Leiser Silva, Carol Hsu, James Backhouse, Aidan McDonnell

Resistance and power in a security certification scheme: the case of c:cure

Article (Accepted version) (Refereed)

Resistance and Power in a Security Certification Scheme: The Case Of *c:cure*

Abstract

Using the lens of Clegg's Circuits of Power (CoP) framework, this study examines the resistance to a UK information security certification scheme through three episodes of power that led to its withdrawal in 2000. The UK authorities sought to generate market competition between a generic certificate scheme with lower costs and international recognition and one based on technical rigor, but they failed in their objectives because of resistance from organizational players. This paper makes contributions to the understanding of the discursive nature of resistance to change in the research of standards and certification, and contributes to the literature by formulating the concept of discourse resilience: the property of discourses to resist change. It identifies the non-agentic nature of resistance in the absence of coercive power and presents a reflection on legitimacy as a required attribute for the acceptance of a certificate scheme. The research finds that what organizations deem to be legitimate is the result of power.

Keywords: Information security certification, circuits of power, resistance, qualitative research

1. Introduction

Information security standards and certification schemes have played a significant role in helping organizations safeguard information assets against a variety of internal and external threats. One example is the first security standard for information systems - BS 7799 – which evolved into an international standard now known as ISO/IEC 27002. In this sense, Barnard and von Solms [5] discuss the importance of BS 7799 and its certifications for securing e-commerce practices while Gomes and Velez [35] highlight their value in the Health Sector. With the emergence of new technologies such as cloud computing and biometrics there is a constant need to formulate national and international national standards in the field of information technology security (see [64]). However, Brunsson et al. [11] argue that "the development of standards is often a political and conflict-laden process" involving a variety of players from different domains with different interests, such as government authorities, certification agencies, experts and potential standard adopters. From the literature, we learn that security standards can have an impact on organizational information security practices [71, 6]. Hence, we argue that by studying the processes that bring standards and their respective certification schemes into being we are able to understand the content and practices associated with their implementation (e.g. [3, 11]). Such findings can bring theoretical and practical knowledge to those developing information security policy and security standards for the next period.

This research investigates an early attempt by industry stakeholders to implement a certification scheme, known as *c:cure*, for the information security management standard BS7799 in the UK. In discussing the importance and dynamics of standards and certification schemes, prior studies of certification predominantly using economics as research theory range from market penetration strategy [6,9,69], the economics of user involvement [19,28], and its relationship with institutional and technological change [2,74]. Overall, the economic perspective assumes that the motivation for standardization arises from the economic and strategic incentives in market penetration and diffusion [27]: organizations make rational choices when choosing to obtain certification, weighing up the balance of cost and benefit.

Nonetheless, critics have questioned the mechanistic and hegemonic view of certification, which was dominant in the economic approach [8, 84]. Brunsson et al. [11] argue that from the perspective of organization studies, standardization is "essentially a dynamic phenomena" where tension and conflicts among different interest groups are most likely to emerge during the creation, promotion and distribution process. IS scholars have also demonstrated the political nature of various information technology standardization processes [37,56]. Therefore, in this research, we align our theoretical position with these researchers, and draw on Clegg's Circuits of Power (hereafter CoP) framework to examine the complex social and political interactions embedded in the process of developing the certification scheme. This gives rise to our research questions: 1) *what is the role of power in influencing the rejection or acceptance of standards certification scheme?* 2) *what are the theoretical lessons that can be learnt from this particular case?* To address the research questions, we first examine the literature on standardization with a particular focus on the perspective of power and resistance. We then discuss the theory chosen to support the analysis: Clegg's [16] Circuits of Power (CoP). After this, we present our case in three key episodes. Each episode is followed by an analysis in terms of CoP. There follows a discussion formulating the main conceptual contributions of the analysis and reviewing their implications vis-à-vis the literature. The paper concludes with reflection on the scope and value of our research.

2. Power, Resistance and Standardization

In the IS security literature, the dominant research work on information security policy has concerned the organizational level including studies on end-user security policy compliance [73, 17, 40] and the role of management support and organizational culture [44, 47]. While these studies enhance our knowledge with respect to organizational and behavioral aspects of information security policy implementation, we found that only a few researchers have looked beyond the organizational boundary to examine the origin of industry-wide information security standardization. For instance, Backhouse et al. [3] draws on the CoP to examine the negotiation and interaction among different agencies during the BS 7799 development in the UK. Their study explains how exogenous contingencies triggered the need for security standards and identifies how power relations bind the different actors so they form alliances which eventually engender the legitimacy of the certification scheme, which the authors found, was crucial for the standard development. Their findings indicate that success relies heavily on making the certification scheme an obligatory passage for all relevant industry actors which required the realignment of political interests and decisions [13]. Others have drawn from institutional perspectives to discuss the effect of regulatory authority and industry competitors on the organizational adoption of information security policy [43,44]. These studies tend to concentrate on the role of professional and certification bodies. The purpose of our paper is not to reject or invalidate alternative approaches to studying standards but to complement them by adding a power perspective. Accordingly, to identify the complexities of engaging multiple parties in standardization, we review the literature studying power and politics, and in particular the roles these play in forming the consensus and fostering the legitimacy which are essential during standardization processes [14,27,77]

Even though organizational researchers have not concentrated specifically on aspects of resistance to and rejection of standards and their certification, some of them have focused on power-related phenomena such as resources, stakeholders' relations and negotiations. For example, Boström [10] discusses the importance of power resources for standards organizations in achieving credibility and authority, and the problem of the power shift resulting from the imbalance of power among key actors. In particular, he highlights the value of symbolic resources in maintaining moral legitimacy during the standard setting process. Fransen and Kolk [33] argue that multi-stakeholder standards can offer a more effective power balance among business and social representative of interest groups. Nunez-Nickel and Gutierrez [58] demonstrate the relevance of the political context in influencing the performance of independent professionals. Similarly, Dokko et al. [22] challenge the assumption of technological determinism of diffusion and argue that shaping and selecting technological standards is mediated through the social process of negotiation, debate and interaction between the participating organizations. Drawing on negotiated order theory, they demonstrate the dynamic interaction between technological change and social order.

Thus, while several studies have pointed to aspects of power in standard creation and the subsequent implications [3,80,77,9], the concept of resistance, especially discursive resistance, has not been extensively discussed,. The term discursive resistance is used here in the Foucaultian [30, 31,32] sense denoting resistance to knowledge conveyed in symbolic form. We argue that this type of resistance is relevant when agencies proposing certification schemes have no access to power in the form of authority or other disciplinary resource. Therefore, we argue by drawing on the literature in management control and organization studies that resistance is an important part of analyzing standards creation, since the failure to identify and manage it can have an impact on the acceptance or rejection of the associated certification scheme. We explain below the concept of resistance and its relevance to this research.

In sociological studies researchers have conceptualized resistance in power relationships as the opposite of induction [65]. Induction in this context means asking someone to do something he or she would not do of his or her own will [18]. Induction is normally interpreted as positive power while resistance is perceived as the source of negative power [16]. This notion of resistance as negative power has been, for example, the conventional approach to theorizing labor resistance to management control [76,68,50]. Fleming and Sewell [26] argue that earlier literature on resistance primarily focuses on the analysis of observable resistance such as official strikes and worker protests, and ignores the informal aspects of resistance such as meaning and routines [60]. Helin and Sandstrom [39] illustrate how a code of conduct ethics was resisted in the Swedish branch of a US company and find “resistance through distance” a more ambiguous and informal dimension of the concept of resistance. Resistance to induction, or positive power, is central to our study of certification scheme acceptance or rejection. A group of agencies – those proposing the scheme – attempt to induce others to adopt it.

Although researchers in the field of organizational studies have begun to consider resistance as something less visible and more subtle, in the area of standardization and certification this perspective has not been explicitly applied. As we discuss in the next section, resistance and power are not single dimensional and observable phenomena. Power and resistance are intertwined with language, discourse, rules of meaning and membership as well with techniques of production and discipline. It is this multi-perspective that makes CoP such a powerful lens for analyzing our case. Our conceptualization of resistance as a multi-directional activity links to Rus’s [65] argument defining “power as a cyclical relationship of induction and resistance” (p.7).

