INFORMATION SECURITY STANDARDS: ADOPTION DRIVERS (INVITED PAPER)

What drives organisations to seek accreditation? The case of BS 7799-2:2002

Jean-Noel Ezingeard and David Birchall
Henley Management College, Greenland, Henley-on-Thames, RG9 3AU, United Kingdom

Abstract: ISO/IEC 17799 is a standard governing Information Security Management. Formalised in the 1990s, it has not seen the take up of accreditations that could be expected from looking at accreditation figures for other standards such as the ISO 9000 series. This paper examines why this may be the case by investigating what has driven the accreditation under the standard in 18 UK companies, representing a fifth of companies accredited at the time of the research. An initial literature review suggests that adoption could be driven by external pressures, or simply an objective of improving operational performance and competitive performance. It points to the need to investigate the influence of Regulators and Legislators, Competitors, Trading Partners and Internal Stakeholders on the decision to seek accreditation.

An inductive analysis of the reasons behind adoption of accreditation and its subsequent benefits suggests that competitive advantage is the primary driver of adoption for many of the companies we interviewed. We also find that an important driver of adoption is that the standard enabled organisations to access best practice in Information Security Management thereby facilitating external relationships and communication with internal stakeholders. Contrary to the accepted orthodoxy and what could be expected from the literature, increased regulation and the need to comply with codes of practice are not seen as significant drivers for companies in our sample.

Key words: Information Security, Adoption, ISO/IEC 17799, ISO/IEC 27001, BS 7799, Best practice

1. INTRODUCTION

BS7799 was initiated in the UK in 1993 as a "Code of Practice" for Information Security Management. It was inspired by a UK ministry (the Department of Trade and Industry – DTI) in co-operation with a number of leading commercial organisations including Shell and a number of major banks, who were perceived as highly developed in security techniques. The Code of Practice became a British Standard in 1995. Globalisation, and the requirement for common security standards encouraged propagation and recognition of BS7799 worldwide, culminating in it becoming the ISO standard ISO/IEC 17799:2000. Further work was done by the British Standards Institution on Management Systems for Information Security, leading to the publication of BS7799 part 2 (BSI, 2002). Although this was not adopted as part of the International Standard, it is used in many countries other than the UK, such as Sweden, Finland, Norway, Japan, China (Hong-Kong), India, Australia, Taiwan and Korea (Waloff, 2002). BS7799 part 2 is expected to be replaced by ISO/IEC 27001:2005 in late 2005 (BSI, 2005). Until then, companies seeking some form of accreditation must do so under BS 7799 Part 2:2002.

Proponents of the standard argue that significant benefits can be gained from its implementation. For instance, the introduction to the Information Security Management Systems (ISMS) part of the standard emphasises the benefits of adoption:

> "The ISMS is designed to ensure adequate and proportionate security controls that adequately protect information assets and give confidence to customers and other interested parties. This can be translated into maintaining and improving competitive edge, cash flow, profitability, legal compliance and commercial image." (BSI, 2002, p3)

From its inception the code received much attention, but as far back as 1996, concerns were raised about its uptake. At the time, a survey of 1452 organisations based in the UK had shown that adoption, or indeed intention to adopt, were very low despite the wide-spread publicity given to the standard at the time (Kearvell-White, 1996). In 2004, awareness of the standard and its detailed content was still thought to be low (DTI, 2004). Perhaps not surprisingly, certification figures for BS 7799 Part 2:2002 themselves are running significantly below 100 organisations in most European countries, as shown in *Table 1*. Some commentators argue that certification figures themselves do not provide an accurate picture of the take-up as many companies choose to use only part of the standard and prefer an incremental approach than full 'all or nothing' certification (von

Solms and von Solms, 2001). In particular, it has been argued that general standards such as ISO 17799 are not always helpful in their entirety because they do not take into consideration the unique circumstances of each company (Baskerville and Siponen, 2002). However, the number of registrations for other standards is strikingly higher than those for BS 7799 Part 2:2002, with over 242,000 accreditations in Europe alone for ISO 9001:2000 (ISO, 2003) and it is legitimate to hypothesise that there is mismatch between what accreditation under BS 7799-2:2002 offers and what companies seek.

