European Journal of Information Systems (2009) 18, 140–150
© 2009 Operational Research Society Ltd. All rights reserved 0960-085X/09
www.palgrave-journals.com/ejis/

Frame misalignment: interpreting the implementation of information systems security certification in an organization

Carol W. Hsu

Department of Information Management, National Taiwan University, Taiwan

Correspondence: Carol W. Hsu, Department of Information Management, National Taiwan University, No.1, Sec. 4, Roosevelt Road, Taipei City 106, Taiwan.
Tel: +886 2 3366 1196;
Fax: +886 2 3366 1199;

Abstract

Although several studies have discussed the framework and value of information systems (IS) security standards and certification, there has been relatively little empirical research on how different groups of stakeholders in an organization interpret and behave during the implementation process. In an attempt to fill this research gap, this study employs a socio-cognitive perspective, namely the concept of frames analysis, to investigate how the managers and employees of a financial institution make sense of IS security certification, BS 7799 Part 2, and how these interpretations influence their actions. Using an interpretive case study approach, the findings show that the expectations of management have a strong impact on the implementation of the certification process. Moreover, the incongruence between the perceptions of managers and those of the certification team and other employees means that IS security management concepts may not be fully embedded in the organization's work practices and routines. This article argues that during the certification process, managers should place more emphasis on the identification of frame incongruence and undertake early intervention to align frames in order to achieve overall security effectiveness in the organization.

European Journal of Information Systems (2009) **18,** 140–150. doi:10.1057/ejis.2009.7; published online 31 March 2009

Keywords: IS security; technological frames; IS security standard; security certification; interpretive research; institutionalization

Introduction

An increasing number of organizations are initiating information systems (IS) security management projects to tackle the growing number of security incidents, and also to meet the requirements of regulatory compliance legislation, such as the Sarbanes-Oxley Act and the Data Protection Act (DTI & PWC, 2006; Gordon *et al.*, 2006). One strategy involves implementing IS security standards, such as BS 7799 Part 1 or ISO/IEC 17799, or acquiring certification, such as BS 7799 Part 2 or ISO 27001 (Tashi & Ghernaouti-Helie, 2007). These standards and certifications set out the requirements of good IS security management practices covering aspects of people, processes, IT systems and policies (von Solms, 1998, 1999). From a research perspective, although IS security researchers have acknowledged the importance of these standards and certifications, there are relatively few empirical studies of their actual implementation. However, empirical investigation is fundamental to help IS security scholars and professionals understand the organizational changes and consequences resulting from the application of these standards in practice.

Received: 1 April 2008
Revised: 16 August 2008
2nd Revision: 15 January 2009
Accepted: 23 February 2009

In an attempt to fill this research gap, this study investigates how a financial organization's members understand and interpret BS 7799 Part 2 certification, and how they use these meanings to guide their actions over the course of the certification implementation process.

Focusing on the interpretive process, the study adopts frames analysis as the theoretical lens. The objective is to identify the perceptions and assumptions of different groups of stakeholders in an organization and examine the organizational consequences resulting from frame incongruence. To this end, an empirical study was carried out in a financial institution where the certification process was initiated in early 2004 and completed in late 2005. The results of the investigation have both theoretical and practical implications. From the standpoint of research, the investigation adds to the IS security literature by providing insights into how and why people behave differently in the context of certification implementation. Meanwhile, for IS security professionals, frames analysis provides an analytical tool to obtain the interpretations of organizational members at different stages of the certification process. This can help IS security professionals activate intervention strategies, if necessary, to shape and reshape organizational members' perceptions in order to achieve the desired level of security awareness and effectiveness. The empirical results also identify issues that managers should be aware of during the certification process.

The remainder of this paper is organized as follows. The next section reviews the literature on the IS security standard and certification process, and explains the theoretical framework. The research methodology and the case company, called the Finance House, are also presented. The discussion of the findings focuses on the assumptions of different stakeholder groups and analyzes the incongruence that exists between them. The paper concludes by considering the contributions and implications of this research.

Literature review

Security standards can be either technology-oriented or management-oriented. Technology-oriented standards deal with the physical and logical specification of a product or information technology, while management-oriented standards are designed to ensure good management practices in organizations. In the field of IS security, ISO/IEC 9594-8 for public key certificates and ISO/IEC 9797-1:1999 for message authentication codes are two examples of technological standards; and ISO 17999 is an example of a management standard. Terlaak (2007) argues that standards exemplify the notion of private-centralized institutions because (1) their creation involves various representative stakeholders and their compliance is not mandated by law and (2) they are maintained by a centralized institution, such as the British Standards Institute (BSI) or the International Organization for Standardization (ISO). Most management standards (e.g., ISO 9000 and ISO 14001) also provide a certification scheme for compliant firms. In the area of IS security, BS 7799 Part 1 was published in the United Kingdom in 1995, and BS 7799 Part 2 was published in February 1998 to support the certification process. As part of the internationalization of standards development, in December 2000, Part 1 was published as ISO/IEC 17799 and Part 2 became ISO/IEC 27001 in 2005. Firms seeking certification are required to submit to an audit by an accredited certification body. Such bodies range from government testing laboratories to private organizations and accounting firms (Guler *et al.*, 2002).