He argues for the need to move beyond the conventional dichotomy between induction and resistance to see resistance “not in negativity but rather in means, in the subject of power, or in rule of domination” (p.7). On the one hand, Rus recognizes the need for studying resistance related to discourses, but on the other, he acknowledges the complexity and difficulty of researching such phenomena.

Accordingly, in the next section we introduce our theoretical lens, the CoP. In so doing we discuss its main concepts and argue its suitability as a lens for studying standards certification scheme creation. We begin by illustrating the perspective on tension and politics in standardization, and argue for the value of resistance analysis in this particular context.

3. Theoretical Background

3.1 Clegg’s Circuits of Power

Clegg [16] conceives power as relational, i.e. power exists among two agents who are associated or connected in some way; it is the force that keeps social systems coherent. Therefore from this perspective an organization, understood as organized collective action, is the result of power. For Clegg power in organizational fields is manifested through the production of specific outcomes: tangible products or institutionalized practices. Organizational and social outcomes are possible as the result of relations among persons: relations sustained by power.

Three perspectives on power are integrated into the three circuits of power. The first circuit, the **circuit of episodic power,** is defined by the relationship between two types of agents: As and Bs. The As make the Bs do something they would not do otherwise; note that if the Bs agree with the As’ wishes, then no power is exercised [32]. This view of power as conceived in the relation between As and Bs is similar to the one of induction as mentioned above. Clegg warns however that just looking into the circuit of episodic power is not enough to understand the power phenomenon. There is a need also to consider the conditions that secure access to and control of the resources that ensure compliance and allow As to have power over Bs: what Clegg calls the *standing conditions* constituted by the other two circuits of power, social and systemic integration. This is the most evident of the circuits. In the case of studying the acceptance or rejection of standards we determine that the As in the relationship are those proposing the standard certification scheme while the prospective recipients of the scheme are the Bs. We can say, then that the As are inducing [65] the Bs to accept the scheme.

The second circuit, the **circuit of social integration,** is composed principally of rules of meaning and rules of membership. The rules of meaning refer to how different groups interpret events and objects. This is closely related to the power of discourse described by Foucault, who indicates that power is exercised by virtue of how we interpret events and by what we believe to be true [31]. The rules of meaning are also related to the concept of legitimacy as defined by institutional theorists [57]: in effect the power to decide what is legitimate. The rules of membership refer to power originated by individuals' association with particular groups. Groups, in this case, can be formal groups in an organization and, for example, hierarchical in nature, such as senior management, middle management and ordinary employees. Groups can also refer to public authorities and occupations such as police officers or doctors, whose power stems from their association with social institutions [30], or in the case of the manager, derived from the institutionalized manager-employee relationship that is underpinned by a legal contract. For the purposes of our study, the rules of meaning are related to the interpretation and legitimacy of the proposed scheme. When Bs resist the adoption of the certification scheme in terms of challenging its legitimacy, we call this resistance discursive [65].

The third circuit, **the circuit of system integration**, refers to the material conditions such as the means of production and technologies which afford an organization the production of goods and services, as well as its surveillance practices. Although the interpretation of power provided by the first two circuits mentioned above is incisive, our understanding of the power relation between As and Bs should be complemented by consideration of the systemic integration circuit. The compliance of the Bs with organizational objectives ensures systemic integration. Systemic integration here is understood to be a high degree of cohesiveness in an organization that permits the production of goods and services, and Clegg distinguishes two major concepts: techniques of discipline and techniques of production. The techniques of production refer to material means and procedures drawn on by organizations to generate goods and services, while the techniques of discipline refer to the measures and methods. In the employee example, the techniques of production refer to the definition of tasks in which employees are directed by managers while techniques of discipline would be used if an employee were to dissent from her managers' wishes. When studying resistance to the certification scheme, the techniques of discipline refer to any means the agencies proposing the scheme might deploy to enforce the adoption. As presented in the case, these agencies lacked such resources giving rise to the difficulties encountered in promoting the certification scheme. This is similar to what Boström [10] refers as fundamental power resources for the acceptance of standards.

The circularity of the framework is manifested when the repeated actions of Bs' compliance become institutionalized and integrated into the other two circuits. Returning to the earlier employee example, after continuous repetition the practice of Bs reporting all their activities to As becomes an institutionalized technique of production and discipline. At the same time the institutionalization of this practice will also reinforce the social and working relations between As and Bs. Changes to the circuits of power are induced by exogenous contingencies; i.e. events that are outside the realm of an organizational field or an institutionalized practice. Thus, the CoP provides an appropriate theory of interpretation of our case because it integrates different theoretical perspectives. It allows us to analyze the certification process not only as a strategy for legitimation as suggested by institutional theory, but also to integrate contingent factors such as particular agents' maneuvers and exogenous contingencies.

4. Research Method

Of the various research approaches, we consider that a case study is most suitable for this context for several reasons. First, the case study approach is suitable for studying processes – such as *c:cure*'s implementation – in which context and actions are closely related [83]. Indeed prior research has demonstrated the value of a case study approach in analyzing the complexity of standardization and certification process [3, 15, 56]. Second, case studies enable theory development as part the result of an iterative relation between data and concepts [23]. In this study we use the CoP as the underlying framework to guide our fieldwork and reveal a richer picture of social phenomena in which there are different power actors engaged in the standardization and certification process.

Fieldwork took place in summer 2001. Additional interview data was obtained in 2003 and 2004. While this case might be old, the example of power interaction remains relevant to the current standardization research. As Aggarwal et al. [1] contend, there is need to have a deeper analysis (such as the use of case study research) on "specific standard-setting situations" where stakeholders have different degrees of power" (ibid p.459). Our main method of data collection was semi-structured interviews with those involved in the development, marketing and administration of the certification scheme. We were able to gain good access to key actors in the scheme and 14 interviews were conducted. As Table 1 indicates, our interviewee represented the range of diverse interest groups involved in the *c:cure* scheme, ranging from the director of United Kingdom Accreditation Service (UKAS), the head of the Department of Trade and Industry (DTI) information security group, and head of security managers from different organizations. Given our focus was on the power dynamics among different stakeholders in standard and certification development process, we typically began with a broad question about their role related to the *c:cure* scheme development allowing us further questions on their interpretations of the proposed *c:cure* scheme and the actions taken by other stakeholders. Each interview session lasted between 1 and 2 hours. The second source of data comes from desk-based research, public reports and documents provided by the interviewees concerning the scheme such as the *c:cure* survey by the British Standards Institute (BSI), the DIT report, and BSI study on BS 7799 accreditation and certification scheme.

Interviewee's Position	**Role in BS7799 and *c:cure***
Director of development, UKAS	representing UKAS on the *c:cure* Steering Committee
Chief executive, Association of British Certification Bodies (ABCB)	a member of both BS7799 Accreditation Committee and the *c:cure* Steering Committee
Director, Independent Register of Certified Auditors (IRCA)	representing IRCA on the *c:cure* Steering Committee
Head of enterprise performance practice, The System Company	project manager for the *c:cure* development
Former head of the Department of Trade and Industry (DTI) security policy group (until 1999)	responsible for driving the *c:cure* scheme development until 1999
IT security consultant A	a member of both BS7799 Accreditation Committee and the *c:cure* Steering Committee
Technical services manager, Lloyds Register of Quality Assurance (LRQA)	represent LRQA during the *c:cure* scheme consultation stage
Deputy chairman, BS7799 users group	represent BS7799 users group during the *c:cure* scheme consultation stage and after
Business program manager, BSI Delivering Information Solution to Customer (DISC) Division	a division in the British Standard Institute (BSI) responsible for managing and marketing the *c:cure* scheme
IT security consultant B	was commissioned to draw up a review of the *c:cure* scheme
IT security consultant C	first certified *c:cure* auditor
Head of DTI security policy group (from 1999)	Responsible for BS7799 and certification program
Head of security management in banking sector	original contributor to BS7799 standard
Senior security manager in retailing sector	original contributor to BS7799 standard

Table 1 : Summary of Interviewee Information

4.1 Data Analysis

The approach adopted for analyzing the data consisted in drawing on our theoretical framework to tease meanings out of the case narrative. In so doing we conducted a dialogical process between data and theory [48,81]. Rus [65] suggests that when analyzing the cyclical relationship of power comprising induction and resistance,

> The unit of analysis of power accordingly cannot be a thing, a person, an act, a relation, and also not a status, it can only be the entire context within which the dialectic of power takes place.