Table 1: Number of BS 7799 Part 2:2002 certificates issued in Europe since the creation of the standard. Source: www.xisec.com (31/08/2005)

Country	No. of Certificates	Country	No. of Certificates
Czech Rep	5	Iceland	4
Lithuania	1	Poland	5
Luxembourg	1	Switzerland	8
Macedonia	1	Sweden	7
Romania	1	Norway	10
Slovakia	2	Ireland	11
Slovenia	1	Hungary	13
Belgium	2	Finland	15
Denmark	2	Netherlands	21
Greece	4	Italy	26
Spain	4	Germany	42
Austria	8	UK	212

Despite the low take up of certification for BS 7799 Part 2:2002, the number of calls for greater attention to be paid to Information Security Management have not abated since the inception of the standard. The topic of Information Assurance is now of such concern for governments and international agencies that many have created specialized units to promote the adoption of standards and best practice. For instance the UK government created a specialist division in its Cabinet Office in April 2003 (the Central Sponsor for Information Assurance). At European level this takes the form of the European Network and Information Security Agency (ENISA) created in 2004.

Why then, are there such low certification figures for BS 7799 Part 2:2002 ? This paper attempts to provide a partial answer to the question by investigating what has driven adoption in a sample of companies that are currently accredited. It is organized as follows: Firstly a conceptual framework of adoption drivers is built from the literature. We then describe our research methodology, arguing for an inductive approach based on semi-

structured interviews. Lastly, the results of the research are presented in the form of resulting propositions and discussed in a concluding section.

2. LITERATURE REVIEW

We have found little literature directly discussing adoption and certification drivers for BS 7799 Part 2:2002. Consequently we identified three other streams of literature that could help inform our interview questions. Firstly we examined both the practitioner and the academic literature on ISO/IEC 17799 and BS 7799 to identify what *benefits* could be expected or gained from adoption and subsequent accreditation. Secondly, we identified selected references from the literature on technology adoption (including the adoption of security measures) to help us build a picture of general adoption drivers. Thirdly we reviewed the literature on the adoption of other international standards such as ISO 9000 or ISO 9001. Whilst not directly related to the topic of ISO 17799 adoption, the latter two streams offer sufficient theoretical grounding about adoption to help build an interview framework when triangulated with the practitioner literature on ISO/IEC 17799 adoption and BS 7799 certification.

Both practitioner and academic literature on ISO 17799 are quite coy about the potential benefits of adoption and/or certification. There are broadly four categories of benefits that emerge. A summary is given in *Table 2*. Perhaps not surprisingly, given the emphasis placed in the Information Security literature on the need to raise awareness, 'communication' benefits features are often associated with adoption of the standard as the most quoted benefits. The standard is thought of as a good way to demonstrate commitment, demonstrate good practice and reassure. It is also seen as a way to convince or coach both internal and external stakeholders. The second most quoted type of benefit associated with the standard is connected with best practice adoption that the standard should facilitate. Lastly, although more rarely quoted, other business benefits associated with the standard in the literature include operational and competitive benefits.

Table 2: Benefits of ISO 17799 adoption as expressed in practitioner and academic literature

Category	Benefits	Source
Communication with internal stakeholders	Provides an accepted benchmark that facilitates communication with stakeholders	(Pattinson, 2003, Velayudham et al., 2004)
	Helps change staff behaviour	(DTI, 2004)

	Helps Information Security Managers gain senior management recognition	(Li et al., 2000)
Communication with external stakeholders	Enhances trust between business partners	(Barnard and von Solms, 1998)
	Can facilitate trading or procurement of IT services	(von Solms, 1998)
	Useful / requirement to gain cyber-insurance	(Groves, 2003)
Enhanced operational or competitive performance	Helps achieve efficiency and effectiveness	(DTI, 2004) (Note: Efficiency and effectiveness are not clearly defined in the report)
	Helps reduce the costs of security incidents	(Kenning, 2001)
Best practice	Provides guidance in an otherwise complex field, 'useful framework'	(Armstrong et al., 2002, Gossels, 2003, McAdams, 2004)
	Can aid policy development	(Baskerville and Siponen, 2002, Fulford and Doherty, 2003)
	Facilitates the adoption of minimum standards, common security baselines.	(Brooks et al., 2002, Kearvell-White, 1996)

Having identified what benefits were often associated with the adoption of ISO 17799, we also reviewed what triggered other adoption of innovative practices and new technology. A first stream of literature on technology adoption has traditionally focused on the motivation of individual users to adopt IT artefacts or software (for instance research on technology acceptance, such as Venkatesh et al., 2003). A second stream, more relevant in our case, is the literature looking at organisational factors motivating the acceptance of technology at firm level.

