MIS Quarterly

SPECIAL ISSUE

CIRCUITS OF POWER IN CREATING *DE JURE* STANDARDS: SHAPING AN INTERNATIONAL INFORMATION SYSTEMS SECURITY STANDARD[1]

By: **James Backhouse**
Information Systems Department
London School of Economics and Political Science
London WC2A 2AE
UNITED KINGDOM
james.backhouse@lse.ac.uk

Carol W. Hsu
Department of Management Information Systems
National Chengchi University
Taipei 11605
TAIWAN
carolhsu@nccu.edu.tw

Leiser Silva
C. T. Bauer College of Business
University of Houston
Houston, TX 77204-5282
U.S.A.
lsilva@uh.edu

Abstract

This paper addresses the role of power and politics in setting standards. It examines the interaction of external contingencies, powerful agents, resources, meaning, and membership of relevant social and institutional groupings in generating successful political outcomes. To study these interactions, the paper adopts the circuits of power, a theoretical framework taken from the social sciences, and applies it to understanding the creation and development of the first standard in information security management. An informal group of UK security chiefs sparked off a process which led first to BS7799, the British standard, and later to ISO 17799, the international standard. The case study portrays how the institutionalization of this ad hoc development process results from the interactions of power among the stakeholders involved. The case study also shows how the different interests and objectives of the stakeholders were influenced by exogenous contingencies and institutional forces. The paper discusses theoretical and practical implications for the future development of such standards.

Keywords: Power and politics, institutionalization, information systems security standards, information systems security management, security management code of practice

Introduction

Standards are fundamental compatibility specifications that shape the configuration of information systems. Their influence extends not only to the structure of the IT industry and its markets (Jakobs 2000; Peleg and Lee 2005) but also to how information systems are used and managed (Hanseth and Braa 2001). Since standards contain inscribed actions and processes that influence organizational activities, identities and work tasks, it follows that they are instruments of power (Hanseth and Monteiro 1997). Although political processes

[1]John King was the accepting senior editor for this paper. Maryann Feldman was the associate editor. Richard Baskerville served as a reviewer. The other reviewer chose to remain anonymous.

and related factors around standards have been the subject of several studies in the IS field, these have concentrated mainly on corporate standards (Hanseth et al. 1996; Hanseth and Braa 2001) or technical specifications (Frenkel 1990).

This paper studies how power operates silently but relentlessly in the generation and institutionalization of a standard, and brings to light valuable insights into the social and political processes that form the core of standards setting work. In terms of specific research objectives, we aim at establishing the influence of exogenous contingencies for the creation of a standard and theorize about the power mechanisms required for a standard to evolve from an idea into an obligatory passage point for organizations and agencies. To achieve these research objectives, we conducted a case study around BS7799, the British standard now incorporated into the international information systems security standard ISO/IEC 17799. This standard formulates a number of key managerial controls, and sets out how an IS security policy should be written, implemented, and practiced. For our theoretical approach, we adopted the circuits of power framework (Clegg 1989; Silva and Backhouse 2003). It guided both the collection and interpretation of the data. We apply the circuits of power as a theoretical lens to make sense of the role of power in the creation and adoption of the standard.

The paper is organized as follows. In the next section, we discuss the contributions and challenges of the current literature on standards regarding political factors. We follow this discussion with the introduction of the circuits of power framework. After the research methodology sections, the narrative and interpretation of the case explores four themes elaborated from the underlying theory framework. We conclude by reflecting on the contributions, limitations, areas of further research, and implications of our research.

Power and the Creation of Standards

This paper examines the role of power and political factors behind the formation of a *de jure* standard. Such standards normally follow a set process of approval by authoritative national or international bodies, such as ANSI or ISO respectively (Hanseth and Monteiro 1997), although there are also numerous voluntary standards-writing organizations consisting of members from the relevant industry and standards-publishing bodies (David and Greenstein 1990). Economics has long been applied to understand standards phenomena. Examples range from the impact on economic performance (David and Steinmueller 1994; Swann et al. 1996), market penetration strategy (Besen and Farrell 1994; Bonino and Spring 1999; Shapiro and Varian 1999), the economics of user involvement (David and Foray 1994; Foray 1994), and the relationship with institutional and technological change (Antonelli 1994; Swann and Shurmer 1994). Network externalities and lock-in management have been adopted to study market diffusion (Shapiro and Varian 1999), while other approaches exploit bandwagon and switching-cost models to examine the problem of coordination during the standardization process (Farrell and Saloner 1986). We contend, however, that an economics approach, with its underlying baggage of objectivist rationality, means that "the effects of social relationships and the forces that these exert on the decisions of actors are ignored" (Fomin and Keil 2000, p. 207). Indeed Cargill (1989) arrives at a similar conclusion:

> Very few standards decisions are made from a purely rational economic viewpoint—while it is pleasant to claim that standards are the fruit of quantitative economic roots, it is also highly suspect and more than a little naïve (p. 5).

Cargill used the impact of European harmonization as an example of how political change acts as a force in altering the standards environment, and Scandinavian researchers have contributed to this perspective through the use of actor network theory (Hanseth and Braa 2001; Monteiro 1998; Monteiro and Hanseth 1995).[2] These researchers suggest that the decisions about design and implementation of standards are not normally reached on the basis of a rational-logical process, but are instead constructed through the constant realignment of interests among the actors involved. Our focus lies in revealing the power mechanisms that shape that realignment.

The Circuits of Power and the Study of Standards Development

As mentioned above our main theoretical assumptions about how standards are related to power arise from the work of Stewart Clegg (1989), who proposed as a theoretical framework the circuits of power.[3] Clegg uses the metaphor of a circuit to emphasize the relational nature of power in contrast to that of power reification: conceiving power as a thing that

[2]A very interesting and detailed study of how power plays a fundamental role in the creation of technical compatibility standards is the work of Manninen (2002). He focused on the elaboration of the NMT (Nordic Mobile Telephone) and GSM standards.

[3]The framework has been applied to the study of IS implementation by Silva and Backhouse (2003).

can be owned. For Clegg, power is a force like electricity, which circulates through social relations, working practices, and techniques of discipline. Beyond its relational nature, the framework has the virtue of integrating different insights from other prominent researchers who have focused on organizations and power, such as Callon (1986), Foucault (1980), Giddens (1984), Latour (1987), Lukes (1974), and Parsons (1967). We chose the circuits framework because of its critical emphasis on institutional and environmental factors. In our study, this has a special resonance since one of our main theoretical premises is that even though actors are key to the generation and adoption of standards in general, institutional factors, such as regulation and legislation, also play a fundamental role.

There are three circuits of power whose integration institutionalizes the obligatory passage points. The episodic circuit emphasizes *actions and changes in the organizational context*. It manifests when an *A* makes a *B* do something the latter would otherwise not do (Dahl 1957). The social integration circuit focuses on *rules of meaning and membership* impacting on social relations and alliances. For example, a new IS might be interpreted by trade unions as a threat while, by contrast, the self-same system might for management be simply an instrument for improving efficiency and reducing cost. The emphasis of this circuit is on symbolic power (Bourdieu 1991) and on how authority and influence depend on resources (Pfeffer 1981, 1992), status (Weber 1999), or organizational positions (Hinings et al. 1974). This circuit centers on the necessary conditions that provide *A* with the resources and legitimation to exercise power over *B*. The systemic circuit shows power circulating through *techniques of production and discipline* (Foucault 1977), facilitating and enabling *B*'s compliance (Townley 1993) and often closely relating to the obligatory passage points to which *B* is directed.

Obligatory passage points (OPPs) refer to precisely what *A* wants *B* to do. For example, a financial IS becomes an institutionalized (Callon 1986; Latour 1987) OPP in an organization when users can obtain no financial resource unless they use that system. Besides technological components, OPPs contain a combination of rhetorical devices, such as text, discourse, and disciplinary techniques. Changes in the circuits of power are introduced by *exogenous contingencies*, such as regulations, mimetic forces, or changes in industry (DiMaggio and Powell 1991; Meyer and Rowan 1991) that bring about alterations in either rules of meaning and membership or techniques of discipline and production.

The relationships among the different circuits and their integration in establishing an OPP are depicted in Figure 1. This figure illustrates our theoretical assumption that the institutionalization of a standard as an OPP is initiated by exogenous contingencies in an organizational field (here that of IS security). However, not all exogenous contingencies result in changes in a field. The final institutionalization of the OPP requires that the practices that *A* wants *B* to enact (episodic circuit) reach stability in the circuits of social and systemic integration.[4] As shown in Figure 1, this occurs in a recursive manner. Initially, *A* exercises power over *B* by drawing on rules of meaning and membership (circuit of social integration) and by deploying techniques of production and discipline (circuit of systemic integration). Likewise, insofar as the standard is an OPP for *B*, its actions will reconstitute the circuits of systemic and social integration (see Figure 1). Thus, once adopted as an OPP, the standard itself turns into a source of power.

From the circuits framework, we have formulated four theoretical assumptions to structure the narrative of the case and to guide its interpretation, presented in Table 1, which summarizes the link between the components of the circuits framework and our study of standards. This table also presents the main research questions derived from each of the circuits and their respective theoretical assumptions. These theoretical assumptions and questions are critical in synthesizing the four themes through which we develop our interpretation of the narrative.

Research Methodology

Given our objective of making sense of power moves and institutional factors affecting the adoption and generation of standards, and given the emphasis that circuits place on meaning, we adopted an interpretive stance for conducting our study (Walsham 1993). As mentioned in the introduction, the unit of analysis of our case study is the standard-setting process for BS7799, a security management standard. The timeline for the study runs from 1993, with the establishment of an industry working group, until 2000, when the code was transformed into an ISO/IEC standard. Figure 2 depicts the timeline of the case and Appendix B presents in detail the sequence of events.

[4]The concepts of social and systemic integration as related to power were developed initially by Lockwood (1964) and are also present in Giddens' (1984) structuration theory that conceives power as dual (i.e., i.e., a recursive relationship between agency and structure). We choose Clegg's model for the clarity of its concepts as well as for the relationships among technological artifacts, discipline, meanings, institutions, exogenous contingencies, agency, and obligatory passage points.