This was fundamental for articulating our findings [23] and the analysis was conducted in three steps. The first step was to highlight key themes and major events that took place between 1995 and 2000. Case study notes were prepared containing the responses of the interviewees, summaries of the questions and answers, and comments on documents provided or physical observations. Key themes were then identified and discussed, at the same time; a chronology of the events was also developed. The second step was to derive the three circuits from the interview notes, documents and findings established in the previous episode. The objective was to identify the power agents, the resources and the meaning of membership that are significant in understanding the attempts to institutionalize the *c:cure* scheme. The third step was to offer an in-depth analysis of the basis of the narrative. Although the information had been analyzed and discussed among three independent researchers, to validate our interpretations we decided to share them with the actors involved and fortunately a number of our interviewees offered their services for reading the manuscript and providing feedback. Overall, our informants validated our interpretations but where there was divergence we made explicit their views in our interpretations.

5. The Case Study: The Resistance to C:cure

In this section we present the case study along with our analysis. *c:cure* (a timeline of the events is presented in Table 2 below) was never adopted by a critical mass of organizations and was eventually withdrawn. The purpose of our analysis is to explain its failure from a power perspective and we identify how power struggles hindered the integration of the three circuits. We posit that the lack of integration in the three circuits of power, the result of resistance from different actors, the presence of contradicting discourses, and the lack of disciplinary techniques, ultimately explain why the scheme failed to be widely adopted. For purposes of clarity we have divided the case into three episodes. Each episode is followed by an analysis using each of the circuits of power.

Table 2: Chronology of Key Events

Time	***Description of Key Events***
1995 February	BS7799 Part 1 published
1995 December	BS7799 Industry Working Group submits draft for an accredited certification scheme
1996 August	Department of Trade and Industry (DTI) publishes its idea for scheme
1996 Autumn	DTI commissions implementation plan for certification scheme
1997 August	DTI establishes BS7799 Accredited Certification Committee DTI establishes BS7799 Accredited Certification Committee
1997 October	BSI-DISC commissions an Accreditation and Certification Scheme Study
1998 February	BS7799 Part 2 published
1998 April	Minister for Small Firms, Trade and Industry announces launch of *c:cure* scheme
1998 September	*c:cure* auditor assessment and examination syllabus published
1999 November	Only 3 lead auditors, 4 auditors, 4 provisional auditors certified to act under *c:cure* scheme
1999 December	Only 3 certificates issued to organizations in 1999
2000 March	Review of *c:cure* scheme commissioned
2000 July	10 certificates issued on *c:cure* scheme
2000 October	*c:cure* scheme discontinued

5.1 Episode 1: Initiation of A BS7799 Certification Scheme

To address the rising concern over the increasing number of information systems security breaches in the UK, in 1993 the Department of Trade and Industry (DTI), the British Standards Institute (BSI) and seven major UK companies joined forces to develop a document entitled *A Code of Practice for Information Security Management*. The code became the British standard BS7799 in 1995, transformed in 2001 into the international standard ISO/IEC 17799.

Following the publication of BS7799, the idea of establishing a certification scheme gathered momentum. The original outline for certification against Part 2 of the BS7799 standard was drawn up by the BS7799 Industry Working Group and discussed at a public consultation workshop in December 1995. Shortly afterwards, this Group submitted a final draft for an accredited certification scheme to the DTI. Following the findings of the report, the DTI concluded that alongside the usual generic certification there was a special need for a second certification scheme for BS7799. Under this generic certification, the audit checks that establish the fitness of the applicant organization for certification against the BS7799 standard are performed by employees of an accredited certification body, such as one of the global management consultancies. The accreditor organization receives accreditation, not the individuals performing the actual certification audits. In the *c:cure* scheme, however, the assessor/auditor must be personally assessed and accredited – a much more stringent check on the quality of the auditor performing the review, and it was argued that *c:cure* was therefore a higher quality certification. Both DTI and BSI considered that the requirement of "*auditor competence*" would be "*sufficient to establish c:cure as the preferred BS7799 certification brand*".

The chair of the BS7799 International User Group (IUG), later known as the Information Security Management Systems (ISMS) group, recalled the rationale behind the idea of *c:cure*:

> After publishing BS7799 in 1995, the Group (the BS7799 Industry Working Group) decided to look into the idea of certification. While working on Part 2 of the standard, the Group also started a pilot project looking at a certification scheme. UKAS (*United Kingdom Accreditation Service*) wanted to have different schemes in order to maintain a competitive accreditation environment.

In August 1996, the DTI published a document outlining its ideas on "*certification against BS7799: Code of Practice for information security management*" and a 1997 consultancy report set out a plan emphasizing the crucial nature of:

- Speed to market (an interim scheme was proposed even whilst *c:cure* was being finalized)
- Compliance with the 'open market' requirements of EN4500 and with the UKAS obligations in the international arena to earn mutual recognition.
- Quantification of market demand for the scheme, in keeping with UKAS requirements

Hence there were various stakeholders with different interests. UKAS, the body sitting at the apex of all accreditation in the UK, desired to see competition amongst schemes in order to stimulate demand for high quality certification. BSI, both as a certification body providing generic certification but also as the business manager for the *c:cure* certification scheme, stood in a rather ambiguous position. It did not want to forgo income from the generic certification yet as the premier UK standards body accepted the desire for a higher quality level of accreditation. However, for many potential applicant organizations the choice of two competing paths to certification against the same standard simply resulted in confusion, having the effect of preventing progress on developing security: which way was the right way to go?

5.2 Analysis of First Episode Through the Lens of the CoP

For the purposes of our analysis we start by identifying the As and Bs of a causal episodic relationship. The As are constituted by the DTI, the BSI and UKAS whose missions were to ensure the security of electronic trade and the creation of standards and certification schemes. The Bs of the power relationship are constituted by those British organizations interested in demonstrating that their information systems were secure. The prime objective of the As was to ensure that through the adoption of the *c:cure* scheme and therefore much better security, the growing information-based economy in the UK would thrive and prosper. To achieve their objectives the As were prepared to countenance the two competing certification schemes: (1) *c:cure*, a rigorous scheme provided by specialized auditors and (2) the generic scheme offered by traditional consulting companies providing certification services. The As considered that competition between the two schemes would be fruitful. It would extend the coverage and enhance the quality of the implementation of the underlying standard (BS7799).

From the perspective of social integration, we can appreciate the exercise of power in this circuit through the belief held by the As that offering two competing schemes would improve the quality and extent of certification of information security management. The dominant discourse here is the value of market forces and of competition in enhancing quality and engendering widespread adoption.

Another salient discourse in the circuit of social integration was that of rigor and technical detail. According to this, the As believed that, given *c:cure*'s more stringent technical demands, the Bs would consider *c:cure* to be superior to the generic scheme. Here the belief is that specialization and rigor are fundamental for the acceptance of a security management certification scheme. The dominant notion is that technical detail and specialization should be interpreted as values of the utmost importance. Hence, the As believed that *c:cure* would facilitate and nurture e-commerce by sending out to all a strong message of quality and trustworthiness. Thus, the analysis of this circuit identified two main discourses emanating from the As: (1) competition is valuable and (2) the quality of the scheme is directly proportional to its technical rigor.