BS 7799 has gained a great deal of scholarly support as the most appropriate mechanism for achieving security management best practices in organizations (e.g., Kearvell-White, 1996; von Solms, 1998, 1999). In particular, some researchers emphasize the importance of establishing information security standards as a precondition for achieving trust and thereby fostering electronic commerce (von Solms, 1998). Given their increasing significance in IS security management, other researchers have focused on analyzing the underlying assumptions of these established standards. Applying Burrell and Morgan's framework, Dhillon & Backhouse (2001) argued that the concept of BS 7799 is rooted in the functionalist paradigm to create an evaluation basis for addressing security management issues. Subsequently, Siponen (2005) posited that ISO/IEC 17799, which was developed with a means-end-oriented research objective, has a technical role in an organization because user acceptance is not considered in the framework.

Despite the importance of IS security standards, relatively few studies have considered the issues that arise during the adoption and diffusion process. Backhouse *et al.* (2006) described the institutionalization process of BS 7799 at the industry and international level; and Tejay (2005) developed an efficiency model to help managers make decisions about the appropriate number of standards to adopt. Using semi-structured interviews at four small- and medium-sized enterprises (SMEs), Wiander (2007) found that organizations welcome the competitive advantage and the increase in customer demand that result from adopting ISO/IEC 17799; however, the cost and the heavy administrative workload are the least desirable aspects of the standard's implementation. Wiander (2008) also investigated the role of organizational culture and top management support during the audit process. In short, a review of the existing literature indicates that empirical studies on the adoption of IS security management standards are still relatively lacking (Siponen, 2003; Wiander, 2008). By contrast, the spread of other management standards, such as ISO 9000 and ISO 14000, has generated significant research interest (Westphal *et al.*, 1997; Shannon *et al.*, 1999; Beck & Walgenbach, 2005; Terlaak & King, 2006). Given the predominance of descriptive and conceptual research (Siponen & Willison, 2007), this study contributes to the literature on IS security standards by providing empirical content derived through an interpretive study.

As mentioned earlier, meeting certification requirements involves organizational changes (Wiander, 2008), which are associated with the processes of sense-making and interpretation (Daft & Weick, 1984; Gioia *et al.*, 1994). In the area of security research, researchers have discussed the importance of people's assumptions and their interpretations of IS security requirements (Vroom & von Solms, 2004; Dhillon & Torkzadeh, 2006). Nevertheless, an in-depth investigation of people's expectations, assumptions and attitudes toward IS security certification is still lacking. Given the emphasis on assumptions and interpretations, the next section explains why the concept of frames analysis is an appropriate theoretical lens for this study.

Theoretical framework

Focusing on the interpretive process, this research adopts the concept of frames as the basis of the theoretical framework. Minsky (1975) introduced the term 'frame' to describe 'a data-structure representing a stereotyped situation' (p. 212) in artificial intelligence applications. Many terms can be used to describe the formation and existence of such understanding, for example, 'schema,' 'cognitive maps,' 'mental models,' 'frames,' 'paradigms,' 'scripts' and 'thought worlds' (Orlikowski & Gash, 1994). The term 'frames' is used in this study. The socio-cognitive approach shares the belief of social constructivism theorists that knowledge cannot effectively construct meaning in isolation, and reality is a personal interpretation dependent on how individuals perceive their experiences. On the basis of these views of epistemology and ontology, socio-cognitive theorists maintain that action is subject to the interpretation of the individual on the basis of his worldview and the surrounding environment. Echoing this view, Bandura (1986) argued that 'what people think, believe, and feel affects how they behave' (p. 25).

Within the scope of organizational studies, a frame has several characteristics. Essentially, a frame is a mechanism for an individual's sense-making. It helps people reconcile their current knowledge with new information presented by the environment, and thus gives meaning to their understanding of the world. An individual's frame is always situated in the context of a particular time and space. The same frame can be employed as a reference in different situations; however, the context might constrain or elaborate on an individual's interpretation of an object or event and therefore lead to different understandings and actions. Although frames are normally held independently by individuals, there are situations in which shared frames are important. For example, the 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. In the context of an organization, Pinch & Bijker (1987) refer to such groups as 'relevant social groups' (p. 30) and argue that one can only start defining problems and tracing the common frames shared by members of each relevant social group when all, or at least the most relevant, social groups have been located. Different relevant social groups might define problems or share frames differently. Moreover, each group may assign different meanings to the surrounding organizational artifacts and subsequently take different actions. In other words, when the interpretations of different relevant social groups in an organization are misaligned, there exists an incongruence of the frames. In this situation, the problem of poor IT appropriation and user resistance might occur (Orlikowski & Gash, 1994).

Building on the concept of frames, Orlikowski (1993) and Orlikowski & Gash (1994) extended the applicability of frames analysis to organizational science and developed the concept of technological frames. They use the term 'technological frames' to describe the mental models that members of an organization use to make assumptions about, develop expectations of, and interpret the technology they use in that particular organization. A number of empirical studies have shown that technological frames analysis can be used to determine how different actors make sense of information technology and how they interact with the technology in their organization (Orlikowski, 1993, 2000; Barrett, 1999; Lin & Cornford, 2000). Besides identifying and analyzing frame incongruence, other scholars have studied how frames can be changed through social and political intervention during the organizational change process (McLoughlin *et al.*, 2000; Lin & Silva, 2005).

In this article, the objective is to investigate how different groups within an organization interpret and behave during the IS security certification process. Frames analysis allows a researcher to identify the underlying assumptions and interpretations that different relevant social groups hold throughout the implementation process (e.g., initiation, implementation and completion of the IS security certification scheme), and determine whether there exists any incongruence between the frames in the organization. Before discussing the findings, the next section details the research methodology and the case study.