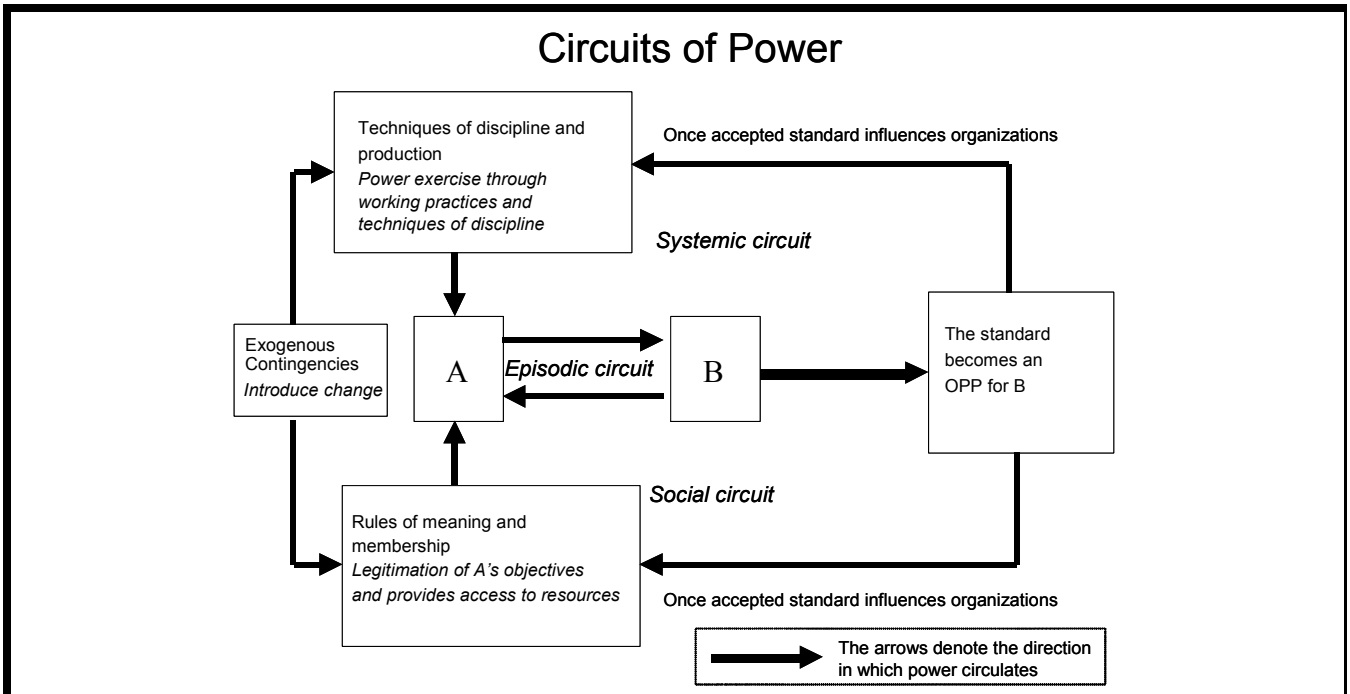

Figure 1. Theoretical Framework (adapted from *Frameworks of Power*, S. R. Clegg, 1989)

Table 1. Summary of Theoretical Framework and Research Questions

Circuits of Power Framework	Key Components	Assumption Regarding Standards	Specific Research Issues
Episodic	A makes B do something B would otherwise not do. Manifest in actions.	This relates to the group proposing the standards (A) and those (B) who have to accept them.	What are the As and Bs of the power relations? Who are the promoters and adopters of the proposed standard?
Social	Symbolic power associated with rules of meaning and membership. It is related to legitimation, authority and access to resources.	The authors of the standards have to be recognized by their organizational field as legitimate and also should be able to relate to those organizational members in power positions so the standards are accepted.	What are the key alliances for the standard to be adopted? How does each group interpret the proposed standard?
Systemic	Power exercised through techniques of discipline and production. It is related to the influence of standards on working practices.	Power is inscribed in the standards through the practices that have been adopted. Once institutionalized, the standard also becomes a source of power.	What is the main content of the standard and how these are interpreted? Are there any regulations that force the adoption of the standard?
Exogenous contingencies	Change is introduced into organizational fields as the result of exogenous contingencies.	The idea to generate standards arose from exogenous contingencies.	What were the exogenous contingencies that trigger the idea of creating the standard? How these exogenous contingencies were interpreted by the different groups?
OPP	The outcome of power is the institutionalization of OPP; those are the integration of rhetorical devices, regulations and technology.	The standard becomes an OPP for managers and organizations insofar as its prescribed practices and policies are considered valuable and interpreted to be technically sound by their peers.	How was the standard defined as an OPP? What is the relationship between the OPP and the circuits of power?

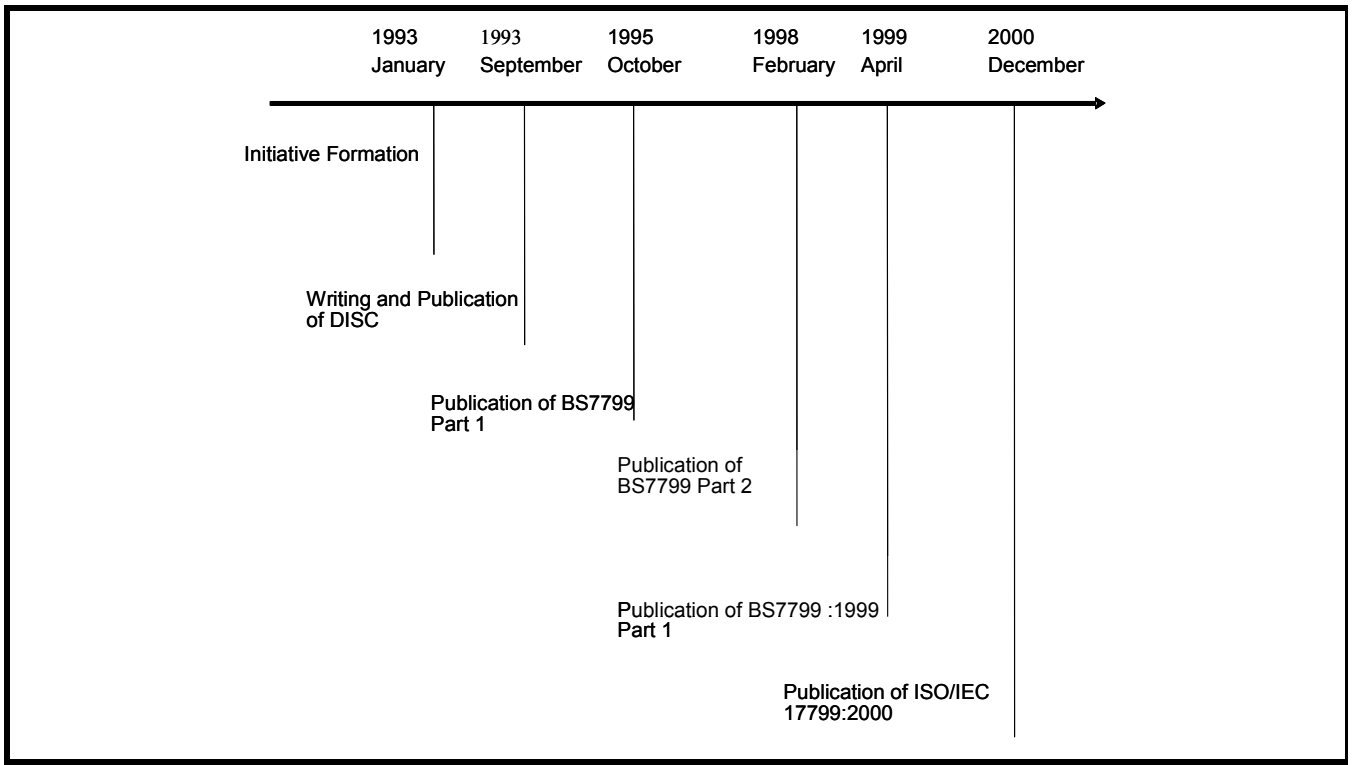

Figure 2. Chronology of Key Events

Data collection took place between September 2003 and March 2004. After a period of intensive e-mail exchange and telephone conversations, we were able to schedule 11 one-on-one semi-structured interviews. Each interview session lasted for about 90 minutes. Prior to the interviews, we developed an interview guide using the theoretical framework.[5] After the interviews, e-mails were exchanged to explore issues that required further clarification. Besides the interviews, other documents and materials were obtained during the period of the fieldwork (see Appendix A). The combination of the different sources of data (interviews, documents, and e-mail communications) provided us with what Eisenhardt (1989) calls theoretical saturation, a term she uses to denote confidence that the data collected constitutes a comprehensive picture of the phenomenon under study.

The approach adopted for analyzing the data consisted of drawing on the circuits of power to frame the narrative of the case, thereby conducting a dialogical process between data and theory (Klein and Myers 1999; Walsham 1993). In addition, when validating our interpretations we bore in mind the set of principles advanced by Klein and Myers (1999), and our reflections on their seven interpretive principles are detailed in Table 2. This activity was fundamental for articulating our findings (Eisenhardt 1989; Yin 1994). The final interpretation of our case, presented in the next section, was developed in four steps.

The first step was to identify the major events taking place between 1989 and 2000; this was achieved by reading the interview transcripts and the other sources of data. Once the main events were identified, we drafted a narrative of the case. The second step was interpreting the data. It was carried out by applying the circuits framework as a theoretical lens to tease meaning out of the data and narrative. The outcome of this exercise was building a table for each circuit of power and for the exogenous contingencies (Appendix C). The third step consisted of validating the narrative and interpretation of the case with the purpose of fulfilling the hermeneutic circle (Klein and Myers 1999). This validation was conducted by sending the initial interpretations of the case to two of our interviewees who mainly confirmed our rendition, but where there was disagreement we incorporated their views into our interpretation.

The last step of the analysis was the integration of the narrative with our synthesized interpretation. Applying the circuits

[5]Available upon request from the authors.

Table 2. Validation Criteria

Klein and Myers Criteria	Our Research
1. *Contextualization* To make sense, the interpretations require historical and social context.	One of the researchers participated in the initial meetings of the committee that set up the standard. Historical documents were collected. In addition, interviewees were asked to recollect the context and the facts surrounding the events that led to the development of the standard.
2. *Interaction between the researchers and the subjects* The subjects of the interviews are offering their interpretations of the phenomenon under study. The social interaction between researcher and interviewees influence the study.	The interviews were semi-structured and the interviewees were asked open questions that allowed them to provide their own interpretations of the events. We discussed a draft of the narrative with two of our interviewees.
3. *Abstraction and generalization* The generalization of particulars to abstract categories; generalization to social theories.	In the narrative section we develop simultaneously four themes. We did this by abstracting our interpretations of our case. We argued from the particular to the general.
4. *Dialogical reasoning* The confrontation of the original assumptions and preconceptions.	The narrative section evolves alongside a review of the four themes that emerge from the underlying theoretical framework.
5. *Multiple interpretations* The relationship among context, power, social actions and intentions.	This is the core of our paper: to explore the social and political processes that influence the development and adoption of an IS standard. We offer this interpretation as an alternative to an economic one.
6. *Suspicion* The unraveling of distortions created by the political, social and historical contexts of the subjects.	Our data collection involved not only interviews but also the gathering of documents with the purpose of validating factual information and in addition we discussed a draft of the narrative with two of our interviewees. This also with the aim of validating our interpretations.

framework as a theoretical lens, we synthesized its main concepts into our four initial theoretical assumptions (see Table 1). These four theoretical assumptions link directly the concepts of the circuits of power with our study. The episodic circuit of power corresponds to the narrative of the case that focuses on the actors' moves toward the creation and institutionalization of the standard. The narrative is interwoven with four themes. Each theme corresponds to the theoretical assumptions as depicted in Table 1: Theme 1 corresponds to the impact of exogenous contingencies while Theme 2 is related to the circuit of social integration. Theme 3 is mainly associated with the circuit of systemic integration while Theme 4 concerns the definition of the standard as an OPP.

A summary of our findings (themes) and their relation to the data and theory is found at the end of the next section in Table 3, which depicts the relationship among the circuits of power, our *a priori* categorization of the phenomenon of standard creation and adoption, and our findings.