Through the lens of systemic integration, we identify that the most tangible technique in this circuit was the certification scheme itself. It consists in the auditing and issuance of a certificate of conformity with the information systems security management standard BS7799. The scheme can be considered a prime example of a technique of discipline and production. The As believed that the effectiveness of the scheme would rest on its detailed and rigorous content; i.e. organizations adopting the scheme would be able to claim more manifestly secure information systems. Moreover, the certification scheme was designed with the purpose of having a disciplinary effect, so that organizations would have to adopt it in order to demonstrate competence and legitimacy for practicing e-commerce. However, in embracing a market discourse the As forwent the deployment of disciplinary techniques to force the adoption of the certification scheme.

5.3 Episode 2: Launch of C:cure Scheme

In August 1997 the DTI established the BS7799 Accredited Certification Steering Committee and appointed BSI-DISC, a unit of BSI, as the scheme manager. This Committee consisted primarily of trade and professional representative bodies providing input to the scheme manager on the scheme's development, marketing and funding.

To demonstrate its commitment and determination to the BS7799 Accredited Certification Scheme, DTI allocated 1 million GBP to the project. This sum was allocated to contracts undertaken by three organizations active in the standards certification business: Level-7, BSI-DISC and the Systems Company[1]. A study contracted to the Systems Company by the *c:cure* scheme manager (BSI-DISC) in February 1998 identified the principal criteria, scheme protocols, and specific criteria for preliminary auditor registration and certification. The requirements held that the scheme should be credible, of demonstrable value, affordable, and self-funded.

Mrs. Barbara Roche, the UK's Minister for Trade and Industry, launched the *c:cure* scheme for certification in April 1998 at the Infosecurity Exhibition, where she emphasized the importance of organizations obtaining certification:

> [*c:cure*] aims to facilitate electronic commerce by allaying fears about security…… [certified organisations] to demonstrate that they have given serious consideration to all the security threats they face, and that they have put appropriate safeguards in place.

In September 1998 the *c:cure* auditor assessment criteria and examination syllabus were published, underlining the high quality of the certification. Meanwhile, the DTI decided to establish the *c:cure* scheme as a fully self-funded program, i.e. no further funding from DTI. The *c:cure* Steering Committee concluded that the financial resources would be generated from three sources: the sale of BS7799 certification guides, the annual *c:cure* maintenance fee charged to certificate holders between full audits, and 12% of the relevant audit fee charged by the certification bodies to applicant organizations. One emerging paradox was that while a sub-unit of BSI (BSI-DISC) was the business manager for the scheme with key responsibility to promote *c:cure*, BSI also numbered as one of the vendors of the cheaper generic route to certification.

Many industry practitioners accused the DTI and BSI of harboring unrealistic expectations about *c:cure* take-up and that optimistic targets would not be realized. The former head of the Information Security Policy Group at the DTI recalled that the target figures were "*20-30*

[1] The names of the organization have been changed.

certificates in year 1 and 60 certificates in year 2, to keep in line with the ISO 9000 scheme". By comparison, IRCA, the Independent Register of Certified Auditors, one of the certification bodies first accredited for the *c:cure* scheme, expected no more than 10 certificates to be issued before July 2000. Lloyds Register Quality Assurance (LRQA), another organization that became a certification body for *c:cure,* expected to issue no more than 2 certificates in the first year of the scheme. One problem was that some organizations (i.e. Bs) that might have been considered as potential scheme applicants had no need for certification. A Chief Information Security Officer in the banking sector explained:

> The success of BS7799 could not really be measured by the number of certifications since many companies see no need for certification despite using BS7799 for its company. For example, at my company, there is always contractual agreement between the partner about complying security management matching BS7799 standard or its equivalent. The contractual agreement gave my company the right of audit if necessary, hence, there is no need for requesting partners to acquire certification.

Several organizations (i.e. Bs) viewed their participation as reluctant or passive rather than voluntary and active. For example, IRCA described the process of their involvement as one of being "*dragged kicking and screaming*" into the scheme – in other words, there was considerable pressure placed on them by the government to become a *c:cure* certification body. UKAS, likewise, complained of being pressured to participate in the scheme. As one interviewee told us,

> as the consultation forum of the *c:cure* scheme continues, our participation was primarily characterized as passive or absent.

The lack of strong industry support was reflected in a number of industry surveys that showed that there were still many businesses in the UK entirely unaware of the security management standard, let alone any certification scheme. The annual Business Information Security Survey

1998 found that only 25% of its 1000 respondents (covering manufacturing, public and service organizations) had even heard of BS7799 and only 5% were planning to seek certification at some stage.

5.4 Analysis of Second Episode Through the Lens of the CoP

The circuit of social integration draws our attention to discourses and how they are interpreted. In our case we identify a prominent discourse influencing As' actions and their corresponding interpretations. It derives from economic rationality, linking and emphasizing the role of market forces and their legitimacy. This was expressed in the report from the Systems Company consultants, suggesting that the *c:cure* scheme should be credible and affordable. The first required attribute of credibility, legitimacy, related to the belief that the scheme had been prepared by reputable industry experts. The second attribute, affordability, on the other hand centered on the economic rationality of the scheme. The rationale was that the cost had to be lower than its value or, as suggested in the literature, that the costs could be transferred to customers [38,61].

There are contradictory interpretations regarding the legitimacy of the As' alliance. To buttress their argument for the legitimacy of the *c:cure* scheme, the As announced that the scheme had been prepared "in consultation with industry"; this was the main discourse of legitimacy for the scheme. The Bs may have interpreted this to mean that if the scheme had been prepared "in consultation with industry", then it would follow that most relevant organizations would adopt it: the dynamics of mimetic forces. However, most Bs did not believe that the scheme had been genuinely prepared "in consultation with industry". Our data shows that organizations were aware that arm-twisting had been applied and were unconvinced by the arguments for the *c:cure* scheme. Thus the discourse of the As identified here is that the certification scheme was formulated in "consultation with industry", and hence legitimate, while for the Bs the scheme was an imposition, expensive and complex.

From the point of view of the circuit of systemic integration, we observe that the method of hiring consultants as a technique to achieve As' objectives was resorted to constantly throughout the case. Consultants were hired with the purpose of conducting a study to determine the feasibility of the more specialized certification scheme. The report emphasized that such a scheme had to be launched quickly and comply with national and international requirements for that type of certification. More importantly, the report stated that before its creation and launch the DTI and its allies had to ensure that there was enough demand in the market. Our data shows that the As moved ahead with their plan because of their strong belief in the value of having two competing schemes and in the technical virtues of *c:cure*. Then after making the decision to go ahead with the new scheme, the As hired another consulting firm. The task of these consultants was to design the content of the scheme as well as its plan of implementation. Accordingly, the consultants' report specified the scheme's protocols and its auditing requirements. The over-reliance of the As on the technique of hiring consultants bears some reflection. First, the reports did not show how the attributes (credibility and affordability) that were stated as key to the success of the scheme would be clear to prospective certificate applicants: how a more rigorous scheme requiring specialized auditors would be worth the extra expense. As one interviewee told us, "firms have spent too much money on getting certification for ISO 9000 and other purpose. In this case (security management), it was more important to have security policy in place within the organization, the issue of security certification was not really important." Second, the reports never warned the DTI about the risks of having two competing certification schemes - the potential ambiguity and confusion created by having two schemes was not foreseen. Third, one of the consultants' reports presented an over-optimistic forecast for demand for *c:cure* certificates. Finally, once the impending demise of the scheme became evident, it was a consultant report that recommended abandoning it. Following this kind of advice hardly ensured a coherent and consistent approach for the As.

5.5 Episode 3: Road to Discontinuation of C:cure Scheme

Despite the 500 auditor information packs issued and 40 applications submitted in June 1999, the rosy start for *c:cure* soon began to fade. By November 1999, only 3 lead auditors, 4 auditors and 4 provisional auditors had been certified under the scheme. The certification scheme manager BSI-DISC voiced regret about the insistence on such rigorous auditor assessment: "the entire auditor registration process turned out to be a frustrating bottleneck".