Research method

Given the objective of capturing people's interpretations and perceptions of IS security certification in a specific organizational context, this research employs an interpretive approach to develop insights into the organization in the case study. Recent research has shown the value of interpretive case studies in understanding the development of standards (Backhouse *et al.*, 2006; Markus *et al.*, 2006) and the certification process (Boiral, 2003). In discussing the application of technological frames analysis, Davidson (2006) argued that the interpretive case study can 'produce a theoretically informed interpretation of the research context, which is one form of general knowledge' (p. 25).

The empirical setting of this research is a Taiwanese financial institution called the Finance House (a pseudonym). The company has over 400 employees in 11 departments. The business operations of the Finance House are tightly regulated by the financial supervisory authority. In early 2004, the organization started the certification process for BS 7799 Part 2, and enterprise-wide certification was obtained in October 2005. This empirical research covers the certification period.

The researcher was a manager with Finance House between July 2004 and December 2005. Data sources included observation notes, informal conversations with employees, internal security policies, minutes of the certification working group's meetings, press releases and follow-up interviews. The observation notes came from the researcher's attendance at 15 monthly Chairman-led management meetings, where the certification project's progress was reported and discussed. The researcher found that social lunches provided an informal setting in which employees felt more relaxed about discussing their perceptions and knowledge of the certification scheme's progress. During the research period, over 30 such lunches were arranged and the topic of certification implementation was raised in a casual manner. In addition, 34 formal documents were used in the investigation, ranging from monthly progress reports by the certification team to internal IS security training materials, internal IS security policies and procedures, meeting minutes and organizational publications. After the researcher left the company, five formal follow-up interviews were conducted in mid-2006 to validate the early interpretations of the results and identify any inconsistencies. The interviews consisted of two interviews with senior executive managers; two group interviews with three and two employees, respectively, from four different departments and one with the staff of the internal audit department. Each interview lasted between 1 and 2 h.

Given the nature of the subject under investigation, gaining access to information could have been difficult, especially when the focus was on personal interpretations of security issues. In this situation, personal contact with organizational actors proved invaluable because it facilitated 'in-depth access to people, issues, and data' (Walsham, 2006, p. 321). The familiarity between the researcher and the interviewees allowed the latter to feel at ease about discussing possibly sensitive or confidential issues. This helped reduce the problems associated with qualitative interviews, such as the lack of trust and the artificiality of the interview process (Myers & Newman, 2007). Even so, it is worth noting that being an *insider* meant that participants were more likely to perceive a conflict of interest between themselves and the researcher. In this case study, the researcher developed a research interest in the subject after becoming acquainted with some internal auditors and having informal conversations about the implementation process. The researcher was in charge of corporate communications with international business partners and did not participate in the certification decision-making process, or work in relevant departments which were in charge of the implementation. Hence, the researcher played a neutral role, which helped to prevent any potential political conflicts with the interviewees that might have impacted on the quality of the data collected. This factor also minimized the possibility that the researcher's own perspective might jeopardize the validity of the research findings. It is also worth noting that the use of multiple sources of information helps demonstrate the credibility and dependability of interpretive case study research (Yin, 1994; Darke *et al.*, 1998).

To analyze the data, the concept of frames was used to structure the narrative of the case, thereby constructing a dialogical process between the data and the theory (Klein & Myers, 1999). The interpretations were validated by following the approach suggested by Orlikowski & Gash (1994). Specifically, the theoretical framework informed the identification process of the relevant social groups and the frames domain. The initial understanding of the implementation process led the researcher to identify three distinct relevant social groups in the empirical setting. The interview data and field notes for each group were then studied and organized into different themes. Through reading the field notes and interview materials several times, the researcher refined the development of the themes and ensured that they were dominant across different interest groups. If conflicting or incomplete interpretations of a certain event or statement were identified, the participants were contacted for clarification. In the last stage, the five follow-up interviews played an important role in validating the frames' domains and themes.

Case study

In late 2003, following a national security assessment exercise, the government decided to incorporate three of Finance House's main computer systems into the national critical infrastructure. Other similar systems included in the infrastructure were the trading systems operated by the securities and futures exchanges. As a consequence of this government decision, in early 2004, the financial supervisory authority mandated that Finance House as well as the above exchanges must achieve a certain standard of IS security management. Explicitly, the authority stipulated BS 7799 Part 2 certification, and required these organizations to complete the certification process within a reasonable period.

A certification team was formed at Finance House to work on the certification project in early 2004. In October, the firm obtained the relevant certificates for its three main operating systems; and a year later, enterprise-wide BS 7799 Part 2 certification was achieved. Table 1 details the composition of the three relevant social groups involved in the process, namely the Management Group (MG), the Certification Team (CT) and Other Employees (OT). Because of the number of

Table 1 Summary of relevant social groups in the Finance House

Group	*Composition*
Management Group (MG)	• Five members at the senior executive management level
Certification Team (CT)	• Members in IT and internal audit departments with responsibility for implementing the project
Other Employees (OT)	• Members from other nine departments

subjects that participated in informal and formal interviews, each participant is identified in terms of his/her relevant social group and a number, for example, the code CT 2 means a member of the Certification Team. The next section presents the findings on the groups' interpretations of why certification was introduced (the certification strategy), how it was implemented throughout the organization (perceptions of the implementation process) and how it impacted on daily work practices after implementation (the outcome of certification).