Case Study: Narrative and Interpretation

Exogenous Contingencies Set the Scene for a Security Initiative

In 1989, the Department of Trade and Industry (DTI) invited tenders to run an IT security awareness program for business organizations in the United Kingdom. The successful company hired a public relations specialist firm to undertake media activities to raise IT security awareness. These included designing a "keep IT safe" kit containing posters, lecture notes, OHP slides, and best practices guidelines, and was sold to organizations for 500 GBP. Alongside the development of awareness programs, the DTI Commercial Computer Security Centre (CCSC) had been tasked to establish a set of security criteria both for products and good security practice. The ITSEC (information technology security eval-

uation criteria) standard for products, recognized throughout Europe, was published in 1990. It represents a single uniform and interoperable standard adopted by the UK, France, Germany, the Netherlands, and the European Commission, thereby reducing the need for products to be evaluated separately in the respective countries. In 1991, DTI worked with SEMA, an information services company, to conduct a "business needs" survey that underlined the need for security management standards and certification. Meanwhile, an international initiative in 1992 emerged in the form of the Organisation for Economic Co-operation and Development (OECD) publication, "Guidelines for the Security of Information Systems," but the general verdict was that these guidelines were too abstract to be of direct practical use for everyday security management. Nonetheless, the idea of security management standards was being discussed regularly by civil servants and industry practitioners in major security forums, including the European Security Forum, the International Information Integrity Institute (I-4), and relevant OECD meetings. A senior manager recalled the discussion.

> *Members at I-4 believed that there was a need for a security management standard. However, I-4 found that it was very difficult to collect security policies from its members. Also, at that time, security policies were written in vastly different ways in terms of content and structure. At the end, we played a war game of attack and defense. The outcome of the game was written as I-4 security baseline.*

A computer virus proved to be the spark that ignited the fire. It originated from a supplier of a well-known UK retailer and temporarily laid that retailer's systems low. A meeting in January 1993 of the DTI and the person responsible for information security at the retailer led directly to establishing, on a volunteer basis, a private industry group. Its purpose was to create a code of practice. The DTI representative who participated in the meeting in 1993 recalled its importance.

> *There were three of us at the meeting: the security manager, his director and myself. At the end of meeting, we agreed to bring together our key contacts who had expressed interest in security standards in formal and informal meetings. This decision was a very significant step forwards in this context.*

Theme 1: Impact of Exogenous Contingencies

Our data identifies two exogenous contingencies that triggered coalitions and alliances conducive to the formation of the standard. One was the publication in collaboration with the UK National Computer Centre of the DTI *Security Breaches Survey* in 1992, which dramatically concluded that UK businesses were hemorrhaging 1.1 billion GBP annually through computer security breaches (NCC 1992). The second exogenous contingency was manifested in the appearance of the virus mentioned above. The first contingency became the tipping point for the government to promote the creation of a standard. By itself, this initiative might have proved insufficient to attract the interest of industry members. However, the virus incident laid bare for all to see the vulnerability of information systems. Not until this happened did industry actors decide to collaborate seriously and share their separate experiences in security. The appearance of the virus in their midst created first a mood of consternation and then cooperation, galvanizing industry players into action. The passage from initial event to the resolution of the situation for the different actors brings to mind the prisoner's dilemma: unless exogenous contingencies alter the way actors make sense of their situations, there is no incentive for cooperation; actors will only cooperate if they believe it will result in some advantage to them.[6]

These events confirm our first theoretical assumption that exogenous contingencies can trigger the introduction of changes in organizational fields. Examining our data through this theoretical lens shows that such contingencies may have different meanings for the different groups of actors. For example, the need felt by the government to regulate IS security was not at first echoed in industry, and so the results of the survey did not signify a threat to many industry actors. Yet the survey results proved serious enough for the government to redouble its own efforts. By the same token, the computer virus did not carry the same significance for government as it did for industry, and especially for those in charge of IS security, who might have perceived it as a threat to the integrity and reputation of their companies and perhaps to their own personal livelihoods. In fact, the interpretation associated with this first theme supported by the management literature (Gersick 1991; Greenwood and Hinings 1996; Meyer and Rowan 1991), which has considered how events in the external environment can affect organizations. Our contribution to this literature rests in showing how such contingencies interact with the formation of IS standards and how they need to be meaningful for all participants if they are to be influential. In this case, the contingency betokened a threat both to security managers and to the companies for which they worked.

[6]For a discussion of the economic and social aspects of the prisoner's dilemma in IS standards, see Markus et al. (2006) and Weitzel et al. (2006) in this special issue.

Developing the Draft Standard

After the 1993 meeting, the private industry group was formed with representation from the DTI and the British Standards Institute (BSI), and from seven UK companies: the BOC Group, British Telecommunication, Marks and Spencer, Midland Bank, Nationwide Building Society, Shell International Petroleum, Shell UK, and Unilever. The representatives were all high-level security managers who had the backing of their senior directors. A head of security management in the banking sector recalled how the different companies came together for different reasons.

> *Although all the companies agreed the importance of this project, there were some slight differences in agendas. Midland Bank was hoping that the code of practice could be used as an "authoritative" document for its external partners. Marks and Spencer and Shell wanted to use this document as the compliance measure for its suppliers. The BOC Group intended to use this document as the internal mechanism for standardizing security management on different local networks. BT did not have a more specific objective, but felt the need to be involved in the development.*

Other security managers from beyond this immediate circle were also interested in this initiative but were unable to participate in the writing stage. Some, such as the security chief for Barclays Bank at the time, offered their services as reviewers. A sense of urgency quickened the pace of the initiative, uniting with a desire to avoid the dispiriting delays that standards-setting bureaucracy normally incurs. The volunteer group was charged up instead by the aim of developing standards by industry and for industry. This motivation was crystallized in the minutes of the first meeting, held on DTI premises on January 13, 1993: "*It [the code of practice] would though be useful in itself. It should be practical, pragmatic, accessible and authoritative. It was needed now*."

Although financial support was not forthcoming from the DTI, it nevertheless provided the meeting venue and facilities, as well as maintaining the emerging working document. Good industry practices were incorporated from the outset, helping to form the table of the contents, as well a checklist for completeness. Having completed the writing, the group circulated the document amongst the members and reviewers for further discussion and amendment. As one original contributor reflected,

> *To start with, all the security managers brought in security-related documents from their own companies. According to the individual's expertise, each member of the team then took a particular section for further development. For instance, S.J was responsible for physical security. D.L was in charge of logical security. Although there was some debate concerning certain sections, it was not a big obstacle and members reached agreement quickly.*

As might be expected, overt attempts at power plays emerged and one took shape in the pressure from CCSC to incorporate ITSEC[7] as a part of the document. But the group considered ITSEC to be insufficiently practical, diplomatically sidelining the protest from CCSC and retaining their focus on what could readily be implemented. Another governmental body, the Central Computer and Telecommunications Agency (CCTA), now part of the Office for Government Commerce, at the time acted as the IT consulting body for the entire UK public service. One of its products was the CCTA Risk Analysis and Management Method (CRAMM), originally developed for deployment in the UK public administration but whose value had also been recognized in the private sector. CCTA was not always supportive of the new initiative, since it had its own agenda for developing another security management standard, which would center on CRAMM. The DTI representative described the pressure he faced at that time:

> *At one of these meetings, there were people coming from CCSC to do a presentation about ITSEC and asking for it to be part of the code of practice. The writing team said no. Subsequently, there was some pressure from a higher level on me about this issue. I made it clear to CCSC and CCTA that the DTI role was neutral and it was a decision that the team would make. However, to compromise, I went back to the next meeting and suggested some form of "narrow reference" to ITSEC criteria. Surprisingly, the team decided to make a small compromise by adding a few lines on technical testing (not directly on ITSEC). The issue was dealt with relatively smoothly at the end.*

Despite the pressures, the whole development took only 6 months. The first draft was completed inside 3 months, the final draft likewise, a record in terms of turnaround time. One original contributor referred to it as the work of 'the magnificent seven" while the DTI representative regarded this remarkable achievement as the result of a magic mix of people.

[7]Von Solms (1999) provides a detailed description on the nature of ITSEC and BS7799 Part 1.

Publication as a Code of Practice

Having completed the draft, the group discussed the issue of publication. A debate raged over the copyright issue: whether to make the document freely available or copyright it and apply some minimum charge for usage. Some argued that failure to copyright would result in the document spawning numerous unapproved versions, bedeviling interoperability and running counter to the original aim of a single common standard. It was the issue and matter of control. As the DTI was reluctant to publish the document itself, BSI was proposed as a possible outlet to launch the document as quickly as possible. BSI decided to publish it as a code of practice rather than as a British Standard. This inspired choice sidestepped a number of obstacles to an early win: the stringent audit process, the strict presentation requirements, and the mandatory public consultation period. There was still, however, a small battle to be won with the BSI DISC (delivering for information solutions customers) unit on the presentation style and language of the document, as the author group wished to make the text as accessible as possible to the general public. To resolve this issue, the DTI representative convened a meeting with BSI DISC.

> *The group did not like the idea of a stiff standard format. Thus, J.B [a member of the group] and I decided to make a trip to BSI office in Milton Keynes. It was no big debate, but we had to make some effort. At the end, it was good to see BSI agreeing the presentation that the group wanted to have.*

Accordingly, the document was published in 1993 as *A Code of Practice for Information Security Management*.

Promotion and Publication as BS7799

The code immediately became a bestseller for BSI. More than 10,000 copies were sold even before the official launch at the Shell Business Centre in September 1993. Big corporations, such as Shell and Marks and Spencer, bought copies in bulk to dispense among their business units, suppliers and contractors. At the launch the audience included, alongside the original contributors, top management from several major companies. Moreover, DTI unveiled a list of 15 other companies endorsing the publication of the document. After the launch, however, no large-scale marketing campaign was mounted, although some marketing techniques were employed: press releases, ministerial public speeches, and radio broadcasts.

The code's popularity sprang from a common perception that it was the right approach at just the right time. The way it had been written made it very accessible, not just to technical experts but also to the wider business community, and even to small and medium-sized businesses that were interested enough to purchase it. Another useful ploy lay in the pricing strategy: small companies could buy it at the low price of 10 GBP. A BSI news release in October 1993 described the code as: *"intended to serve as a single reference document covering the range of controls required for most situations encountered in business."* The code comprised 10 categories, and each category contained stated objectives and a set of security controls.[8]

The transformation from a code into a full-blown British Standard took place between 1993 and 1995, requiring, as predicted, considerable time to complete all the procedures. Facilitating this process, the DTI renamed the original group, now rejoicing in the title "The BS committee in preparation for transforming DISC into a British Standard." In order to accommodate some of the bureaucratic requirements of standardization, the DTI was obliged to add other members. External consultants joined the group, as well as representatives from specific companies, such as SEMA. After a period of public consultation, the code finally matured into a standard, known as BS7799:1995. By this time, the original authoring group had taken a backstage role, with just a few founding members staying on actively to help the process of standardization.

A few participants continued to publicize the initiative in presentations at business conferences, and BS7799 continued to gain support from major companies as the chief route to assuring security standards for their own systems, suppliers, and business partners. Meanwhile, the standard won ever more accolades from industry for its practicality, and larger companies began to adopt it as the basis of their information security policy and management. An IT security consultant described this phenomenon:

> *There was a significant amount of interest in both DISC and BS7799. My company was an IT consultancy company, and after both publications were released and in particular after BS7799, we received a lot of enquires about BS7799 implementation.*

[8]The 10 categories are security policy, security organization, assets classification and control, personnel security, physical and environmental security, computer and network management, system access control, system development and maintenance, business continuity planning, and compliance.