In examining this side of the literature we sought to identify groupings of factors that drive adoption. A large proportion of published research of firm level technology adoption decisions is grounded in the strategic positioning school that argues that competitive advantage can be gained from technology if it influences the competitive position of the firm (Ives and Learmonth, 1984). Furthermore, this school of though argues that competitive pressures can act as drivers of implementation.

A good example of such pressures can be found in the literature on the adoption of Electronic Data Interchange (EDI) technology. Here, competitive positioning factors have been found to be particularly relevant in pushing firms to take up the technology. In particular, the bargaining power

of trading partners is an important influence in driving the adoption of EDI in small firms (Hart and Saunders 1997; 1998). Earlier, Iacovou *et al.* (1995) had also identified competitive pressure and imposition by trading partners as two types of external pressure that encourage take up. They argued that three key factors that affect drive implementation in this range of organisations are: perceived benefits; organisational readiness; *and* external pressure. Such pressures are not confined to adoption decisions pertaining to technological innovation. Of particular relevance to our general problem area, the coercive effect of powerful trading partners has also been found to play a significant role in the adoption of ISO 9000 (Guler et al., 2002). Interestingly, Guler *et al.*'s study also shows that in the case of ISO 9000, coercive effects also came from Nation States.

Another school of strategy used to examine adoption drivers of technological innovation is that of the Resource Based View of the firm which argues that competitive advantage can be obtained when technology is used to create or exacerbate differences between competitors (Dehning and Stratopoulos, 2003, Feeny and Ives, 1990, Griffiths and Finlay, 2004). Such differences have been found to be a factor playing a role in the sustainability of the advantage (Anderson et al., 1999), particularly where the resources at the source of the difference are not freely mobile (Mata et al., 1995). The idea of *asymmetry*, whether informational, technological or structural, is diametrically opposed to that of *standardisation*. Specifically, the accreditation to any standard is particularly 'mobile' in that standards are widely published. Therefore, the adoption of an international standard and subsequent accreditation, for differentiation purposes may seem paradoxical. However, in the case of ISO 9000 adoption, it has been found that many firms did seek differentiation through take up and subsequent accreditation (Anderson et al., 1999). In such cases the differentiation was sought between firms that were accredited and those that were not. This is akin to Clemons and Row's argument (1991) that there are cases where the first mover advantage is significant in affording an organisation competitive advantage from differentiation and that customer preferences may change to favour the innovator.

In summary, the literature on ISO 17799, the literature on technology adoption and the literature on the adoption of other standards yield to a theoretical classification of adoption and/or certification drivers based on:

- Adoption driven by external pressures, or coercion (such as trading partners or States)
  a) Because certification is a 'licence to trade'
  b) Because certification helps demonstrate superior Information Security performance to potential trading partners

- Adoption driven by the desire to seek competitive or operational advantage through superior Information Security
  a) Because adoption and/or certification will yield, or help achieve, better Information Security practices
  b) Because adoption will help create resource asymmetry that can then be marketed to internal and external stakeholders and customers.

This points to the need to examine the influence of four key contextual aspects of the decision to seek accreditation and its benefits: competitors, trading partners, legislators and regulators and internal stakeholders. This is illustrated in figure 1. Furthermore, because the acquisition of best practice features as a potential motivator, there is a need to examine the accreditation process itself, including the role of consultants and the factors influencing the success of the process.