Certification strategy

The Management Group initiated the BS 7799 Part 2 certification project to comply with the mandatory requirement of the financial supervisory authority. Although the regulatory authority did not set an explicit deadline for completion of the certification process, an urgent management-level meeting was held at Finance House to discuss the issue. At the meeting, senior management felt that, initially, the scope of certification should be limited to the three main operating systems. By focusing on those systems, which already had good IT security controls in place, senior management believed the company could obtain certification without making too many adjustments to the existing security infrastructure. The timeline was important because, as one senior executive pointed out: 'speedy completion would allow the company to quickly demonstrate the firm's compliance to the authority.' Besides meeting the regulatory requirements, the Chairman also believed that, given the nature of the financial business, obtaining BS 7799 certification would have a positive impact on public confidence in the company. In one meeting, he expressed this belief as follows:

> The certification will demonstrate to the public that we have secure back-office securities processing systems. Therefore, investors will have confidence when trusting us with securities settlements and the computerized book-entry services we provide.

As instructed by the Management Group, the IT department and internal audit department formed a task force for the project, referred to as the Certification Team. When asked during informal conversations about the reasons for forming the team, some members mentioned compliance (CT 1, 2 and 4). In addition, during a social lunch with four internal auditors, one senior member (CT 9) responded with 'taking orders' and two other members (CT 1, 6) echoed this view with similar comments like 'doing as instructed by the boss.'

Similar responses were given by employees from another department in the organization. During social lunches designed to gain information, the researcher asked employees whether they were aware of the project and why the company decided to seek BS 7799 Part 2 certification. Many had no knowledge of the project and showed very little interest in continuing conversations on the topic during informal discussions. In a social gathering with five employees (OT 12, 16, 22, 23, 24), one employee made the following comment, which the others agreed with:

> This is probably some strategic decision by the big boss. It probably won't really affect daily work practices, except for the IT people. Not knowing what it is does not worry me.

Image of the implementation process

The Management Group assumed that the implementation of the BS 7799 standard would be fairly straightforward because the organization had a strong IT security infrastructure. At the start of the implementation process, the Management Group learnt that the leading organization in their sector had successfully obtained certification with highly complementary comments from the external auditor. Despite having confidence in their existing technical controls, members of the Management Group were concerned that unfamiliarity with specific certification requirements might slow down the process and impact on the outcome of the external audit. This concern led to a decision to hire consultants to assist with the project. One of the consultants made the following remark about the Management Group's commitment to scoring high marks in the audit exercise:

> I was told that the company wanted to be the best. After the first few meetings with the senior management, I realised that the goal was not only obtaining the certificates, but also getting 90 or even higher in the audit assessment.

With the strong technical security already implemented, the Certification Team concentrated on preparing documents for the first stage of the BS 7799 audit. At the same time, all members of the team were studying for the qualification of BS 7799 Lead Auditor. During 2004, 22 members obtained the qualification. This number was higher than in other comparable organizations. Members of the Certification Team also expressed satisfaction with the increase in their knowledge of risk management and security management resulting from their interaction with the external consultants and the training program for the qualification exam.

Because of the pressure to complete the process, the Certification Team believed that they did not have sufficient resources or time for appropriate employee education and awareness programs. In the follow-up interview, one member from the business department (OT 45) commented on the compliance-centric attitude of the Certification Team as follows:

> I was asked to provide information on the risk assessment form circulated [by the Certification Team]. I found the criteria were not suitable for the evaluation of the business activities of my department. I wanted to discuss this with them, but they told me to try to squeeze information in. I think that they did not really care about learning how risks might arise in my department!

The opinion that the process was an exercise in document production was also observed in other employees' interpretations. During informal conversations, there were comments that the process was an extension of the ISO 9000 certification, which the company had obtained a few years earlier. The lack of emphasis on employee empowerment and development of a security culture was also reflected in the organization of the 144 sessions of the security-related training program. Materials were delivered in a lecture format by the consultants. The content was generic about IS security policy and risk management, and there were no interactive discussions designed to educate employees about the risks in their daily work practices. As a consequence, employees believed that the attendance was just one way to accumulate the hours required to fulfill annual training course attendance quotas. After the training, one employee (OT 31) stated that

> Some people fell asleep. We had to fulfil enough [training] hours, so we picked the program that is offered after work.

Outcome of certification

With respect to the interpretation of the outcome of the certification process, we observed that the Management Group thought the certification was a major milestone and a success in terms of increasing the profile of the company. For publicity purposes, in October 2004, the company organized an official BS 7799 certificate presentation ceremony, which was attended by a large number of Finance House employees, as well as guests from the supervisory authority and a representative from the British Standards Institute. In the ceremony, the Chairman remarked that

> The company has 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 strategy of informing the public about achieving BS 7799 Part 2 certification was complemented by the publication of newsletters, monthly company journals and flyers sent to individual/institutional investors.

Furthermore, one senior executive believed that having completed the process, the organization had enhanced its internal compliance procedure. His view on a strict compliance environment was consistent with the following continuous developments in the organization: (1) the requirement that at least two employees obtain relevant information systems auditor certification each year, (2) the installation of full-scale intrusion and detection systems as well as intrusion and prevention systems and (3) the installation of an Internet monitoring system.

The Certification Team held similar opinions to the Management Group, that is, 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, some members (e.g., CT 2, 4 and 5) cited the reduction in the number of technical and operational errors in the compliance report, rather than commenting on changes in other employees' knowledge or behavior.