In 1994 and 1996, DTI and their sponsors published the second and third *Security Breaches Survey*. Marking the new importance of the wider notion of information security management, in 1996, the title of the survey was changed from *IT Security Breaches Survey* to the *Information Security Breaches Survey*. In addition, from that year on, the survey included "awareness of the Code of Practice" as a questionnaire item. The name "Code of Practice" was replaced after the transformation into the British Standard BS7799.

Theme 2: Key Role of Legitimacy, Position, and Alliances

This theme stems from examining the case from the perspective of the circuit of social integration, seeing power as circulating through rules of meaning and membership. They are manifested in the alliances that representatives from different organizations formed early on, the alliances being key for the standard to be considered legitimate and necessary for later adoption. As participants gradually began to feel the standard was theirs, they defended it accordingly. Rules of meaning were clear conduits of power when the actors involved in the creation of the standard interpreted their participation as required not only for maintaining the reputation (in terms of IS security) of their respective organizations but also as a core task required by their roles and responsibilities in their firms.

For the development of this standard, an alliance was required between government and industry, two different groups of actors. Our data shows that these actors began to cooperate as a response to two different threats. For industry participants, as discussed above, the critical issues were to protect the companies that employed them, the company reputations, and not least their own job security, while for government it was the sense of complying with its mandate to regulate and to ensure stable and secure business relations. This is an interesting finding, since there were no actors interested in enrolling others, as might have been suggested by a theoretical lens such as actor network theory. However, this should not imply that no power was being exercised. The issue is that power was being exercised through discourse rather than by actors (Foucault 1980). The discourse that prevailed for the formation of the standards was triggered by the exogenous contingencies, in that the computer virus was a real threat to IS security and the survey of 1992 revealed the need to regulate IS security. This is one of the most important contributions of the circuits of power: to conceive of power beyond agency.

The alliance between industry and government was a key factor in the development of the standard. By participating, industry representatives brought legitimacy with regard to other organizations and businesses. The content they provided brought direct relevance to the standard. Without this, the standard would have been regarded as detached from practice and might not have been adopted. The participation of government was also key in three respects. First, at a practical level, it provided the infrastructure for the initial meetings. Second, it provided not only the necessary resources for the standards to be published, but also channels of distribution. Third, government backing conferred authority on the developing standard, undoubtedly clearing its way to becoming first a national and then an international standard. Therefore, this theme suggests that *de jure* standards require alliances between industry and government, and although the motivation for participation may be different, the spirit of cooperation is fundamental. Cargill's insights into the decisive position of the committee in "agreeing the scope and nature of the work facing it," together with the pivotal role of the chair person, were to some extent obviated by the fact that there was no single originator of the standard, but rather a wider-based group concentrating on the same target (Cargill 1997, p. 10).

Diffusion: Certification and Internationalization

Between 1996 and 2000, there were two important developments concerning the diffusion of BS7799. The first one was the preparation of BS7799 for its metamorphosis into an ISO standard and the second was the development and promotion of certification against BS7799. Although both developments took place concurrently, we describe first the issues surrounding certification and then the international development of the standard. Further, we describe how two new elements influenced the diffusion of the standard: the UK Data Protection Act of 1998 and the widespread adoption of outsourcing.

British companies began to adopt BS7799 as the basis of their information security policy and management, and attention began to turn to certification as consultancy and accounting firms suddenly awoke to the market potential in certifying against the standard. In September 1997, the DTI established the BS7799 Accredited Certification Steering Committee. To support the certification process, BS7799 Part 2 was published in February 1998.[9] There was unanimous agreement

[9]BS7799:1995 was a code of practice, and tailored for the certification process. BS7799:1998 Part 2 was developed to state the process of implementing and maintaining security controls identified in Part 1. Details about the differences can be accessed at http://www.xisec.com/faqs.htm#q4.

among our research respondents that the goal of facilitating commercial trading through a verifiable security certification had indeed been a primary objective of the scheme.

In April 1998, a UK minister launched the ill-fated *c:cure* certification scheme against BS7799 Part 2. Offered alongside as a generic alternative, *c:cure* was a more rigorous national scheme through which companies could obtain certification against BS7799, but was discontinued in 2000 because of low adoption rates. The confusion and frustration surrounding *c:cure* served to dampen interest in BS7799. As one IT security consultant commented,

> *I think that if there was one thing that could kill the value of BS7799, then* c:cure *did the job. There was a big confusion about the* c:cure *scheme. Also, it would cost an organization around 30,000 to 50,000 pounds to get through the whole process. The certificate only lasted for 3 years. Security managers find it difficult to justify this cost to their boss.*

The head of DTI Information Security Policy Group decided to deal with the problem of *c:cure* after his appointment in late 1998. He told us that he attended a *c:cure* steering committee meeting on the first day of his job, and concluded that *c:cure* was going nowhere:[10]

> *I knew that we had to finish* c:cure *after I heard a comment from UKAS. The person told me that they cannot really stop the certification organization issuing BS7799 certificates. So what is the value of* c:cure *which even costs more than a generic certificate? Also, it is rather an absurd idea, on the one hand, we are promoting the internationalization of standard, on the other stand, we are developing a certification that is localized. This does not make sense.*

In 2000, the *c:cure* steering committee decided to discontinue the scheme because of the limited number of *c:cure* auditors licensed, as well as the lack of interest from industry in the scheme. In total, the scheme awarded to companies, at the 1999 InfoSec Conference, only three certificates and retained only ten *c:cure* certified auditors. The 2000 *Information Security Breaches Survey* showed that only 1 percent of organizations surveyed were aware of *c:cure* and, of that 1 percent, only 1 percent was currently certified. A BSI report about the scheme discontinuation noted "confusion between *c:cure* and non *c:cure* certification as well as low market take up" (DTI 2000).

Theme 3: Practicality the Key to Adoption

This theme arises from interpreting the data using the circuit of systemic integration as the main theoretical lens. In so doing we focus on power as circulating through techniques of discipline and production, apparent in the embeddedness of IS security practices in the standard. We found that systemic integration was achieved to the extent that there was a fit between the content of the standard and what practitioners considered to be meaningful IS security practices. This theme also shows the relationship between the circuit of systemic integration and that of social integration, particularly in the rules of production being interpreted as meaningful and valuable by IS security practitioners.

Our data shows that the government would never have accepted and sponsored the eventual standard had it not originated from practitioners, and not been regarded as practical. Furthermore, organizations would have not adopted the standard had it not addressed the concerns of IS security managers. In this sense, the adoption of the initial code of practice as a standard confirms the third theoretical assumption in the sense that systemic integration is crucial for the adoption of innovation. Systemic integration is understood as a fit between the proposed innovation and current working practices. Without that fit, we might argue, the standard could have been spurned. Instead, a constant refrain of "praise for the standard because it is practical and down-to-earth" reverberates throughout our interview data. For instance, the UK Department for Education and Skills told its staff that

> British Standard BS7799 on Information Security is a practical way for many organizations to ensure that their process, policies, security and management of information are as robust as possible (DES 2006, p. 18).

Meanwhile in the same year (2000), a magazine for security managers was also spelling out the practicalities of the standard.

> BS7799 has two main parts: a code of practice for information security management, and a specification for information security management systems. It prescribes a specific process to determine what policies should be in place, how to document them,

[10]The *c:cure* saga is certainly an interesting one for students of how standards and certification schemes can founder unless there is detailed preparation of the social and organizational terrain. The authors hope to make it the subject of a future study.

> and how to develop those that are not specifically identified in the model. When applied to an organization, the result of the BS 7799 standard is a set of custom policies with a process for evaluation, implementation, maintenance and support (Johnston 2000).

The practical benefits lay in providing the information security manager, and the organization, with a ready-made template of policies and processes for developing information security. Against the background of a new awareness of the risks to information assets, having a set of management tools available with the mere purchase of the standard offered a tantalizing prospect for many organizations and managers. Moreover, the standard was designed not only for large corporations, but also for small and medium enterprises (SMEs): the original document included the 10 key controls that could be adopted by SME managers, helping it reach a wider audience. The widely distributed UK paper, *Computer Weekly,* could be found, again, in 2000, trumpeting the ready-to-hand benefits to small companies:

> BS7799, on the other hand, is generally considered more practical and less likely to generate gratuitous paperwork. In its current version, advocates feel that it can be applied realistically by even small companies (Classe 2000).

Systemic integration also explains the failure and aftermath of *c:cure*. Most business organizations considered *c:cure* as an unnecessary disruption to work practices because of the uncertain value of the certificate in relation to the high cost of the audit process to obtain it, especially when compared to the cheaper generic certification.

The diffusion of the standard also required social integration. The social integration of a proposed innovation is achieved when, in the eyes of those who are to adopt it,[11] there is no mismatch between the values and beliefs it embodies and those enshrined in working practices. This explains the problems associated with ITSEC. Many organizations interpreted ITSEC as meeting military and engineering needs, rather than commercial. Consequently, there was a limited take-up of ITSEC in industry. By direct contrast, BS7799 was widely adopted by IS security managers because it originated from other IS security managers, highly respected both within industry and the security profession itself. Hence social integration, in terms of rules of meaning and membership, was achieved by the fact that the standard was promoted by some IS security managers to others of their ilk and was unfailingly practical in nature.

Internationalization

In the international setting, the context of the circuits of power change as the main actors are not IS managers but international and government agencies. As discussed at the end of the next theme, the international institutionalization of the standards is the result of its reputation and the results it achieved in the UK.

In the summer of 1996, BS7799 was submitted to ISO for consideration as an international standard. It met with rejection. The DTI view, in retrospect, was that the submission might have been better handled and more could have been done to familiarize committee members with the benefits of the standard. An additional factor might have been the strong committee representation of two giant IT companies opposed to the British initiative at that time. The head of DTI Information Security Policy Group reflected that

> *The whole process was mismanaged. The document probably should not have been submitted in the first place. It required some updating. In particular, the 1995 document was written in a pre-Internet era.*

To retrieve the situation, the DTI contrived a more targeted approach for steering the standard through ISO. The chairman of the ISMS International User Group Ltd.,[12] together with DTI, participated in, and indeed chaired, a special committee, BDD/2, looking at strategies for the internationalization of BS7799. The head of DTI Information Security Policy Group considered that this involvement again underlined DTI's belief in the quality and importance of this particular standard. He averred that "the DTI rarely chaired standards-related committees or was so actively involved in standards development. This showed how much we believed in its worth."

Apart from polishing the text, the special committee also updated the content to take into account the new risks incurred by the advent of the Internet. After a period of public consultation, the revised version was published as BS7799:1999 in April 1999.

[11]This entails that the meanings assigned to the standards have to agree with the interpretive frames of those adopting the system (Orlikowski and Gash 1994; Silva and Backhouse 2003; Walsham 1993), and if this is not the case, then disciplinary forces are required.

[12]ISMS International User Group Ltd. (IUG) was established in 1997. Although similar to other security groups, this organization offers a community in which members can discuss and share experiences surrounding BS7799.

During this period, major international companies also voiced their support for BS7799 becoming an ISO standard. Companies considered that this transformation would enhance credibility when doing business. As one IS security director in the petroleum sector told us,

> *We were very supportive of DTI pushing BS7799 to become an ISO. When the standard only existed as BS7799, we suffered a lot of resistance from non-UK companies. Those companies considered this standard as British. For instance, American companies felt that they should use ANSI when talking about security requirements in the contract.*

In October 1999, BS7799:1999 part 1 was proposed as an ISO standard through the fast track scheme,[13] becoming ISO/IEC17799:2000 on December 1, 2000.