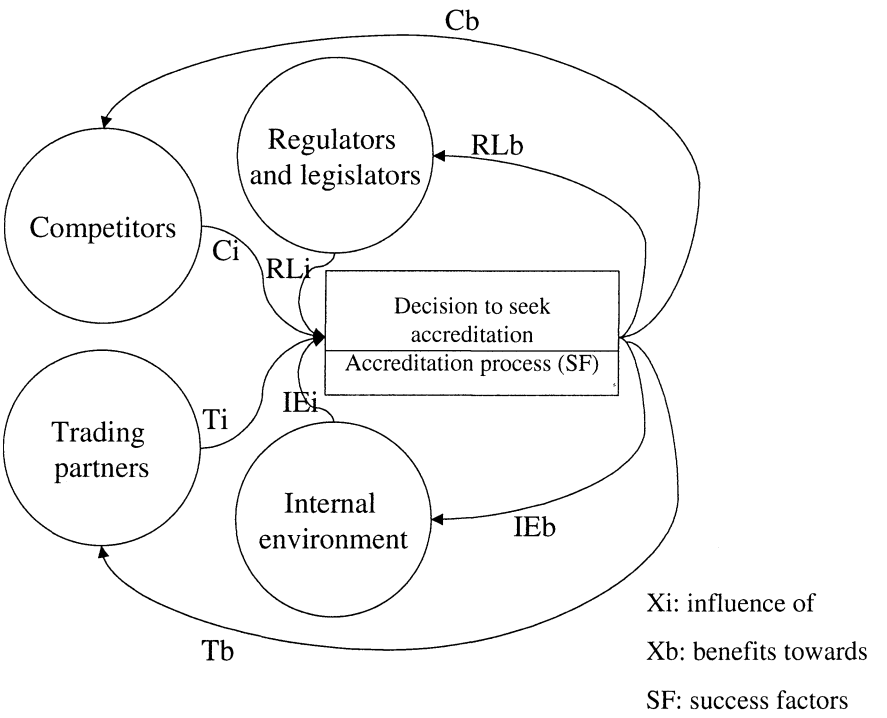

Figure 1. Model of theoretical influences on companies seeking ISO 17799 accreditation and resulting benefits

3. METHODOLOGY

3.1 Research context

The empirical context for the research carried out is complex for two practical reasons. The first is that many organisations are reluctant to discuss their information security arrangements. This lead Kotulic and Clark (2004) to suggest that large scale surveys in the area of information security have a very small chance of attracting a sufficient number of participants to produce worthwhile results. They suggest that "time is better spent focusing on a few selected firms with which the researcher has developed an excellent rapport and trust" (p 605). This potential difficulty was exacerbated by a very pragmatic and simple factor: that the low number of companies accredited (see *Table 1*) would make it very difficult to get statistically meaningful response numbers from a survey.

From an epistemological point of view, the literature review so far has shown that an interpretive approach is needed at this stage of understanding of adoption factors for BS 7799-2:2002 accreditation. Interpretive research in IS is "aimed at producing an understanding of the context of the information system, and the process whereby the information system influences and is influenced by the context" (Walsham, 1993, p4). Although our review of the literature has produced a theoretical classification of adoption drivers which could be used as the basis of a research model and hypothesis, it would be inappropriate to carry on the study relying on what Lee calls "hypothetico-deductive logic" (Lee, 1999). This is because we were interested in gaining further insights under each of the potential drivers identified in the literature review, rather than trying to examine whether they contributed or not to the adoption decision. The literature review has shown that a better understanding of the *context* of the adoption decisions is needed, for instance to understand what external pressures are at play when organisations examine how competitive or operational advantage can be gained through accreditation. Similarly, a better understanding of the *process* by which the context (competitive, legislative or internal) influences the decision to seek accreditation is necessary to explain the true nature of potential external pressures for adoption.

3.2 Research approach

In order to investigate what the adoption drivers behind BS 7799-2:2002 certifications were, we chose an interview-based approach. This was done

because of the empirical context explained earlier (difficulties in gaining access and low number of organisations accredited). Because we opted for exploratory, inductive research; we felt that semi-structured interviews would yield greater insights.

We initially developed an interview framework on the basis of the theoretical headings identified in the literature review, although the questions listed in the interview framework (Appendix 1) were used as prompts rather than rigidly followed by the interviewer. Interviews were taped and transcribed by the interviewer. This was done as soon as possible after the interview and ensured that gaps could be bridged from the context. The interviews lasted between 40 and 90 minutes. Our interview base was selected from the published lists of companies that had achieved accreditation under BS 7799-2:2002. Companies were initially approached by phone, either through a 'cold call' or through contacts from the research team. As such, a large amount of convenience sampling is present in our interview pool (shown in appendix 2). As part of this convenience sampling process, we selected two companies we knew (subject 12 and subject 17) that have not actually sought formal 7799 accreditation. However both operate very closely with many of the terms of the certificate. This base represents around a fifth of all UK organisations accredited at the time of the research.