Another senior information security consultant confirmed the clash of cultures when recalling the experience of his interview for accreditation as a *c:cure* auditor:

> I had one interview by two security experts and a member of IRCA who was an ISO 9000 auditor. The interview descended to farce when the ISO 9000 person said that he could not understand why there was no client names, given on my application, for whom I had worked. I stated that my contract did not permit me to divulge any client details at all, whereupon he said that he had never heard of this in his whole ISO 9000 experience.

More disquiet emerged. A keenly felt problem was the cost of *c:cure* certification. Rigorous auditor assessment inevitably added to the cost of the certification bodies, which subsequently passed the cost on to the companies seeking *c:cure* certificates. One consultant told us,

> When I was in the National Computing Centre, only 1 client was ready to go ahead with certification. There were another 3 initially preparing for the process, but then all decided to drop out after the cost and unclear business benefits. The cost was too huge for SMEs. The certification is valid for 3 years. The company needs to have pre-audit preparation and then pass 5 steps of surveillance programs. All these probably would cost a firm between 3,000 and

> 5,000 (GBP). It is very difficult to justify this to the top management

Indeed, two of the scheme's certification bodies, IRCA and LRQA openly complained about making losses and both blamed the rigorous assessment for *c:cure* auditor accreditation. Owing to the small numbers of auditors being certified, IRCA declared it was not able to generate sufficient income from its own triennial registration fee. LRQA was expecting to recover its investment and obtain a additional revenue stream from *c:cure* certifications once the scheme started to operate. But the anticipated demand for *c:cure* certification never materialized.

Even outside the UK, the *c:cure* scheme was negatively received. The chair of the BS7799 International User Group told us that even among the groups that were supporters of the BS7799 standard, one country strongly objected to the proprietary and localized (i.e. UK) nature of the *c:cure* certification scheme and that they "*point blank refused to support it*". The head of DTI Information Security Policy Group also commented,

> It is rather an absurd idea. On the one hand we are promoting the internationalization of the standard, on the other hand we are developing a certification that is localized. This does not make sense.

This Group head also told us that he attended a *c:cure* Steering Committee meeting on the very first day of his appointment in late 1998, and concluded that *c:cure* was going nowhere:

> 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 certification organizations issuing BS7799 certificates. So what is the value of *c:cure* which costs even more than a generic certificate?

In 1999, the first *c:cure* certificates were awarded to just 3 organizations. By early 2000, in the light of the continuing low levels of applications, the Steering Committee commissioned a consultant to undertake a review of the *c:cure* scheme. By the time of the first draft, only 10 *c:cure* certificates had been issued. The final version of the report was circulated to the Steering Committee members in August and at their meeting in October 2000 the members agreed to discontinue the scheme, citing "confusion between *c:cure* and non *c:cure* certification as well as low market take up".

5.6 Analysis of Third Episode Through the Lens of the CoP

At the end of the case we observe that very few Bs were enrolled wholeheartedly into the As plans. Our analysis shows that none of the circuits of power achieved integration and here we summarize the main reasons. First, British organizations did not adopt the scheme in large numbers. Second, few industry experts responded to the call made by the steering committee to join the ranks of auditors conducting the scheme assessments. Third, those organizations which had joined the steering committee of *c:cure*, i.e. the members of the As' alliance, harbored serious doubts about the viability of the scheme and remained in the committee only with reluctance.

By scrutinizing the circuits of social integration and episodic power we observe that the meanings assigned by the As to the scheme were not the same as those assigned by the Bs. For example, the As' strategy of two competitive schemes was interpreted differently by the Bs: they were eventually confused by the choice of two schemes. The discourse espoused by the As was that the scheme was legitimate and rigorous, while for the Bs the scheme was confusing and onerous. What is interesting here is to notice how the discourse of the Bs prevailed over that of the As since, most Bs chose not to adopt either scheme until the confusion had been cleared. As discussed below, we call resilience this property of a discourse that prevails over a competing one. In a similar manner, international bodies were also confused by the presence of two certification schemes and followed the same course of action as their British counterparts; i.e.

they adopted a policy of wait and see. In addition, prospective auditors interpreted the content of the scheme not as being more sophisticated and attractive, as the As intended, but as too difficult and complicated. We note here the resilience of Bs discourse, which prevails over that of the As.

One outcome of these disparate interpretations, of these contradicting discourses, was a smaller than expected pool of suitably accredited auditors. Worse still, industry saw the *c:cure* accredited auditors not as experts and specialists but, in some cases, as consultants of dubious quality converted in an *ad-hoc* manner from other kinds of auditing into security auditors. Nor did the Bs recognize the economic benefits, as the As had expected, of adopting a more expensive scheme when a cheaper rival (the generic option) was also available. Many Bs, retail banks for instance, through their bilateral contractual relations with suppliers were still able to ensure compliance with BS7799 to the satisfaction of their commercial partners without needing to be certified. The direct competition from the generic scheme, as well as the availability of other ways in which to enforce and demonstrate compliance with the standard, undermined the credibility of the discourse espoused by the As that *c:cure* was economically viable. The analysis of the case from the lens of the social integration circuit reveals the reasons for the actions of As and Bs. The organizations that were supposed to accept the discourses associated with the scheme: technical sophistication, economic viability and widespread industry acceptance – not only rejected those discourses, but also countered them with alternative discourses; that the certification scheme was confusing, onerous and localized (UK centered).

Analysis through the lens of the circuit of systemic integration shows that a constant theme in the case was the As' deployment of market-driven techniques. This was evident in the decision to allow market competition, eventually a major reason for confusion because the existence of competition drew attention to the commercial infeasibility of *c:cure*. With two certification schemes in the market, British organizations could compare the costs of one scheme against the other. Market estimates calculating the demand for *c:cure* might well have been off-target because they may have not considered the impact and availability of the other certification scheme. Furthermore, market estimates could have failed to factor in the existence of contractual relations between organizations that forced them in any case to comply with BS7799. In addition, the DTI overestimated the demand from prospective auditors to be enrolled and accredited into the scheme.

The analysis of the case from the perspective of the systemic integration circuit highlights the failure of the techniques adopted by the As. By over-depending on consultants and market studies, the As underestimated the challenges in designing and implementing a rigorous and proprietary scheme that had to compete with another which was generic and more affordable. Surprisingly, the most glaring mistake made by the As consisted in the techniques that they did <u>not</u> deploy. For example, a technique of discipline that could have worked might have been the introduction of specific legislation or regulation, making *c:cure* obligatory for conducting electronic trading in the UK. Such a regulation would have been a coercive force that eventually might have eventually triggered the widespread adoption of the scheme. Yet, in the case of *c:cure* it did not happen, perhaps to be expected given the strong market orientation. Indeed, there are several general lessons that can be drawn from this analysis and they form the main topic of the next section.

6. Discussion

In this section we discuss the implications of our study. The discussion is structured around the insights derived from our analysis and by the CoP. The underlying assumption is that *c:cure* was a technique of production proposed by the As to alter the current circuits of power of the organizational field comprised of British organizations interested in information systems security. In our discussion we also articulate the main contributions of our paper: formulating the concept of discourse resilience to explain resistance in the circuit of social integration, reflecting on the power struggles to determine legitimacy and establishing the role of non-agentic resistance in the absence of facilitative power. These theoretical implications are not generalized to predict which competing standards win, rather they are *analytical generalization* focusing on contributions to the extent body of knowledge of standards and certification scheme [52, 81].

6.1 Resistance from Resilient Discourses

We found that resistance to the introduction of *c:cure* arose from prevailing discourses in the circuit of social integration, specifically in the extant rules of meaning. The discourse with which the As promoted the scheme was one of technical rigor. However, the Bs of the relation did not accept this discourse because they interpreted it through a simple economic discourse: the scheme was too expensive and confusing. Organizations, the Bs of the power relation, interpreted the proposal of the As with the rules of meaning prevailing in the extant circuits of power; that of market economy in which the principle of total utility [41] prevailed: i.e. given the availability of a generic certificate that was enough to convey compliance and that at the same time cost less, the need for a higher quality certificate was not justified for the Bs. As our case shows, eventually the market economy discourse prevailed. The marginal utility discourse, that prefers low cost, resisted the discourse of technical *rigor* and developed in consultation with industry. Despite the As efforts the Bs did not change their interpretation.