Between 1998 and 2000, a host of countries took up the British standard, adopting it as their own, including Brazil, Finland, Iceland, Ireland, Norway, the Netherlands, Sweden, Australia, New Zealand, and South Africa. The international interest in the standard had begun as early as 1994, when *Computer Security & Audit Magazine* reported that

> Even before the official publication day, a number of companies had pledged their support for the code Interest has been international, with enquiries coming from as far afield as Australia. (Jones 1994, p. 11)

Concerning the uptake of BS7799 by other nations, the head of DTI Information Security Policy Group told us that "DTI certainly had no program of persuading countries of its value." The interest from abroad was achieved through presentations and discussions at international security events, as well as "through the work of enthusiasts in their own countries." Even where some countries did not adopt it as a national standard, their interest in BS7799 was nevertheless displayed by translating the BS7799 content into the local language, such as Japanese, German, and Chinese. Indeed, to date the IUG has 16 local chapters established in Europe, North America, and Asia.[14]

The publication of the UK 1998 Data Protection Act, requiring organizations to safeguard adequately both manual and computerized information, brought BS7799 into play as a way of meeting the statutory requirements. In terms of public recognition, the results of the 1998, 2000, and 2002 *Information Security Breaches Surveys* revealed much greater industry awareness of the Data Protection Act than of BS7799. DTI also published news releases about the usefulness of BS7799 for compliance with the act. As one IT security consultant commented,

> *The Data Protection Act requires firms to notify the information commissioners if they are handling personal information when not for the purpose of accounts, staff administration, and advertising. Failure to notify is a criminal offence. Firms need to fill in a notification form and one question in the form asks whether the company implements security in compliance with BS7799. Not all my clients know about BS7799 and it was the opportunity to raise the issue.*

Furthermore, ISO/IEC 17799 emerged as a valuable instrument for dealing with the security management aspects of outsourcing. In 2003, IUG rolled out a business game, in which participants discussed the relevance of ISO/IEC 17799 in the context of outsourcing management. Two interviewees from the retailing and petroleum sectors commented on the importance of ISO/IEC 17799 and certification in this context. A senior security manager from the retailing sector informed us, "My company also offshores a lot of its application systems. We use BS7799 as the basis for measuring and auditing the security management of our contractors."

Likewise, a security director from the petroleum sector commented on the impact of outsourcing and the usefulness of BS7799 and ISO/IEC 17799 in different industries.[15]

> *The impact of BS7799 on the financial industry was not as great as it had been for other sectors in the early 1990s. The finance sector already had a banking association taking control of the standardization of financial systems. BS7799 was not really enough to cover requirements for some financial systems, such as payment system control. Nevertheless, as the financial industry started to outsource more, the usefulness of ISO 17799 became more significant. The standard played an important role*

[13]There are two ways of developing ISO standards: fast track or normal process. Fast track is tailored for a well-established national standard to become an ISO without much change required. Once the document is submitted, representatives in the relevant committee either vote in favor or against. The normal procedure, however, requires the nation to submit the standard as a working item to the relevant committee for further refinement and development. This process is much slower.

[14]For additional information on the IUG, see http://www.xisec.com.

[15]The interviewee was in charge of IS security in a large UK bank until the late 1990s when he moved to the petroleum sector.

> *in helping companies express the security requirement in outsourcing agreement.*

In the oil sector, however, the reception for the standard was rather different.

> *The value of BS7799 has been much greater in the oil sector right from the beginning, since by their nature, companies in this sector have a lot of outsourcing activities as well as joint venture partnerships. When we decided to outsource lots of operations to India, there was a big increase in Indian companies taking up BS7799 certification. Also, after the British standard became an ISO, my company has more legitimacy by having ISO17799, in contrast to BS7799, in the contractual agreement.*

On November 14, 2005, BS7799 Part 2 was updated and released as the international standard ISO/IEC 27001:2005. The 2002 *Information Security Breaches Survey* concluded from over 1,000 telephone interviews that 42 percent of large and 27 percent of medium-sized companies were aware of the BS7799 content. A separate web site poll associated with the survey also revealed that 69 percent of respondents were aware of BS7799 content.[16]

Theme 4: Standard as an OPP

The standard did not become an OPP for all British organizations. However, there were clear efforts in that direction, especially in relation to the certification schemes. As we saw, one scheme failed because it was expensive and the certification was regarded as meaningless. Indeed, our interviewees assured us that this debacle tangibly slowed the diffusion of the standard. Nevertheless, in the context of the Data Protection Act, BS7799 became an OPP insofar as companies needed to notify the information commissioner about the use of personal data. The notification form requires the firm to demonstrate security management compliant with BS7799. In this case, BS7799 serves as an OPP for fulfilling the legal obligations of data protection in bilateral relations.

The standard became an OPP in bilateral power relations. Our findings show that the standard only becomes an OPP in power relations in which *A* asks *B* to adopt the standard if *B* wants to do business with *A*. This occurs particularly in outsourcing situations where it serves as the security template for the contract signed between the two parties. In other words, *A* would not hire *B* unless *B* were contractually bound to comply with the standard. The OPP is defined through the circuits of social and systemic integration that were fixed by the power moves of the different actors involved in the process of creation and diffusion of the standard. Systemic and social integration were achieved because the practices contained in the standard (episodic circuit) were considered valuable and meaningful by IS security professionals and because of legislation supporting its adoption. Likewise, the standard itself became a source of power, given that its adoption brought an aura of trust and confidence to the adopting organization (social integration) because it was associated with sound IS security practices (systemic integration). Thus, the standard became the result or outcome of power, but at the same time turned into a source of power once it was fixed into the circuits of power of IS security (see Figure 1).

This theme relates to two of our initial theoretical assumptions, the first on exogenous contingencies, and the fourth on episodic power and OPPs. Institutional theorists (DiMaggio and Powell 1991; Meyer and Rowan 1991; Scott 1995) indicate that changes in an organizational field can be the result of mimetic, coercive, and normative forces. Coercive forces are irrelevant in our analysis given that at the time there were no laws, as such, in the UK obliging organizations to adopt the standard. Nevertheless, our data shows how regulatory forces can explain the adoption of the standard. For example, a former IS security manager of a large UK bank told us that although there was no requirement for the bank to adopt the standard, it would do so in order *"to demonstrate good internal control and management. Having BS7799 in place made a big difference in these discussions."*

However, the adoption of the standard in the UK and its subsequent internationalization can be explained in terms of mimetic forces. Although the first adopters of the standards were major corporations in the UK, smaller organizations that did business with them also adopted the standard in their wake. In many cases, because these smaller organizations were part of the same supply chain of goods and services, they were obliged willy-nilly to match security levels. This logic also applied at the international level: the success of the standard in the UK was one of the reasons why ISO decided to promote BS7799 to an international standard, a decision reinforced by the fact that many countries were already adopting BS7799 as their national standard. These countries preferred to adopt a proven IS security standard rather than develop one of their own from scratch.

The mimetic forces that influenced the adoption of the standard internationally are illustrated in the examples of Japan

[16]The question asked about BS7799 was modified from one survey to the next, hence, in addition to sample difference, there are no consistent results about BS7799 awareness level. The 2002 survey is available at http://www.pwc.com/images/gx/eng/about/svcs/grms/2002Detailedreport.pdf).

and in its diffusion in Europe. Japan, for example, established a dedicated division within a government agency (JIPDEC)[17] specifically for the purposes of promoting and encouraging Japanese organizations to adopt and be certified against recognized information security standards pertaining to information security (i.e., based on ISO/IEC 17799 and BS 7799-2). The results of this institutionalization can be seen in the numbers of certifications against the standards registered on the ISMS web site.[18] As of September 19, 2005, the number of certificates in Japan had reached 1,023, compared with just 215 from the UK, the country with the next largest number. In Europe, once the standard was confirmed, the social networks and organizations of the expanding information security profession, such as those mentioned earlier, like the European (now Information) Security Forum[19] and I-4, the International Information Integrity Institute,[20] featured it regularly as part of the material for their members to use in managing information security risks. This theme, therefore, suggests that our understanding of the adoption of standards is enriched when, by means of the circuits framework, we apply the lens of institutional theory.

Contributions

Table 3 contains a summary of the main theoretical contributions of the paper, presented in the form of analytical generalizations that stem from the data and are synthesized in the form of themes and expanded in the third column of the table. We chose to interweave the themes with the narrative so the relationships between data, findings, and theory becomes more evident. In this section, we present a summary/synopsis of the main contributions of our study.

Concentrating on the power and resistance aspects of the development of a standard naturally brings into sharper focus the impact that each new event and external stimulus has on the whole process. The study reconfirms our earlier criticism of an approach based on economics. The paper also contributes to the all-too-frequently overlooked area of research on standardization (Cargill 1989, p. 7). Cargill suggests that the existing literature provides a descriptive picture of the standardization process, but omits the more interesting concepts involving the human, social, or economic dimension. Here we have demonstrated how these elements interplay and influence the development of standards. What began just as an immediate response of a small group of security managers to their immediate needs transformed speedily into a standard of international acclaim.

The circuits framework offers an explanation of how standards setting works in practice through episodic power circuits that trigger social and systemic integration in which alliances and social relationships are formed and reshaped. The realignment of power relationships itself generates new systems of production and discipline embodied in the new OPP. In effect standards setting can be understood as simply another important arena of political action, albeit vital for the well-being of IS development. Standards developers can use this study and the framework to support their efforts in achieving standards. The framework allows standards setters to identify the power relations that bind the key actors and events and to discern the obligatory passage points that will be vital for obtaining success. The study underlines the part played by alliances and legitimacy in obtaining sufficient support for an emerging standard. Adopting the framework of power and politics as a lens through which to interpret the context of standards development equips the protagonists with an important tool to guide their evolving strategy. The study also demonstrates convincingly that the circuits can cope with the full complexity of a typical international standards context, offering a coherent account of unfolding events and shifts in alliances. Using the lens of the circuits framework, this paper explained how this occurred for BS7799. What emerges in this study is how, although the agents concerned adhere to no overall governance structure, except perhaps when they operate within their own particular jurisdiction, their actions and the responses to those actions can be interpreted and made sense of within an overarching framework of political action.

The paper contributes to the literature on reference standards. In contrast to the economic explanations, it offers an account of the role of political action. It examines the effects of the social relationships among the actors and the power of those relationships for the way that the relevant actors make their key decisions. The publication of a d*e jure* standard first requires members to reach a consensus on a set of requirements. During this process, the motivation does not always arise from the economic or strategic incentives, but rather from the influences of exogenous contingencies and the effects of powers. As shown, this case study presents highly pertinent evidence about how key actors form and reshape alliances within the circuits framework and generate important new disciplines and OPPs.

[17]http://www.isms.jipdec.jp/en/.

[18]http://www.xisec.com/register.htm.

[19]http://www.isfsecuritystandard.com/index_ns.htm.

[20]https://i4online.com//.