In addition, the Certification Team believed that maintaining the good result in the ongoing external audit and minimizing the operational errors would depend on their ability to perform more frequent internal audits, rather than on trusting employees' self-awareness and ability to follow good security management practices. One internal auditor (CT 6) told the following amusing story about the use of instant messaging, which was not allowed under the organization's IS security policy.

> After the first round of the internal audit, users knew that MSN was not allowed. I asked them to remove it. However, they moved to web MSN, which can be detected by our Internet monitoring software. Again, they were notified, and they complied. However, their good behavior only lasted for short periods, either before or after my audit of the department. This pattern keeps going on as a cycle.

Other employees held different views about the certification outcome. During informal conversations, some staff (e.g., OT 2, 6, 16 and 30) expressed the view that the increase in compliance resulting from the certification project created more inconvenience than benefits. The perception of inconvenience and strict compliance 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 were not permitted to use portable devices, such as USB memory sticks or portable hard disks, unless they had written approval from the appropriate manager. However, it was observed that employees tended to violate this rule because they had to attend meetings outside the company or travel on company business.

Discussion

Table 2 summarizes the findings about the frames of the three relevant social groups at Finance House during the BS 7799 Part 2 certification process. The following section critically assesses the assumptions and interpretations of different stakeholder groups and analyzes the incongruence that existed.

Table 2 Understanding and actions of three relevant social groups on different frame domains

Frame domain	*Understanding of relevant social groups*	*Actions of relevant social groups*
Certification strategy	Management group • Compliance with the regulatory requirements • Certification has positive impact on public confidence in the company	Management group • Start certification process on the three main operating systems • Make progress report at the Chairman-led monthly management meeting
	Certification team • Compliance with the regulatory requirements • Top management decisions	Certification team • Only work within the scope of certification required by the regulations and top management
	Other employees • Do not know the purpose of certification • Top management decision, not relate to their job	Other employees • Show little interest in learning the nature and value of certification
Images of implementation process	Management group • A straightforward task given the existing good IT security controls in place • Can achieve high score in the audit assessment	Management group • Hire external consultants to assist with the preparation of audit documents • Certification team members required to obtain BS 7799 Lead Auditor qualification
	Certification team • Meet the management's expectations about auditor qualification • Focus on the scope of certification required by the regulations • Knowledge improvement	Certification team • Study for BS 7799 Lead Auditor qualification • Develop the formal compliance policy and procedures
	Other employees • Another ISO 9000 project • Implementation is the responsibility of certification team	Other employees • Limited to producing documents required by the certification team • Passively attend the required training program
Outcome of certification	Management group • Highly successful project • Develop a strict security management system	Management group • Organize the certification presentation ceremony • Publish the achievement in company newsletter and journals
	Certification team • Establish formal compliance procedures • Maintenance requires frequent internal audits	Certification team • Perform more internal audits • Correct inappropriate user behavior through regular audits
	Other employees • Strict security controls create inconvenience	Other employees • Violate certain security controls if business needs arise

Institutional isomorphism shapes the assumptions of the management

Neo-institutional theorists suggest that practices travel from one organization to another because of the isomorphic nature of social systems. Researchers have defined three types of institutional forces, namely coercive, normative, and mimetic isomorphism (DiMaggio & Powell, 1983), which influence an organization's decisions about the adoption and assimilation of new ideas. *Coercive* isomorphism refers to the political influence exerted by government agencies or powerful organizations. *Mimetic* isomorphism represents the imitation of one organization perceived by others as successful or legitimate in an organizational field. *Normative* isomorphism represents the collective influences resulting from the development of professionalization. This study found that coercive force and mimetic force played an important role in shaping management's interpretation of the certification process, while normative force facilitated knowledge improvement of the certification team, as described later in the article.

Previous IS security studies have offered the conceptual arguments that the IS security standard and certification can help organizations comply with regulatory requirements (Haworth & Pietron, 2006; Hu *et al.*, 2006; Tashi & Ghernaouti-Helie, 2007) and achieve competitive advantages (Wiander, 2007). Both arguments were empirically supported by the findings of this case study. At Finance House, the Management Group viewed certification as a means of meeting the regulatory requirements and demonstrating the firm's compliance to the authority. These interpretations led to the subsequent action of initiating BS 7799 Part 2 certification. Furthermore, the regulatory authority had a significant influence on the Management Group's expectations about the scope of the information systems considered for BS 7799 Part 2 certification. In other words, the coercive pressure shaped the management's assessment of the value of BS 7799 Part 2 certification, which led to the decision about limiting it to three key operating systems.

Besides regulatory pressure, the data also shows that structural equivalence in the institutional environment led to competitive mimicry between Finance House and other companies in the inter-organizational network. Institutional mimicry is more likely to occur for competitive reasons, or as a strategy to address uncertainty and ambiguity (DiMaggio & Powell, 1983; Guler *et al.*, 2002; Tingling & Parent, 2002). In the context of the financial sector, Ang & Cummings (1997) pointed out that in the hyper-competitive financial environment, 'peer banks exert considerable influence on each other because of tight professional networks formalized by memberships in regional and national bank associations' (p. 237). The results of this study also suggest strong rivalry and competitive pressure in the financial sector as well as tight links. Peer influence on the adoption of BS 7799 Part 2 certification was evidenced by the Management Group's concern over the external audit score. The concern about whether the company could achieve a better score than rival organizations indicates that the company did not want to be disadvantaged in the marketplace. This competitive mimicry also led to the Management Group's decision about the timeline to complete the certification process, as the company did not want to be a late adopter and lose its competitive edge.