The *resilience* of the marginal utility discourse over other discourses in a market of standards and certification can also be found in other empirical research [63,53]. Reinecke et. al. [63] suggest, for example, that in case of the presence of multiple certification organizations will tend to choose the most economic option to avoid higher costs. Their findings are related to our research, as the cost of *c:cure* was one of the main reasons given for its non-adoption. Lee and Oh [53] studied the failure of the Chinese government in promoting WAPI as the standard of wireless networking and one main reason for its non-adoption was its higher cost in comparison with its main competitor WiFi. We conclude that in the absence of facilitative power exercised by the As, the dominant discourse in the circuits of power will tend to prevail. Facilitative power here refers to deploying techniques of discipline to ensure compliance.

In cases where the resilience of a current discourse is strong, the As may consider deploying techniques of discipline. The resilience of an extant discourse can be weakened through the promotion of different rules of meaning but, we argue, it will still require the exercise of facilitative power as in the case of ecological friendly and environmental sustainability discourses, in which public opinion is not enough to induce structural changes in organizational fields. For example, Sarkar and Young [67] found that organizations are reluctant to adopt "green" IT because of its high costs; despite acknowledging the positive effects this technology may have in the environment. We conjecture that had the British Government introduced regulations supporting *c:cure*, certification would have been widely adopted and changes to the circuits would have stabilized over time. Our findings are contributions in that they qualify the widespread belief that the adoption of a new practice requires a combination of coercive, mimetic and normative forces [21]. When proposing changes in extant circuits of power with resilient discourses, organizations may not rely only on dispositional power – i.e on discourses; changes may not be implemented without deploying facilitative (coercive) power.

Examples of the need for facilitative power for introducing change in organizational fields have been documented widely in the literature. For example, Guler *et al.* [36] found that governmental bodies and multinationals apply coercive power effectively in the diffusion of quality management certificates. For example, the European Union has played a key role in requiring firms, especially new market entrants, to seek ISO 9000 certification, while the Singapore government mandates it for large construction firms wishing to register to undertake public-sector projects [59]. The coercive pressure for conformity plays a fundamental role in the diffusion of new organizational practices or strategies. We argue that without coercive power and if left to the market those proposed standards and certifications may have not been adopted.

Moreover, we hold that there is a relationship between time and the resilience of a discourse. We argue that the resilience of discourses will be stronger the longer they have been the dominant discourse in the circuits of power. In our case the market economy (principle of marginal utility) has been the prevailing rule of meaning in British businesses for many years. Indeed, the marginal utility principle lies at the core of any market economy and has done for centuries [69]. Similar observations have been made by other researchers [80,22]. For example, Vermeulen et. al. [80] found that the Dutch government, in its attempt to create a market in the construction industry, failed to change the core beliefs in a market that had existed since the 19th century. Dokko et. al. [22] in a similar fashion suggest the resilience of discourses through time, as they explain technological change in organization fields from an evolutionary perspective. They explain the resistance to change in systems from the point of view of punctuated equilibrium: that systems tend to remain stable for long periods of time until change is introduced by disruptive contingencies [78,34,66].

The notion of resilience is intimately connected to that of legitimacy which the literature recognizes as a fundamental and necessary attribute for the adoption of a standard or a certification scheme [63,30,69,3,38,52]. Timmermans and Epstein [77] in their study of a resistance movement for altering the practices of standardizing human beings in biomedicine research observe that neither certificates nor standards can be adopted when they are deemed to have no legitimacy. Researchers have also pointed out the centrality of the discourse of legitimacy for the adoption of information security certification [44,51,43]. Instead of explaining adoption in terms of economic benefits, these researchers explore the sources of conformity and the organizational consequences of implementing certification. Accordingly, these studies have shown that holding a recognized certificate increases a firm’s legitimacy, i.e. its good reputation and trustworthiness [4,46,62]. This institutionalization, they argue, is mainly the result of mimetic forces [20] whereby the firm imitates the practices of successful, dominant organizations. Our contribution here is to show what happens when two certificate schemes with dissimilar discourses compete. We discovered that the dominant one in the current circuits of power, i.e. the more *resilient* one, will prevail.

6.2 Non- Agentic Resistance

Our study also demonstrates that in the absence of disciplinary techniques, resistance to change in the circuits is not only offered by agencies but also by discourses. As observed above, in the absence of systemic power, disputes will occur between discourses. That is not to say that the discourses acted on their own, as clearly they achieved it through different agencies: government authorities, consultants, auditors and managers, just to mention some. What we observed, though, is that agencies seem not to be responding to personal interests but to be defending what they thought was rational and true [30,32]. It was in this sense that we say that the discourses were the ones offering resistance. In our case, the competing discourses were marginal utility (low cost) against a discourse of quality (technical rigor and "in consultation with industry").

In our case we found that the As favored a technocratic discourse as they thought that competition between certificates would be based on quality. The belief in the superiority of the technocratic discourse was crystallized in the DTI's conviction that the more technical and rigorous the scheme the more attractive it would be for organizations. This is an example of what Andrew Feenberg [25], the critical theorist of technology, calls *technocracy*, that is, the conviction that given its intricacies, technology development and its diffusion should be the responsibility of technical experts. The technocratic perspective of the DTI is also reflected in its over-reliance on consultants. Consultants were seen as experts in market studies and were also considered to be experts in financial matters. The DTI paid more attention to what the consultants were saying in respect of the market for *c:cure* than to the opinions of other members of the committee. Had the technocrats of the DTI questioned the strength of its technological discourse, they might not only have prevented the failure of *c:cure* but also saved at least one million British Pounds. The over-reliance of the DTI on consultants and its failure sufficiently to heed key users reduced the chances of useful early feedback.

The non-agentic power of discourses and its relation to technological change is noted, for example, by Knights and McCabe [49]. In their study of Total Quality Management (TQM) programs Knights and McCabe, reflecting on the views of power of Foucault and Lukes, point out that power has to be understood beyond mere actions and highlight the relevance of the power of discourse. In their study they notice the non-agentic power of discourses that provide TQM programs with a sense of inevitability in fostering legitimacy in an organizational field. Similarly, in studying resistance in public management service, Thomas and Davis [75] challenge the dominant view of resistance as passive and behavioral, and argue for focusing on meanings and symbolic interpretation. Our contribution is to identify the circumstances in which non-agentic resistance will be predominant, that is when agencies promote changes in circuits of power without deploying facilitative power, but just through competition of discourses in a market economy.

7. CONCLUSION

In this research, we investigate the dynamics of institutionalizing an information security certification scheme in the UK. Our analysis raises important practical issues about both the creation and diffusion of certification schemes. As highlighted in the discussion, technical superiority does not necessarily hold sufficient attraction for the early adopters, and simplicity with broader collective objectives can become determining factors in the game of survival between two competing schemes. This study found that where two discourses compete, the more resilient discourse, the one more deeply rooted in the current circuits of power is the one that prevails: the market discourse takes precedence over that of technology. Furthermore our study confirms the role of the non-agentic resistance of discourses: discourses themselves compete when agencies may not be consciously resisting but rather merely defending what they see as rational and true. Our study once again underlines the critical importance of legitimacy in the standards and certification field. The two schemes were rooted in two different legitimacies, the technical rigor of c:cure against the international and low-cost nature of the generic certification scheme. Instead of technical rigor, market legitimacy won the day, underlining the power of a prevailing legitimacy.

In terms of practical implications, our findings related to circuit of systemic integration suggest that government or any agency promoting the adoption of a certification scheme may consider that in cases of low legitimation, coercive power may be the only way to ensure adoption. As coercive power is rarely deemed viable, especially in market economies and democratic societies, our study suggest that agencies proposing certification schemes should pay careful attention to and make efforts to strengthen the legitimacy of their proposal. For information security standards, our empirical study shows that potential adoptors still consider market legitimacy and logic as a determining factor in their evaluation of standard adoption. Over-reliance on technical-featured legitimacy could potentially lead to a failure in diffusing a new security technology standard.