Table 3. Summary of Findings and Their Relation to Data and Theory

Assumption Regarding Standards (Derived from the Circuits of Power)	Themes	Findings
This relates to the group proposing the standards (A) and those (B) who have to accept them (Episodic Circuit).	**Theme 4: Standards as Obligatory Passage Points** • These relationships are manifested only when the *de jure* standard has become institutionalized	The formation of *de jure* standards may not display episodic power (A making B do something B would otherwise not do). This is because *de jure* standards are generated initially in a cooperative manner. Relations of episodic power are manifested once the standard has been institutionalized.
The authors of the standards have to be recognized by their organizational field as legitimate and also should be able to relate to those organizational members in power positions such that the standards are accepted (Circuit of Social Integration).	**Theme 2: Key Role of Legitimacy, Position, and Alliances** • The creation of the standard required the alliance between government and industry **Theme 3: Practicality the Key to Adoption** • Neither government nor industry would have promoted or adopted the standard without it being regarded as practical	On the one hand, the active participation of industry in the formation of the standard brings legitimacy and credibility that could have not been brought about exclusively by government. Government, on the other hand, facilitates resources for publication, channels of distribution and acts as legitimate authority for converting the standard into a national standard. The diffusion and adoption of the standard requires it to be regarded as practical and down-to-earth.
Power is inscribed in the standards through the practices that have to be adopted (Systemic Integration). *Once institutionalized, the standards also become a source of power on their own (Systemic Integration).*	**Theme 3: Practicality the Key to Adoption** • Government would have not promoted the standard had it not originated in industry and without it being regarded as practical • Organizations would have not adopted the standard if it had not addressed the concerns of IS security managers	In the early stages of formation of a *de jure* standard, the components of the standard have to display systemic integration etween current practices and the content of the standard. Systemic integration (working tasks fit) in this case precedes social integration (rules of meaning and membership).
The idea to generate standards arose from exogenous contingencies.	**Theme 1: Impact of Exogenous Contingencies** • Publication of the DTI Security Breaches Survey • Virus	The motivation for producing an *de jure* IS standard that may require the sharing of information but in which there is an incentive to withhold it ike security standards esembles the prisoners dilemma (see Markus et al. (2006) and Weitzel et al. (2006) in this special issue). Exogenous contingencies impact by breaking the deadlock for the generation of standards; but they have to be meaningful (e.g. a threat) for all stakeholders.
The standard becomes an OPP for managers and organizations insofar as its prescribed practices and policies are considered valuable and interpreted to be technically sound by their peers.	**Theme 4: Standards as Obligatory Passage Points** The adopters of the standard rejected certifications deemed as expensive and meaningless The government through the Data Protection Act notification form required compliance with BS7799 The standard is also an OPP in bilateral relations when an organization (*B*) wants to do business with another (*A*) and the latter establishes compliance with the standard as a prior condition	The institutionalization of the standard is strengthened if compliance is required in other pieces of legislation. Expensive certification is regarded as without value if the standard achieves systemic and social integration. The institutionalization of the standard enables and is reinforced in bilateral relations in which As ask Bs to comply with the standard if the latter want to do business with the former.

Limitations and Areas of Further Research

Here we identify the limitations of our paper and reflect on areas of further research. Limitations of the circuits framework have been previously identified (Silva and Backhouse 2003) as arising from its complexity and interpretive nature. To depict the three circuits and identify the agents and key events, a significant amount of data must be gathered in order to allow the researchers sufficient material to interpret appropriately. There seems little prospect of an abbreviated version and researchers adopting the framework will need to take note. Further, in order to configure fully the circuits, researchers need to gain real familiarity with the social and organizational context, as the power and resistance issues may not be always readily perceptible to the untrained eye. In addition to the requirement for adequate data volumes, the framework itself has issues to be dealt with. Rather than offering a normative template for viewing systems and interactions, which can simplify the task of reconciling the data with the underlying perspective, the framework instead provides a focused set of elements, of chess pieces and rules of the game, that must be interpreted for the context once sufficient knowledge has been elicited. Deploying these elements—the circuits, the OPPs, the exogenous factors—can leave the uninitiated a little bemused at times and this itself constitutes a limitation: the framework is not exactly intuitive. Our use of this framework does not deny the strengths of other perspectives on standards development, for there are clearly many other ways in which the research might have been framed. The standpoint of power was the one selected by the researchers as important and interesting because the aim was to investigate the power and politics contingencies. Economic and social theories help to highlight important factors at work in standards development but focus on different aspects.

Another limitation concerns the scope of the study. Although the application of the circuits framework can be extended to study other types of standards, the scope of the paper concerns *de jure* standards. Thus, an area of further research would be the application of the circuits framework to other types of standards. A further limitation regards the retrospective nature of the investigation. As many events occurred in the early 1990s, we had to rely on our interviewees to piece together the history. To address this limitation, we resorted to documentary sources. This allowed us to double-check factual information. Therefore, an interesting area of research would be to apply the circuits framework to establish whether the theoretical themes and generalization make sense in other contexts (Lee 1989). A remaining limitation centers on the generalizability of our results, as we concentrated on one standard only. This is a common criticism of single case studies. However, in case studies, the generalization of the results should be extrapolated not to populations but to analytical generalizations (Lee and Baskerville 2003) or to bring about insights (Walsham 1995). Indeed, the context of standards setting varies tremendously in the IS and security arena. Many *de facto* standards are set by the Internet community with RFCs (requests for comment), such as RFC 2527 for Certificate Practice Statements, which are in fact merely embryonic standards, at an intermediate stage in the process of finalizing a full *de jure* standard. It would be difficult to generalize to include such diversity of population. In this regard, this paper offers four theoretical themes (Sanders 1982) concerning the development of *de jure* standards.

One of the advantages of studying power through the circuits of power is its integrative nature. The circuits of power framework encompasses different views of power, such as the duality of power (Giddens 1984) expressed in its circular nature, the emphasis on agency as initiators of power relations (Dahl 1957; Parsons 1937), the definition of OPPs (Callon 1986; Latour 1987), as well as the conception that power is exercised beyond agency and operating through discourse and discipline (Foucault 1977). However, a missing perspective is that of a critical theory (Habermas 1972; Lyytinen 1992), that is, the circuits of power are ideal for studying and describing the main strategies and mechanisms of how power operates, yet cannot provide an emancipatory perspective. Thus, an area of further research would be to conduct a critical study of standards that concentrates on the oppressive and emancipatory attributes of standards. This could be done by using the circuits of power to identify the main actors and sources of power and then studying critically those forces.

Conclusion

The study reveals a number of levels of jurisdiction within which the actors operate: the company level where, for instance, an information security chief seeks to draw upon the power of his director to lend authority to his approach to the DTI; the industry level, such as oil or finance, where perhaps outsourcing cries out for common standards; still yet the national and international level, where national standards bodies tussle over which standard will ultimately succeed in becoming an ISO standard. At whatever level power is deployed, researchers need to be able to understand the process that governs it. The circuits of power framework offers one way of making sense of that process in the arena of standards setting.

References

Antonelli, C. "Localized Technological Change and the Evolution of Standards as Economic Institutions," *Information Economics and Policy* (6), 1994, pp. 195-216.

Besen, S., and Farrell, J. "Choosing How to Compete: Strategies and Tactics in Standardization," *The Journal of Economic Perspectives* (8:2), 1994, pp. 117-131.

Bonino, M., and Spring, M. "Standards as Change Agents in the Information Technology," *Computer Standards and Interfaces* (20:4), 1999, pp. 279-289.

Bourdieu, P. *Language and Symbolic Power*, Harvard University Press, Cambridge, MA, 1991.

Cargill, C. F. *Information Technology Standardization: Theory, Process, and Organizations*, Digital Press, Bedford, MA, 1989.

Cargill, C. F. *Open Systems Standardization: A Business Approach,* Prentice Hall, Upper Saddle River, NJ, 1997.

Callon, M. "Some Elements of A Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay," in *Power, Action and Belief*, J. Law (ed.), Routledge & Kegan Paul, London, 1986, pp. 196-233.

Classe, A. "Security: Rallying to the Standard," *Computer Weekly.com*, Technology Security Products, April 6, 2000 (available online at http://www.computerweekly.com/Articles/2000/04/06/175429/SecurityRallyingtothestandard.htm).

Clegg, S. R. *Frameworks of Power*, Sage Publications, London, 1989.

David, P., and Foray, D. " Percolation Structures, Markov Random Fields and the Economics of EDI Standards Diffusion," in *Global Telecommunication Strategies and Technological Changes*, G. Pogorel (Ed.), Elsevier, Amsterdam, 1994

David, P., and Greenstein, S. "The Economics of Compatibility Standards: An Introduction to Recent Research," *Economics of Innovation and New Technology* (1), 1990, pp. 3-41.

David, P., and Steinmueller, W. "Economics of Compatibility Standards and Competition in Telecommunication Networks," *Information Economics and Policy* (6:3/4), 1994, pp. 217-241

Dahl, R. "The Concept of Power," *Behavioral Science* (2), 1957, pp. 201-105.

DES. "Managing Information Across Partners: Data Sharing Framework," Version 1.1, Department for Education and Skills, London,March 2006 (available online at www.dfes.gov.uk/learning&skills/docs/MIAP%20Data%20Sharing%20Framework%20FINAL.doc).

DiMaggio, P. J., and Powell, W. W. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields," in *The New Institutionalism in Organizational Analysis*, W. W. Powell and P. J. DiMaggio (eds.), The University of Chicago Press, London, 1991, pp. 63-82.

DTI. "Review and Examination of the Process of Infrastructure for c:cure Certification: Report for Consideration by the c:cure Steering Committee, Version 6.0," Department of Trade and Industry, February 2000 (http://www.dti.gov.uk/index.html).

Eisenhardt, K. M. "Building Theories from Case Study Research," *Academy of Management Review* (14:4), 1989, pp. 532-550.

Farrell, J., and Saloner, G. "Installed Base and Compatibility: Innovation, Product Preannouncements, and Predation," *American Economic Review* (76), 1986, pp. 940-955.

Foray, D. "Users, Standards and the Economics of Coalitions and Committees," *Information Economics and Policy* (6:3/4), 1994, pp. 269-293.

Fomin, V., and Keil, T. "Standardization: Bridging the Gap between Economic and Social Theory," in *Proceedings of the 21st International Conference on Information Systems*, W. J. Orlikowski, S. Ang, P. Weill, H. C. Krcmar, and J. I. DeGross (eds.), Brisbane, Australia, 2000, pp. 206-217.

Foucault, M. *Discipline and Punish*, Vintage Books, New York, 1977.

Foucault, M. *Power/Knowledge: Selected Interviews and Other Writings 1972-77*, Harvester Press, Brighton, UK, 1980.

Frenkel, K. "The Politics of Standards and the EC," *Communications of the ACM* (33:7), 1990, pp. 40-51.

Gersick, C. J. G. "Revolutionary Change Theories: A Multilevel Exploration of the Punctuated Equilibrium Paradigm," *Academy of Management Review* (16:1), 1991, pp. 10-36.

Giddens, A. *The Constitution of Society*, Polity Press, Cambridge, UK, 1984.

Greenwood, R., and Hinings, C. R. "Understanding Radical Organizational Change: Brining Together the Old and the New Institutionalism," *Academy of Management Review* (21:4), 1996, pp. 1022-1054.

Habermas, J. *Knowledge and Human Interests*, Beacon Press, Boston, 1972

Hanseth, O., and Braa, K. "Hunting for the Treasure at the End of the Rainbow. Standardisation Corporate IT Infrastructure.," *Computer Supported Cooperative Work* (10:3/4), 2001, pp. 261-292.

Hanseth, O., and Monteiro, E. "Inscribing Behaviour in Information Infrastructure Standards," *Accounting, Management & Information Technology* (7:4), 1997, pp. 183-211.