Meanwhile, the frames of the Certification Team and Other Employees for the certification strategy revealed an interesting finding. In the early stage of the organizational decision-making process, the impact of institutional pressure on people's perceptions seems to have been limited to the power-holders in the organization. By comparison, members of the above groups held similar interpretations of the reasons for undertaking the certification process. The understanding and actions of these two relevant social groups indicate that internal structural influences, that is, the instructions of top management, were stronger than the pressure of external institutional forces.

Frame incongruence during the implementation process

While the frames of the certification strategy shed some light on the institutional pressure for certification, the other two frame domains help us understand how different groups of stakeholders viewed the implementation process and their actions during the process. By tracing the assumptions, we can gain a better understanding of the extent that the introduced security requirements became embedded in the work routines. In the case company, the certification appeared to be successful; however, the incongruence between the management group's expectations and those of the other two groups suggests otherwise, as discussed later.

During the implementation process, the understanding and the associated actions of the Management Group reflects what Boiral (2003) identified as 'ceremonial-integrators' in his investigation of the adoption of the ISO 9000 management standard. He concluded that

> Ceremonial-integrator respondents thus focused on superficially implementing the ISO requirements, while limiting the genuine changes to their work practices to a minimum. (p. 726)

The empirical results of the current study indicate that the attitudes of management being 'ceremonial-integrators' had a dominant impact on how the other two relevant social groups made sense of the certification project. When asked for their opinions about the implementation process, the Certification Team members interpreted their role as following the instructions of the management group, whereas members of the Other Employees group viewed their role as complying with management expectations. In other words, staff from the internal audit and IT departments would not have sought to become qualified BS 7799 Lead Auditors or written the formal security policy if the requirements had not been mandated by the Management Group. Thus, this study argues that while the support of top managers is crucial in ensuring the success of IS security management in an organization, their understanding of the implementation process is another important issue that requires further research. In the case of Finance House, the management group seemed to focus on 'ensuring the existence of processes rather than the content of the processes' (Siponen, 2006, p. 97) during the certification process. However, if management had believed that IS security was everyone's concern and that it involved a change in the organization's culture, the implementation process would have been different in this case.

The findings also highlight an interesting issue concerning the design of the training program. The IS security literature recognizes that user training programs and education are crucial in enhancing employees' awareness (Thomson & von Solms, 1998; Siponen, 2000).

At Finance House, the education and training program seemed to be ineffective, as the employees retained their existing beliefs about IS security, that is, it is the responsibility of the IT department. Perhaps the program should have focused on bringing about attitude and belief changes in the staff, since 'a change in attitude is also much more likely to result in a long-term modification of behavior' (Thomson & von Solms, 1998, p.170). Without a change in the belief system, compliance behavior will only be temporary, as happened at Finance House. Lin & Silva (2005) posited that since power tends to rest with the stakeholder group initiating organizational change, this group will be in a strong position to alter the frames held by other relevant social groups in the organization. Thus, this study suggests that, to enhance security awareness, frames analysis would help IS security professionals and company managers identify whether any staff members have undesirable attitudes toward IS security, and activate an early intervention strategy accordingly.

Following the above argument about an intervention strategy, in the case of the certification team, there is evidence that their understanding of IS security was partially reframed. Through their interaction with the external consultants and participation in the auditor qualification exam, the team members' knowledge of security management improved. This demonstrates the influence of the normative force, which represents the collective influences resulting from the development of professionalization. As a result, staff from the internal audit and IT departments had the skills necessary to establish a more formal compliance procedure in the last stage of the implementation. Nevertheless, while the knowledge of meeting certification requirements had increased, employees' perceptions of their role in certification process remained 'to meet management expectations.' Consequently, little effort was made to change employees' inappropriate behavior, other than through the frequent audit procedures.

Implications of frames analysis

In this article, the author has applied the concept of frames analysis to investigate the process of implementing an IS security certification scheme in an organization. It is believed that this approach provides an analytical tool for understanding the perceptions and behavior of relevant social groups when new IS security management practices are introduced in an organization. The following sections consider the research and practical contributions of the present study.

Research contributions

This study contributes to the literature on institutional research and IS security standards in a number of ways. First, it supports Orlikowski & Gash's (1994) argument about the contribution of frames analysis to other social construction processes such as power and legitimization. Orlikowski and Gash suggested that 'social cognitions connect to institutional analyses, which are concerned with shared, taken-for-granted systems of social rules and conventions' (p. 199). The concept of frames allows researchers to develop a deeper understanding of how and why people behave in a certain way towards the introduction of new organizational practices. For example, the institutional environment shapes the assumption of the management group about the certification strategy and implementation process. By applying frames analysis, it provides a lens through which to understand the interpretive schemas of human actions during the implementation process. The analysis of interpretations and assumptions reveals a rich picture of what different stakeholder groups within the organization really believe about the implementation of an IS security certification scheme. These explanations would have been missed if the analysis had focused solely on the structural properties of the organization.