In terms of research limitations, perhaps, the CoP does not function quite so well in a fluid situation when agents do not remain in the same role over time. In particular it may not be able to explain power relations when the clear distinction between As and Bs fails to apply or when there are changes in alliances such as As becoming Bs and vice-versa. In our data the BSI is an important standards player in the UK, but it also has a department of its organization (BSI-DISC) which was the business manager for the *c:cure* certification scheme business but also sold generic certification. This was an example of the overlapping of boundaries with a lack of clear distinction about whether an organization can be deemed irrefutably an A or a B.

Another limitation of the CoP that we found in our analysis is the mechanistic nature of the Obligatory Passage Point concept. This is clear metaphor for As who try to make Bs do something they otherwise would not do. Whilst this is useful as an indicator of when power is being exerted, there may be different interpretations about what may be obligatory. In our case the passing of regulation requiring organizations to acquire certification would have been a clear obligatory passage point. In our data though we find that the Bs were always able to decline certification, and *c:cure* in particular, because although demonstrating security was useful, it was not at the time necessary. So what was the passage point that ultimately failed? The failures were several and not just one.

In conclusion, this study has shown the contingent nature of the stabilization or institutionalization of a security certification scheme. We argue that the fate of a scheme will depend on the resistance in and around the different stakeholders. Although the area of standards and certification is broad because it encompasses different traditions – economic, institutional and critical – we hope our study constitutes a contribution to those literatures. We believe the political perspective for studying stabilization is an approach from which researchers can learn. This paper constitutes an effort in that direction.

References

[1] N. Aggarwal, Q. Dai, E.Walden, The more, the merrier? how the number of partners in a standard-setting initiative affects shareholder's risk and return, MIS Quarterly 35 (2) (2011) 445-462

[2] C. Antonelli, Localized technological change and the evolution of standards as economic institutions, Information Economics and Policy 6 (3/4) (1994) 195-216

[3] J. Backhouse, C. Hsu, L. Silva, Circuits of power in creating de jure standards: shaping an international information systems security standard, MIS Quarterly 30 (Special issue) (2006) 413-438.

[4] P. Bansal, T. Hunter, Strategic explanations for the early adoption of ISO 14001, Journal of Business Ethics 46(3) (2003) 289-299

[5] L. Barnard, R. von Solms. The evaluation and certification of information security against BS 7799, Information Management & Computer Security 6 (2) (1998) 72-77.

[6] R. Baskerville, P. Spagnoletti, J. Kim, Incident-centered information security: managing a strategic balance between prevention and response, Information & Management 15 (1) (2014) 138-151

[7] S. Besen, J. Farrell, Choosing how to compete: strategies and tactics in standardization, The Journal of Economic Perspectives 8 (2) (1994) 117-131.

[8] O. Boiral, ISO 9000: Outside the iron cage, Organization Science 14 (6) (2003) 720-737

[9] M. Bonino, M. Spring, Standards as change agents in the information technology market, Computer Standards and Interfaces 12 (2) (1991) 97-107

[10] M. Boström, Regulatory credibility and authority through inclusiveness: standardization organizations in cases of eco-labelling, Organization 13 (3) (2006) 345–367

[11] N. Brunsson, A. Rasche, D. Seidl, The dynamics of standardization: three perspectives on standards in organization studies, Organization Studies 33(5-6) (2012) 613-632

[12] B. Bulgurcu, H. Cavusoglu, I. Benbasat, Information security policy compliance: an empirical study of rational-based beliefs and information security awareness, MIS Quarterly 34(3) (2010) 523-548

[13] M. Callon, Some elements of a sociology of translation: domestication of the scallops and the fishermen of St Brieuc Bay. In J. Law (eds), Power, Action and Belief: A New Sociology of Knowledge, London: Routledge and Kegan Paul (1986) 196-223

[14] C.F. Cargill, Information Technology Standardization: Theory, Process and Organizations, Bedford, MA: Digital Press (1989)

[15] C. Chang, S. Jarvenpaa, Pace of information systems standards development and implementation: The case of XBRL, Electronic Markets 15 (4) (2005) 365-377

[16] S. Clegg, Frameworks of Power, London: Sage Publications (1989)

[17] J. D'Archy, A. Hovav, D. Galletta, User awareness of security countermeasures and its impact on information security misuse: a deterrence approach, Information Systems Research 20 (1) (2009) 79-98

[18] R. A. Dahl, The concept of power. Behavioral Science 2 (3) (1957) 201-215.

[19] P. David, D. Foray, Markov random fields, percolation structures and the economics of EDI standard diffusion. In. Pogorel, (Eds), Global Telecommunication Strategies and Technical Change, Amsterdam: Elsevier (1994) 135-170

[20] P. DiMaggio, W. Powell, The iron cage revisited: institutional isomorphism and collective rationality in organizational fields, American Sociological Review 48 (2) (1983) 147-160.

[21] M.L. Djelic, Exporting the American model: The postwar transformation of European business, New York: Oxford University Press (1998) 322

[22] G. Dokko, A. Nigam, L. Rosenkopf, Keeping steady as she goes: A negotiated order perspective on technological evolution, Organization Studies 33 (5/6) (2012) 681–703

[23] K. Eisenhardt, Building theories from case study research, Academy of Management Review 14 (4) (1989) 532-550

[24] D. Elmuti, Y. Kathawala, An investigation into the effects of ISO 9000 on participants' attitudes and job performance, Production Inventory Management Journal 38 (2) (1997) 52-57

[25] A. Feenberg, Questioning Technology, New York: Routledge (1999)

[26] P. Fleming, G. Sewell, Looking for the good soldier, Švejk: alternative modalities of resistance in the contemporary workplace, Sociology 36 (4) (2002) 857-873

[27] V. Fomin, T. Keil, Standardization: bridging the gap between economic and social theory, Proceedings of the International Conference on Information Systems, (2000) 206-217

[28] D. Foray, Users, standards and the economics of coalitions and committees, Information Economics and Policy 6 (3) (1994) 269-293

[29] V. Formin, K. Thomas, Standardization: bridging the gap between economic and social theory, Proceedings of the International Conference on Information Systems (2000) 206-217

[30] M. Foucault, Discipline and Punish, New York: Vintage Books (1977)

[31] M. Foucault, Power/Knowledge: Selected Interviews and Other Writings 1972-1977, Brighton: Harvester Press (1980)

[32] M. Foucault, The subject and power. In. H.L. Dreyfus, & P. Rainbow, (eds.) Michel Foucault: Beyond Structuralism and Hermeneutics, London: Harvester Wheatsheaf (1982) 208-229

[33] L. Fransen, W., A. Kolk, Global rule-setting for business: A critical analysis of multi-stakeholder standards, Organization 14 (5) (2007) 667–684

[34] C. J. Gersick, Revolutionary change theories: a multilevel exploration of the punctuated equilibrium paradigm, Academy of Management Review 16 (1) (1991) 10-36

[35] R. Gomes, L. V. Lapão, The adoption of IT security standards in a healthcare environment, Studies in Health Technology and Informatics 136 (2008) 765-770.

[36] I. Guler, M. Guillen, J. Macpherson, Global competition institutions, and the diffusion of organizational practices: the international spread of ISO 9000 quality certificates, Administrative Science Quarterly 47 (2) (2002) 207-223

[37] O. Hanseth, K. Braa, Hunting for the treasure at the end of the rainbow. standardization corporate IT infrastructure, Computer Supported Cooperative Work 10 (3/4) (2001) 261-292

[38] C. Haksever, TQM in small business environment, Business Horizons 39 (2) (1996) 33-40

[39] S Helin, J Sandström, Resisting a corporate code of ethics and the reinforcement of management control, Organization Studies 31(5) (2010) 583-604

[40] T. Herach, H. Rao, Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness, Decision Support System 47 (2) (2009) 154-165

[41] J. Hicks, The foundations of welfare economics, The Economic Journal 49 (196) (1939) 696-712

[42] C. Hsu, Frame misalignment: interpreting the implementation of information systems security certification in an organization, European Journal of Information Systems 18 (2) (2009) 140–150

[43] C. Hsu, J.N. Lee, D. Straub, Institutional influences on information security innovations, Information Systems Research 23 (3) (2012) 918-939

[44] Q. Hu, P. Hart, D. Cooke, The role of external influences on organizational information security practices: An institutional perspective, Journal of Strategic Information Systems 16 (2) (2007) 153–172

[45] Q. Hu, T. Dinev, P. Hart, D. Cooke, Managing employee compliance with information security policies: The role of top management and organizational culture, Decision Sciences, 43 (4) (2012) 615-660.