Hanseth, O., Monteiro, E., and Hatling, M. "Developing Information Infrastructure: The Tension between Standardisation and Flexibility," *Science, Technology and Human Values* (21:4), 1996, pp. 407-426.

Hinings, C. R., Hickson, D. J., Pennings, J. M., and Schneck, R. E. "Structural Conditions of Intra-Organizational Power," *Administrative Science Quarterly* (9:1), 1974, pp. 22-44.

Jakobs, K. *Information Technology Standards and Standardization: A Global Perspective*, Idea Group Publishing, Hershey, PA, 2000.

Johnston, R. E. "86ing BS 7799: Why Is It So Hard for Us to Agree on a Universal Standard for Infosecurity Policies?," *Information Security*, June 2000 (available online at http://infosecuritymag.techtarget.com/articles/june00/columns4_logoff.shtml).

Jones, M. "A Better Way to Manage Your Information Security," *Computer Security & Audit Magazine* (5), March/April 1994, pp. 10-12.

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

Latour, B. *Science in Action*, Harvard University Press, Cambridge, MA, 1987.

Lee, A. S. "A Scientific Methodology for MIS Case Studies," *MIS Quarterly* (13:1), 1989, pp. 33-50.

Lee, A. S., and Baskerville, R. L. "Generalizing Generalizability in Information Systems Research," *Information Systems Research* (14:3), 2003, pp. 221-243.

Lockwood, D. "Social Integration and System Integration," in *Explorations in Social Change*, G. K. Zollschan and W. Hirsch (ed.), Routledge & Kegan Paul, London, 1964, pp. 244-257.

Lukes, S. *Power: A Radical View*, The Macmillan Press Ltd., London, 1974.

Lyytinen, K. "Information Systems and Critical Theory," in *Critical Management Studies*, M. Alvesson and H. Willmott (eds.), Sage Publications, London, 1992, pp. 158-169.

Manninen, A. T. *Elaboration of NMT and GSM Standards: From Idea to Market*, unpublished Academic Dissertation, University of Jyväskyalä, 2002.

Markus, M. L., Steinfield, C. W., Wigand, R. T., and Minton, G. "Industry-Wide Information Systems Standardization as Collective Action: The Case of the U.S. Residential Mortgage Industry," *MIS Quarterly* (30:Special Issue on Standard Making), August 2006, pp. 439-465.

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

Monteiro, E. "Scaling Information Infrastructure: The Case of the Next Generation IP in Internet," *The Information Society* (14:3), 1998, pp. 229-245.

Monteiro, E., and Hanseth, O. "Social Shaping of Information Infrastructure: On Being Specific about the Technology," in *Information Technology and Changes in Organisational Work*, W. J. Orlikowski, G. Walsham, M. Jones, and J. I. DeGross (eds.), Chapman & Hall, London, 1995, pp. 325-343.

NCC. *Security Breaches Survey*, National Computing Centre, Manchester, UK, 1992.

Orlikowski, W. J., and Gash, D. C. "Technological Frames: Making Sense of Information Technology in Organizations," *ACM Transactions on Information Systems* (12:2), 1994, pp. 174-207.

Parsons, T. *Sociological Theory and Modern Society*, Free Press, New York, 1967.

Peleg, B., and Lee, H. "Impacts of Standardization on Business-to-Business Collaboration," in *Electronic Commerce and the Digital Economy*, M. Shaw (ed.), M. E. Sharpe, Armonk, NY, 2005.

Pfeffer, J. *Managing with Power*, Harvard Business School Press, Boston, MA. 1992.

Pfeffer, J. *Power in Organizations*, Pitman, Marshfield, MA, 1981.

Sanders, P. "Phenomenology: A New Way of Viewing Organizational Research," *Academy of Management Review* (7:3), 1982, pp. 353-360.

Scott, W. R. *Institutions and Organizations*, Sage Publications, London, 1995.

Shapiro, C., and Varian, H. *Information Rules: A Strategic Guide to the Network Economy*, Harvard Business School Press, Boston, 1999.

Silva, L., and Backhouse, J. "The Circuits-of-Power Framework for Studying Power in Institutionalization of Information Systems," *Journal of the Association for Information Systems* (4:6), 2003, pp. 294-336.

Swann, P., and Shurmer, M. "The Emergence of Standards in PC Software: Who Would Benefit from Institutional Intervention?" *Information Economics and Policy* (6:3/4), 1994, pp. 295-318

Swann, P., Temple, P., and Shurmer, M. "Standards and Trade Performance: the UK Experience," *The Economic Journal* (106:438), 1996, pp. 1297-1313.

Townley, B. "Foucault, Power/Knowledge, and its Relevance for Human Resource Management," *Academy of Management Review* (18:3), 1993, pp. 518-545.

Von Solms, R. "Information Security Management: Why Standards Are Important," *Information Management and Computer Security* (7:1), 1999, pp. 50-57.

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

Walsham, G. "Interpretive Case Studies in IS Research: Nature and Method," *European Journal of Information Systems* (4:2), 1995, pp. 74-81.

Weber, M. "The Three Types of Legitimate Domination," in *Essays in Economic Sociology*, R. Swedberg (ed.), Princeton University Press, Princeton, NJ, 1999, pp. 99-108.

Weitzel, T., Beimborn, D., and Köning, W. "A Unified Economic Model of Standard Diffusion: The Impact of Standarization Cost, Network Effects, and Network Typology," *MIS Quarterly* (30: Special Issue on Standard Making), August 2006, pp. 489-514.

Yin, R. K. *Case Study Research: Design and Methods*, Sage Publications, London, 1994.

About the Authors

James Backhouse is a senior lecturer in the Department of Information Systems at the London School of Economics. His research centers on social science perspectives on information security. In 2004, he was a policy adviser to the UK government's Foresight CyberTrust and Crime Protection Project. He is a founding member and board member of FIDIS (Future of Identity in the Information Society), a European Union Research Network of Excellence. His work has been published in journals such as the *Journal of the Association for Information Systems, Information Systems Journal*, *European Journal of Information Systems,* and *Communications of ACM*.

Carol Hsu is an assistant professor in the Department of Management Information System at National Chengchi University, Taiwan. Prior to her appointment at Chengchi University, she was a tutorial fellow in the Department of Information Systems at the London School of Economics and Political Science, where she also received her Ph.D. in information systems. Her current research focuses on the organizational and cultural issues concerning security policy and technology implementation. Her work has been published in *Communications of the ACM* and *Journal of Information Systems Education*.

Leiser Silva is an assistant professor in the Decision and Information Sciences Department at the C. T. Bauer College of Business, University of Houston. He holds a Ph.D. in information systems from the London School of Economics and Political Science. His current research examines issues of power and politics in the adoption and implementation of information systems. In addition, he is looking at managerial aspects of information systems, specifically, contextual and institutional factors. His work has been published in journals such as *Journal of the Association for Information Systems, Communications of the Association for Information Systems, European Journal of Information Systems, The Information Society*, and *Information Technology and People*.

Appendix A

Interviewees and Documents

Position	Role	Interview method
Security director in petroleum sector	supporter of the original initiative	Face-to-face interview, e-mail
Senior security manager in retailing sector	original contributor to the document	Face-to-face interview
Head of security management in banking sector	original contributor to the document	Face-to-face interview, e-mail
IT security consultant 1	involved in the first U.K. IT awareness program	Telephone interview
Senior security analyst in petroleum sector	current generation of security managers	E-mail and telephone interview
BSI business program manager	*c:cure* certification program	Face-to-face interview
DTI representative	set up the industry group and acted as coordinator for the development	Face-to-face interview
Head of security management in petroleum sector	original contributor to the document	Face-to-face interview, e-mail
IT security consultant 2	involvement in DTI second and third Information Security Breach Surveys	Face-to-face interview, telephone follow-up, e-mail
Head of DTI security policy group	internationalization of BS7799 and certification program	Face-to-face interview, e-mail
Head of security management in banking sector	current generation of security managers	E-mail

Documents	Websites
Minutes of the first meeting held at DTI premises in 13 January 1993	Department of Trade and Industry
Three photos of DISC launch at Shell Centre in September 1993	International Standardisation Organization
DTI and BSI press release between October 1993 and May 1994	British Standard Institute
Newspaper reports in 1994	UK Information Commissioner's Office
Internal company news February 1994	ISMS International User Group
DISC PD003 *A Code of Practice for Information Security Management* 1993	
BS7799:1999 Part 1 and Part 2 *Information Security Management*	
OECD *The Guidelines for the Security of Information Systems* 1992	
UK Data Protection Act 1998	
DTI Information Security Breach Survey 1998, 2000, 2002	
DTI 7799 *Go Global* Conference Opening Speech 2000	

Appendix B

Chronology by Themes

Year	Key Actors	Event
1989-early 1993 Initiative formation	DTI Private industry working group	• In 1989, DTI found that there was a disconnection between the institutional standards and the needs of the industry. This was also highlighted in one of 1989 SEMA survey on the need of standards. • Department of Trade and Industry's (DTI) Commercial Computer Security Centre (CCSC) had tasks to establish a set of security criteria for products and good security practice. The security product criteria ITSEC were published in 1990. • OECD published the Guidelines for the Security of Information Systems • Meeting was held between MJ and SJ about operationalizing the initiative. • The publication of first DTI computer security breach survey. • **In January 1993, DTI established a private group of industry consortium, consisting of Shell International Petroleum, Shell UK Ltd, Midland, the BOC Group, Marks and Spencer, British Telecommunication, and Uniliver. The participation was on a volunteer basis.**
1993 (6 months) Development of draft	DTI Private industry working group CCTA CCSC	• There was a sense of urgency among the group to draft this document quickly. • The group was driven by the thinking of developing standards by the industry and for the industry. • There was no financial support from DTI, it only provided the support by offering meeting venue and facilities as well as helped maintaining the master document. • Each participant brought along their individual security management documents. These would form the table of the content as well the checklist for completeness. • The group agreed on the division of the labor. Each participant was responsible for a particular section. Having completed the writing, the document was then circulated among the group for further discussion and amendment. • There was a pressure from CCSC to incorporate ITSEC as a part of the document. But the group considered that ITSEC was not practical. The team diplomatically sidelined the protest from CCSC and managed to keep the BS7799 practical. • CCTA was not always supportive, since there was an agenda of developing another security management standard, which would center on the concept of CRAMM. • The whole development took 6 months. In 3 months, the first draft was produced. The final draft was completed in another 3 months. It was a record in terms of turnaround time.
1993 Publication as A Code of Practice	DTI Private industry working group BSI NCC	• Having completing the draft, the group discussed the issue of publication. There was a debate over the copyright issue, i.e., whether to make it freely available or to copyright the document with some minimum charge for usage. • In order to get this document out as soon as possible, it was decided to publish as A Code of Practice rather than British Standard. This is to avoid the certain audit process, strict presentation and the required public consultation period. • The group also fought a successful battle against BSI DISC unit on the presentation and language style of the document. • The launch took place in Shell Business Centre in September 1993. • The document was first published as *A Code of Practice for Information Security Management* (Vol. DISC PD003, British Standard Institution, London, 1993).