Second, this research contributes to the literature on IS security standards research by providing empirical evidence of how organizations implement security certification requirements internally. Frames analysis allows researchers to fully investigate how people make sense of and hence enact the interpretations of their experiences and the world around them. The interpretive case study approach provides valuable insights (Walsham, 1995) into the meanings and actions associated with the implementation of the IS security standard and certification process in an organization. The research findings demonstrate that imposing strict compliance procedures at Finance House did not guarantee improved security, since employees did not change their assumptions about and interpretations of the relevance of security management. For example, some employees continued to use instant messaging and portable devices because of their convenience. In addition to supporting the conceptual beliefs put forward by others, this study extends the discussion of important issues, such as the role of top management beliefs and the design of user education programs.

Practical contributions

This empirical investigation calls for increased managerial attention to the relationship between security certification and a secure organization. The study's findings confirm the observation of Boiral (2003) that achieving certification is not the same as implementing good management practices in an organization. While security certification might have a perceived value in gaining external commercial advantages, effective security in an organization requires much more effort than simply following the normative model put forward by BS 7799 Part 2 or equivalent standards. The findings also highlight the significance of management beliefs and behavior in directing the certification implementation process. Specifically, their interpretation and understanding of the process have major consequences in terms of the shape and scope of security management changes in the organization.

In addition, the study demonstrates how IS security professionals and managers can adopt frames analysis to identify relevant social groups in their organization (Pinch & Bijker, 1987). As mentioned earlier, such groups tend to define problems in different ways; hence, each group assigns different meanings to the surrounding artifacts or technology and acts accordingly. Having an appropriate understanding on how different groups perceive IS security can strengthen the design and institutionalization of security management practices. Early identification of these inconsistencies and efforts to reconstruct meanings for employees may help reshape their perception of IS security. For instance, it would help IS security professionals design appropriate training programs that actually alter attitudes, instead of temporarily modifying behavior. In other words, rather than embrace the formal model fully, adopting a soft approach to meanings and interpretations would help increase employees' security awareness and hence their ability to make sound judgments and risk assessments when 'exceptional situations' arise (Siponen & Iivari, 2006). Security management would be more effective because employees would accept and incorporate new security principles into their work practices.

Conclusion

The primary motivation for this study was to contribute to the literature on IS security standards through an empirical investigation of the implementation process for obtaining security management certification in a financial institution. The author employed the analytical framework of frames, which considers people's assumptions, interpretations, expectations and knowledge about the nature and role of a technological artifact or organizational practice. The findings demonstrate that the relevant social groups in an organization assign different meanings to IS security management certification and use these meanings to make decisions about how to implement the related practices. The rich insights generated by this empirical investigation provide a good starting point for further research and empirical testing in the field of IS security standards. The frames analysis approach provides an analytical tool that managers can use to enhance employees' security awareness in an organization. Finally, the findings can serve as a basis for further studies of how social-organizational mechanisms can shape and reshape the interpretations of an organization's members to enhance the success and effectiveness of IS security management in the organization.

About the author

Carol Hsu is an assistant professor in the Department of Information Management at National Taiwan University, Taiwan. She holds a Ph.D. in information systems from the London School of Economics and Political Science, U.K. Her current research focuses on the organizational and cultural issues concerning security policy and technology implementation. Her work has been published in *Journal of Information Systems Security*, *Communications of the ACM* and *MIS Quarterly*.

References

ANG S and CUMMINGS L (1997) Strategic response to institutional influences on information systems outsourcing. *Organization Science* **8(3)**, 235–256.

BACKHOUSE J, HSU C and SILVA L (2006) Circuits of power in creating de jure standards: shaping an international information systems security standard. *MIS Quarterly* **30(special issue)**, 413–438.

BANDURA A (1986) *Social Foundations of Thought and Action: A Sociocognitive Theory*. Prentice-Hall, Englewood Cliffs, NJ.

BARRETT M (1999) Challenges of EDI adoption for electronic training in the London insurance market. *European Journal of Information System* **8(1)**, 1–15.

BECK N and WALGENBACH P (2005) Technical efficiency or adaptation to institutionalized expectations? The adoption of ISO 9000 standards in the German mechanical engineering industry. *Organization Studies* **26(6)**, 841–866.

BOIRAL O (2003) ISO 9000: outside the iron cage. *Organization Science* **14(6)**, 720–737.

DAFT RL and WEICK K (1984) Toward a model of organizations as interpretive systems. *Academy of Management Review* **9(2)**, 284–295.

DARKE P, SANKS G and BROADBENT M (1998) Successfully completing case study research: combining rigour, relevance and pragmatism. *Information Systems Journal* **8(4)**, 273–289.

DAVIDSON E (2006) A technological frames perspective on information technology and organizational change. *The Journal of Applied Behavioural Science* **42(1)**, 23–39.

DHILLON G and BACKHOUSE J (2001) Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal* **11(2)**, 127–153.

DHILLON G and TORKZADEH G (2006) Value-focused assessment of information system security in organizations. *Information Systems Journal* **16(3)**, 293–314.

DIMAGGIO PJ and POWELL WW (1983) The iron cage revisited: institutional isomorphism and collective rationality in organizational fields. *American Sociological Review* **48(2)**, 147–160.

DTI and PWC (2006) Information security breaches survey 2006 – Technical report.

GIOIA DA, THOMAS JB, CLARK SM and CHITTIPEDDI K (1994) Symbolism and strategic change in academia: the dynamics of sensemaking and influence. *Organization Science* **5(3)**, 363–383.

GORDON L, LOEB M, LUCYSHYN W and RICHARDSON R (2006) *CSI/FBI Computer Crime and Security Survey*. Computer Security Institute, San Francisco.

