Strategies and Institutional Approaches," *Academy of Management Review*, 20(3), 1995, pp. 571-610

Teo, H.H., Wei, K.K., and Benbasat, I. "Predicting Intention to Adopt Interorganisational Linkage: An Institutional Perspective," *MIS Quarterly* (27:1) 2003, pp 19-49.

Tingling, P., and Parent, M. "Mimetic Isomorphism & Technology Evaluation: Does Limitation Transcend Judgment?," *Journal of Associations for Information Systems* (3:5) 2002, pp 113-143.

Vroom, C., and von Solms, R. "Towards Information Security Behavioral Compliance," *Computer & Security* (23) 2004, pp 191-198.

Walsham, G. "Interpretive case studies in IS research: nature and method," *European Journal of Information Systems* 1995, pp 474-481.

Whitman, M., Townsend, A., and Aalberts, R. "Information Systems Security and the Need for Policy," in: *Information Security Management: Global Challenges in the New Millennium,* G. Dhillon (ed.), IDEA Group Publishing, Hershey, 2001.

Willcocks, L., and Margetts, H. "Risk Assessment and Information Systems," *European Journal of Information Systems* (3) 1994, pp 127-139.

Willison, R. "Understanding the Offender/Environment Dynamic for Computer Crimes," *Information Technology & People* (19:2) 2006, pp 170-186

Yin, R. *Case Study Research Design and Methods* SAGE Publications, Thousand Oaks, 1994.