[46] R. Jiang, P. Bansal, Seeing the need for ISO 14001, Journal of Management Studies 40 (4) (2003) 1047-1067

[47] A. Kankanhalli, H.-H. Teo, B.C.Y. Tan, K.-K. Wei, An integrative study of information systems security effectiveness, International Journal of Information Management 23 (2) (2003) 139-154

[48] H. Klien, M. Myers, A set of principles for conducting and evaluating interpretive field studies in information systems, MIS Quarterly 23 (1) (1999) 67-94

[49] D. Knights, D. McCabe, Are there no limits to authority? TQM and organizational power, Organization Studies 20 (2) (1999) 197-224

[50] D. Knights, D. McCabe, Ain't misbehaving? Opportunities for resistance under new forms of "quality" management, Sociology 34 (3) (2000) 421–436

[51] C.-Y. Ku, Y.-W. Chang, D. C. Yen, National information security policy and its implementation: a case study in Taiwan, Telecommunications Policy 33 (7) (2009) 371–384

[52] A. Lee, R. Baskerville, Generalizing generalizability in information systems research, Information System Research 14 (3) (2003) 221-243

[53] H. Lee, S. Oh, A standards war waged by a developing country: Understanding international standard setting from the actor-network perspective, Journal of Strategic Information Systems 15 (3) (2006) 177-195

[54] H. Leland, Quacks, lemons and licensing: a theory of minimum quality standards, The Journal of Political Economy 87 (6) (1979) 1328-1346

[55] M.A. Lima, M. Resende, L. Hasenclever, Quality certification and performance of Brazilian firms: an empirical study, International Journal of Production Economics 66 (2) (2000) 143-147

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

[57] J. Meyer, B. Rowan, Institutionalized organizations: formal structure as myth and ceremony. In. W.W. Powell, P.J. DiMaggio, (eds.) The New Institutionalism in Organizational Analysis, London: The University Press of Chicago (1991)

[58] M. Nuñez-Nickel, I. Gutiérrez, Governmental context determines institutional value: Independently certified performance and failure in the Spanish newspaper industry, Organization Studies 27 (10) (2006) 1513-1531

[59] G. Ofori, G. Gang, ISO 9000 certification of Singapore construction enterprise: its costs and benefits and its role in the development of the industry, Engineering, Construction and Architectural Management 8 (2) (2001) 145-157

[60] P. Prasad, A. Prasad, Stretching the iron cage: The constitution and implications of routine workplace resistance, Organization Science 11 (4) (2000) 387–403

[61] H. Quazi, S. Padibjio, A journey toward total quality management through ISO 9000 certification- a study on small and medium sized enterprises in Singapore, International Journal of Quality & Reliability Management 15 (5) (1998) 489-508

[62] H. Rao, The social construction of reputation: certification contests, legitimation, and the survival of organizations in the American automobile industry, Strategic Management Journal 15 (S1) (1994) 29-44

[63] J. Reinecke, S. Manning, O. von Hagen, The emergence of a standards market: multiplicity of sustainability standards in the global coffee industry, Organization Studies 33 (5/6) (2012) 791–814

[64] J. Repschlaeger, E. Koray, Z. Ruediger, Cloud computing adoption: an empirical study of customer preferences among start-up companies, Electronic Markets 23 (2) (2013) 115-148

[65] V. Rus, Positive and negative power: thoughts on the dialects of power, Organization Studies 1 (1) (1980) 3-19

[66] R. Sabherwal, R. Hirschheim, The dynamics of alignment: insights from a punctuated equilibrium model, Organization Science 12 (2) (2001) 179-197

[67] P. Sarkar, L. Young, Managerial attitudes towards green IT: an explorative study of policy drivers, Proceedings of Pacific Asia Conference on Information Systems (2009)

[68] H. Scarbrough, The unmaking of management? Change and continuity in British management in the 1990s, Human Relations 51 (6) (1998) 691–715

[69] C. Shapiro, H. Varian, Information Rules: A Strategic Guide to the Network Economy, Boston: Harvard Business School Press (1999)

[70] M. Siponen, J. Iivari, Six design theories for IS security policies and guidelines, Journal of Associations for Information Systems 7 (7) (2006) 445-472

[71] M. Siponen, R. Willison, Information security management standards: problems and solutions, Information & Management 46 (1) (2009) 267-270

[72] A. Smith, An Inquiry into the Nature and Causes of the Wealth of Nations, University of Chicago Press, Chicago (1977)

[73] D. Straub, Effective IS security: an empirical study, Information Systems Research 1 (3) (1990) 255-276

[74] P. Swann, M. Shurmer, The emergence of standards in PC software: who would benefit from institutional intervention, Information Economics and Policy 6 (3/4) (1994) 295-318

[75] R. Thomas, A. Davies, Theorizing the micro-politics of resistance: new public management and managerial identities in the UK public services, Organization Studies 26 (5) (2005) 683-706

[76] P. Thompson, S. Ackroyd, All quiet on the workplace front? A critique of recent trends in British industrial sociology, Sociology 29 (4) (1995) 615–633

[77] S. Timmermans, S. Epstein, A world of standards but not a standard world: toward a sociology of standards and standardization, Annual Review of Sociology 36 (1) (2010) 69-89

[78] M. L. Tushman, E. Romanelli, Organizational evolution: a metamorphosis model of convergence and reorientation, Research in Organizational Behavior 7 (1985) 171-222

[79] J. van den Ende, G. van de Kaa, S. den Uijl, H. J. de Vries, The paradox of standard flexibility: The effects of co-evolution between standard and interorganizational networks, Organization Studies 33 (5/6) (2012) 705–736

[80] P. Vermeulen, R. Büch, R. Greenwood, The impact of governmental policies in institutional fields: the case of innovation in the Dutch concrete industry, Organization Studies 28 (4) (2007) 515-540

[81] G. Walsham, Interpreting Information Systems in Organizations, Chichester: John Wiley & Sons (1993)

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

[83] R. Yin, Case Study Research: Design and Methods. Thousand Oaks:Sage publications, 2013.

[84] M. Zbarachki, The rhetoric and reality of total quality management, Administrative Science Quarterly 43 (3) (1998) 602-636

Appendix A: Comparison between Generic Certification Scheme and *c:cure*

	Generic Certification Scheme	***c:cure Scheme***
Applicable Countries	Global	UK only
Scheme oversight	The European co-operation for Accreditation EA7/03 document, recognized and accepted internationally	*c:cure* accreditation scheme, accepted within the U.K.
Standards adopted for certification	BS 7799	BS 7799
Validity of certificate	Initial validity for 3 years	Initial validity for 3 years
Accreditation Body	United Kingdom Accreditation Services (UKAS)	United Kingdom Accreditation Services (UKAS)
Certification Bodies	Required to be accredited by UKAS, but can be operated both in the U.K. and other countries	Required to be accredited by UKAS, operated only in the U.K.
Auditor assessment	No mandatory requirements	Required for independent *c:cure* auditor competence assessment organised by Independent Register of Certified Auditor (IRCA)
Cost	Depends on • the number of existing controls implemented; • the size of the organization; • the numbers of sites audited; • the cost of the certificate itself; • the daily rate of assessor.	Depends on • the number of existing controls implemented; • the size of the organization; • the numbers of sites audited; • the cost of the certificate itself; • the daily rate of assessor. However, the daily rate of assessor will normally be higher than the generic scheme because of additional auditor assessment cost.