GULER I, GUILLEN M and MACPHERSON J (2002) Global competition institutions, and the diffusion of organizational practices: the international spread of ISO 9000 quality certificates. *Administrative Science Quarterly* **47(2)**, 207–233.

HAWORTH D and PIETRON L (2006) Sarbanes-Oxley: achieving compliance by starting with ISO 17799. *Information Systems Management* **23(1)**, 73–87.

HU Q, HART P and COOKE D (2006) The role of external influences on organizational information security practices: an institutional perspective. In *Proceedings of the 39th Hawaii International Conference on System Sciences* p 1–10, Hawaii.

Kearvell-White B. (1996) National (U.K.) computer security survey. *Information Management & Computer Security* **4(3)**, 3–17.

Klein H and Myers M (1999) A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly* **23(1)**, 67–94.

Lin A and Cornford T (2000) Framing implementation management. In *Proceedings of the Twenty-First International Conference on Information Systems* p 197–205, Brisbane, Australia.

Lin A and Silva L (2005) The social and political construction of technological frames. *European Journal of Information Systems* **14(1)**, 49–59.

Markus L, Steinfield C and Wigard R (2006) Industry-wide information systems standardization as collective action: the case of the U.S. residential mortgage industry. *MIS Quarterly* **30(special issue)**, 439–465.

McLoughlin I, Badham R and Couchman P (2000) Rethinking political process in technological change: socio-technical configurations and frames. *Technology Analysis & Strategic Management* **12(1)**, 17–37.

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

Myers M and Newman M (2007) The qualitative interview in IS research: examining the craft. *Information and Organization* **17(1)**, 2–26.

Orlikowski W (1993) Learning from notes: organizational issues in groupware implementation. *Information Society* **9(3)**, 237–250.

Orlikowski W (2000) Using technology and constituting structures: a practice lens for studying technology in organizations. *Organization Science* **11(4)**, 404–428.

Orlikowski W and Gash D (1994) Technological frames: making sense of information technology in organizations. *ACM Transactions on Information Systems* **12(2)**, 174–207.

Pinch TJ and Bijker WE (1987) 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* (Bijker WE, Hughes T and Pinch TJ, Eds), pp 17–50, MIT Press, Cambridge, MA.

Shannon W, Andersson J, Daly D and Johnson M (1999) Why firms seek ISO 9000 certification regulatory compliance or competitive advantage? *Production and Operation Management* **8(1)**, 28–43.

Siponen M (2000) A conceptual foundation for organizational information security awareness. *Information Management & Computer Security* **8(1)**, 31–41.

Siponen M (2003) Information security management standards: problems and solutions. In *Proceedings of the Seventh Pacific Asia Conference on Information Systems* p 1550–1561, Adelaide, Australia.

Siponen M (2005) An analysis of the traditional IS security approaches: implications for research and practice. *European Journal of Information Systems* **14(3)**, 303–315.

Siponen M (2006) Information security standards focus on the existence of process, not its content? *Communications of the ACM* **49(8)**, 97–100.

Siponen M and Iivari J (2006) Six design theories for IS security policies and guidelines. *Journal of Association for Information Systems* **7(7)**, 445–472.

Siponen M and Willison R (2007) A critical assessment of IS security research between 1990–2004. In *Proceedings of Fifteenth European Conference on Information Systems* p 1551–1559, St. Gallen, Switzerland.

Tashi I and Ghernaouti-Helie S (2007) ISO security standards as a leverage on IT security management. In *Proceedings of the Thirteenth Americas Conference on Information Systems* p 63, Keystone, USA.

Tejay G (2005) Making sense of information systems security standards. In *Proceedings of Eleventh Americas Conference on Information Systems* p 3344–3348, Omaha, NE, USA.

Terlaak A (2007) Order without law? The role of certified management standards in shaping socially desired firm behaviors. *Academy of Management Review* **32(3)**, 968–985.

Terlaak A and King A (2006) The effect of certification with the ISO 9000 quality management standard: a signaling approach. *Journal of Economic Behaviour & Organization* **60(4)**, 579–602.

Thomson M and Von Solms R (1998) Information security awareness: educating your users effectively. *Information Management & Computer Security* **6(4)**, 167–173.

Tingling P and Parent M (2002) Mimetic isomorphism & technology evaluation: does limitation transcend judgement? *Journal of Association for Information Systems* **3(1)**, 113–143.

Von Solms R (1998) Information security management (3): the code of practice for information security management. *Information Management & Computer Security* **6(5)**, 224–225.

Von Solms R (1999) Information security management: why standards are important. *Information Management & Computer Security* **7(1)**, 50–57.

Vroom C and Von Solms R (2004) Towards information security behavioral compliance. *Computer & Security* **23(3)**, 191–198.

Walsham G (1995) Interpretive case studies in IS research: nature and method. *European Journal of Information Systems* **4(2)**, 74–81.

Walsham G (2006) Doing interpretive research. *European Journal of Information Systems* **15(3)**, 320–330.

Westphal J, Gulati R and Shortell S (1997) Customization or conformity? An institutional and network perspective on the content and consequences of TQM adoption. *Administrative Science Quarterly* **42(2)**, 366–394.

Wiander T (2007) Positive and negative findings of the ISO/IEC 17799 framework. In *Proceedings of the Eighteenth Australasian Conference on Information Systems* p 622–663, Toowoomba.

Wiander T (2008) Implementing the ISO/IEC 17799 standard in practice – experiences on audit phases. In *Proceedings of the Australasian Information Security Conference*, Wollongong, Australia.

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