Year	Key Actors	Event
1994-1995 **Promotion and Publication as BS7799**	DTI Private industry working group ISMS IUG NCC External IT Consultants	• Marketing techniques such as press release, minister public speech and radio broadcast were deployed. • Both Shell, and Marks and Spencer bought nearly 5,000 copies of DISC for internal and external company use. • The industry consortium was not directly involved at this stage. Some members gave talks in various business conferences. • The document became very popular because it was the right document published at the right time. It was also suitable for SMEs. • Not all people in the consortium stayed on to help the process of standardization. • BS7799 gained support from major large-size companies as the way to ensure the security standards of its own system, suppliers and business partners. • The industry praised the practicality of the document. • The second DTI computer security breach survey was published. • **After a period of public consultation, this document became BS7799:1995. There was not much difference between BS7799 and the original draft.**
1996-1999 Internationalization of BS7799 and Certification	DTI ISMS IUG External IT Consultants	• In the summer of 1996, BS7799 was submitted for the consideration of becoming international standard, but was rejected. • Chief security officer of a large corporation gave a talk at ISO about the value of BS7799. • After BS7799:1995 was published, some consultancy and accounting firms started to get interested in the idea of certification. • ISMS International User Group was established in 1997 to promote internationalization of BS7799. • In September 1997, the DTI set up the BS7799 Accredited Certification Steering Committee. • In April 1998, a UK minister launched *c:cure* certification scheme for BS7799. • UK Data Protection Act was enacted in 1998. • Australia and New Zealand adopted the standard and published it as AS/NZS4444. • BS7799:1995 was revised in preparation for becoming an ISO. • **BS7799 part 2 was added on February 1998 and the first revision of BS7799:1999 was published in April 1999.**
2000 ISO17799	DTI ISMS IUG Security managers	• BS7799:1999 part 1 was proposed as an ISO standard through ast Track scheme in October 1999. • In 2000, BSI and DTI decided to discontinue the *c:cure* scheme due to the low uptake of *c:cure.* • DTI and ISMS IUG started to lobby BS 77799 at the international level. • Strong support was given by the Scandinavian and Far East countries. • Large companies started to use IBS7799 to ensure their supplier and outsourcing contractors having a good security management in place. Industry sectors include petroleum, banking and telecommunication. • The number of BS7799 certificates issued is growing steadily. • BS7799 certification started to be accepted by companies in major economies such as U.S, Japan, and Germany. • **BS7799:1999 part 1 became ISO/IEC17799:2000 on December 1, 2000.**

Appendix C

Data and Theory Tables

Source	Data	Interpretation
Exogenous Contingencies		
Original contributors of DISC	Marks and Spencer's network suffered from virus attack coming from one of its suppliers. The company urged DTI to act on the need for security management standards. The work on security management standards was then initiated.	The arrival of this virus triggered a sea change in attitudes. The security chief quickly realized that the future of the company could be harmed, given its dependence on a networked system which included a vast number of smaller suppliers.
DTI Representative	In 1989, DTI found that there was a disconnection between the institutional standards and the needs of the industry. This was also highlighted in one of 1989 SEMA survey on the need of standards.	This DTI discovery altered the state of play and prepared the ground for what became the BS7799 initiative. It prepared the ground at the DTI for their willingness to support the later initiative.
Security director at the petroleum sector (who was working in banking sector in the early 1990s)	The reason that Barclays was supporting the development but not directly involved could be explained from the issue of outsourcing. At that point of time, the banking industry was not heavily engaged in outsourcing activities compared with other industry sectors such as oil (Shell) and manufacture sector. Nevertheless, as the financial industry started to outsource more, the usefulness of BS7799 became more significant. The standard played an important role in helping companies expressed the security requirement in outsourcing agreement.	Growth of the phenomenon of outsourcing and now offshoring were exogenous factors that militated in favor of the adoption of the standard.
Episodic Power		
Source	**Data**	**Interpretation**
Meeting minutes in 13 January 1993	There was no financial support from DTI; it only provided the support by offering meeting venue and facilities.	The DTI was interested in the initiative but kept its support fairly informal until outcomes were clearer.
Original contributors of DISC	CCTA was not always supportive, since there was an agenda of developing another security management standard, which would center on the concept of CRAMM.	CCTA had its own agenda and hankered after developing a standard around its own methodology for dealing with risk in IS. CRAMM was at that time a cumbersome and expensive risk analysis method that suited bureaucracy but not business.
Security director at the petroleum sector (who was working in banking sector in the early 1990s)	However, before BS7799 became an ISO, we suffered a lot of resistance from U.S. companies. Those companies considered this standard as British, and felt that they should use ANSI when talking about security requirements in the contract. This is why BP was very supportive of DTI pushing BS7799 becoming an ISO. After becoming an ISO, BP has more legitimacy of having ISO17799, rather ANSI, in the contractual agreement.	Acquiring the status of an international standard lent enormous credibility to the British Standard. Such is the power of the standards body behind ISO 17799.

Source	Data	Interpretation
Security director at the petroleum sector (who was working in banking sector in the early 1990s)	BS7799 certification is also useful. BP uses this as a method to ensure security obligations of its partners. When BP decided to outsource lots of operations to India, there was a big increase in Indian companies taking up BS7799 certification.	We can see how the power of BP as an international enterprise brought its own pressure on foreign suppliers and offshorers to comply with the British Standard.
The head of Information Security Policy group at DTI	On the first day of my job in 1998, I was in the c:cure committee meeting. I knew that c:cure is dead in the water after hearing one comment from one of UKAS people. I was told that "we [UKAS] can not really stop certification organizations issuing certificates to companies compliant with BS7799." Thus, there was really no point for c:cure. Imagine a company talking to certification organizations about getting BS7799 certificates, understandably the question would be asked about the difference between the normal certification and c:cure certification.	c:cure was the second way in which certification against the standard was available. The way in which the scheme was set up meant that it could never compete against the cheaper, generic certification, always on offer. It represents a failure in episodic power for it did not lead to an OPP.
The head of Information Security Policy at DTI	The problem and confusion about certification and c:cure certainly have some impacts on BS7799 uptake. But with the publication of ISO, the certification is certainly picking up again.	The negative impact on the uptake is contrasted with the positive impact of succeeding in the attempt to create an ISO standard, which results in an OPP for industries demonstrating their adherence to secure standards.
The IT security consultant	During that period, DTI was hoping that the peer-pressure of going for certification would generate the number of uptake. However, this did not happen. The main reason was that there was too much confusion and frustration with the process. Remember, apart from c:cure, there was also a route for general certification. How complicated can things become	This corroborating quote explicitly pinpoints the issue of peer-pressure, which creates the obligation to perform in a specified manner.
Social Integration		
Source	**Data**	**Interpretation**
Original contributors	DTI Commercial Computer Security Centre (CCC) was tasked to establish a set of security criteria for products and good security practice. The security product criteria ITSEC were published in 1990.	This refers to the role of DTI in the process. Its tasks refers to the meaning of its role and responsibility, prior to creation of standard—and afterward.
Original contributors	There was pressure from CCSC to incorporate ITSEC as a part of the document. But the group considered that ITSEC was not sufficiently practical. The team diplomatically sidelined the protest from CCSC and managed to keep the BS7799 practical.	This represented a power play from one of the many agents with a role in the informal process. Overall the volunteer group managed to deflect the power play by means of a simple reference to ITSEC, without naming it specifically. This strengthened the group and embedded the roles and membership.
Original contributors	There was a debate over the copyright issue, i.e., whether to make it freely available or to copyright the document with some minimum charge for usage. Some for copyright argued that the copyright would prevent the materials being developed into numerous unauthentic versions, which later would cause problems as well as damaging the ides of having this document as one common standard. It was the issue matter of control.	An attempt to use the power of the legal control over how the standard was to be published to ensure the shape of its future development. This control would lead to systems integrative power inscribed into the standard. Complying companies would be faced with addressing the standard as designed by the group.

Source	Data	Interpretation
The IT security consultant	It was also interesting to see how the idea of security changed over time. The first survey was named computer security surveys, the second was called IT security breach surveys, and the one published in 1996 was renamed as information security breach survey. The idea to rename the survey in 1996 was in line with the publication of BS7799 that centered on good security management practice in late 1995.	Here we see how the DTI and the groups it worked with in the early to mid-90s gradually altered the titles of the breaches survey in line with the developing focus on management of information security in general rather than simply technical matters. This attention to the meanings is seen as part of the Social Integration circuit. Changes in the sponsorship of each survey, from technical to management consultancy (PWC), confirm this interpretation .
The DTI representative	In order to show the value of DISC document, before the launch, DTI also sent copies to big companies and asked them whether they would endorse this document. By endorsement, it meant that the company would seriously consider use DISC as the base of security management in the organization. DTI had 15 companies replied and the list of companies were shown in the event to boost the value of DISC.	While the government would eventually mandate the standard for its departments, it could only rely on informal pressure and moral suasion to induce private enterprise to take up the (at this point) Code of Practice. But the fact of 15 prominent companies agreeing to endorse it created considerable forward momentum for the standard.
The DTI representative	The development of the DISC had a agic mix of right people from different sectors. These people were very senior management and showed a lot of commitment as well as passion during this process. This idea started with a lot of networking and informal discussion with people in these international committees.	The importance of the informal nature of the volunteer group that wrote the original document should not be underestimated. Without this "magic mix" it would have been difficult to generate the success that was eventually obtained.
Security director at the petroleum sector (who was working in banking sector in the early 1990s	It (BS7799) provides the common language for companies to discuss, compare or demonstrate their security practices.	Social integration relies on a common language – the new standard created this language.
Senior security manager at retailing sector	BS7799 really changed the whole security industry and it changed how people think of security. It enabled security management to be recognized as a discipline and helped to create a new generation of security managers. Nowadays, BS7799 is the basic knowledge for security managers. If I meet someone who is in the security industry and not aware of BS7799, I would probably be surprised and will not really talk to that person about security management.	More than creating just the language more than one respondent asserted that the standard had helped to create the security management profession – at least in the UK.
Systemic Integration		
Source	**Data**	**Interpretation**
The head of IS security policy group at DTI	BS7799 certainly had a big impact within the government sector. All government departments are required to comply with BS7799.	Government was able to mandate compliance throughout the public sector, thus exerting technical discipline.
he IT security consultant	The push for becoming IS0 17799 was also helped by the fact that many countries started to adopt BS7799 as their own national standard before 2000. In Europe, you have Netherlands and then later Denmark and Sweden. Outside Europe, there were Canada, Australia, New Zealand and South Africa.	As the international standard takes root it enmeshes with the peer-pressure element and forms part of the membership requirements of the group of political entities that wish to be known for the seriousness with which they take information security.

Source	Data	Interpretation
The DTI representative	In addition to SEMA survey, I was involved in several security management committees. One was European Security Forum (now called Information Security Forum set up by Coopers and Lybrand-now PWC), which was the club of security managers discussing various problems associated with information security. The other committee was OECD security committee, where I met R.H. from Midland Bank. The benefits of participating in these committees were networking and the opportunities of talking to people about the idea of having security management standards.	The information security community was very small in the early 90s and everyone knew each other, usually by means of the networking enabled through membership of the bodies mentioned here, as well as of I-4, which is mentioned later by this respondent. These networks formed the tissue for the social integration circuits that operated to develop thinking on the standard and ultimately to exert peer-pressure to conform to it.
The DTI representative	At the launch, I was asked how many copies were already sold, and I answered 10,000 copies. Apparently, both M&S and Shell had already bought 5,000 copies each for the company use, either giving to members or suppliers of the company.	The copies purchased by these two companies were destined for mandating internal use or for use by suppliers. Although the standard was still only at the Code of Conduct stage, the controls that it specified were soon to be requirements of doing business in and with these two companies.