3.3 Analysis procedure

The interpretation of the interview data was based on a simple coding process of the interview transcripts. We used the technique recommended by Miles and Huberman (1994, p58) of a "start-list" of codes (in our case Ci, Cb, Ti, Tb, RLi, RLb, Iei, IEb and SF as shown in figure 1). This was sufficient to allow us to develop the propositions presented in the results section below, and codes were not augmented or revised during the process. Our objective for the analysis was twofold. Firstly we sought to discover regularities, patterns and themes that would deepen our understanding of the theoretical drivers that emerged from the literature review, and the processes through which they influenced the decision to seek accreditation. Secondly we sought to identify new drivers that we had not envisaged from the literature. Again, the process through which they were at play was examined.

4. RESULTING PROPOSITIONS

4.1 Competitive Advantage as a primary motivator

Our model of theoretical influences suggests that competitors and trading partners will influence and benefit from accreditation. In examining the data around Ci, Ti, Cb, and Tb in our interviews we were able to describe theses influences further as they manifested themselves mostly under the heading of 'competitive advantage'. For instance, when asked about their primary motivators for seeking accreditation, a large number of respondents (subjects 3, 4, 5, 7, 10, 13, 14, 15, 17, 18) quoted 'competitive advantage'. Perhaps not surprisingly (most of these companies are providers of IT solutions in one way or another), competitive advantage was described by the interviewee as derived from the improved image that ISO 17799 and accreditation under BS 7799-2:2002 would give the organisation. This improved image could be used as a marketing tool and help generate customer confidence. Many argued that in their sector, accreditation was seen as a primary source of credibility and that customers were increasingly demanding that their suppliers should be accredited. In the words of subject 10, many customers *"asked questions [about Information Security] and sought proof... The external certification clarifies this and grounds it in an independent third party measure"*. For many companies that linked accreditation with improved image, there is no doubt that the 'rubber stamp' provided by the certificate was a motivator. As pointed out by subject 4, the certificate is clearly shown on business cards and email signatures issued by employees of his company.

In addition to improved image with customers or potential customers, subject 10 linked accreditation to competitive advantage because it gave his company the opportunity to *"attract investors by signifying a good quality company with well established procedures"*.

For those companies that did not operate in IT services, competitive advantage through accreditation was seen as much more difficult to obtain. For instance subject 7 suggested that their customers, were influential as an accreditation driver through their security expectations, albeit *"..the majority will have no idea of the meaning and definition of 7799."* Here accreditation is seen as a mechanism for the company to improve its Information Security Management, rather than a 'rubber stamp'. Only one interviewee (subject 3) linked competitive advantage from accreditation as derived from enhanced Intellectual Property protection.

4.2 Increased regulation and the need for compliance are not significant drivers

Increased regulation and the need to comply with codes of practice are often quoted as key drivers of the Information Security efforts of organisations. The standard itself suggests that 17799 compliance should help maintain legislative compliance. Compliance with legislation is the last of its 12 control objectives (ISO, 2000, para 4.1.1) – in other words, a company that does not comply with legislation pertaining to Information Security and Data Protection cannot be accredited as compliant under ISO 17799. In practice, compliance was not seen as a key motivator for implementation in organisations we interviewed. Out of 18 interviewees, only one (subject 14) quoted regulation – the need to comply with the Turnbull report, which sets out Corporate Governance standards in the UK (Turnbull, 1999) – as a motivator of their implementation.

Can this be interpreted as a lack of interest in compliance? Perhaps not so. For instance company 6 has linked its internal auditing procedures with 7799. The interviewee argued that as a result of BS 7799, the audit process was now *"probably tougher"*, indicating that the standard has a role to play in aiding compliance. A similar argument was used by subject 7 who pointed out that *"Ongoing compliance checks [for BS 7799] dovetail effectively with both internal and external audit"*. We also need to take into account that IT auditors and IT risk managers tend to use other frameworks for audit purposes (such as COBIT, see von Solms, 2005). Going back to our model in Figure 1, and more specifically RLi and RLb, our interpretation is that the need for compliance may be a positive moderator of the drive to seek accreditation, but not an influence. It is construed as a nice by-product of accreditation. Any further research should therefore start from this angle.

4.3 Access to, and delivery of, best practice

4.3.1 Best practice for its own sake, or as a lever?

More than half of the interviewees quoted access to best practice in Information Security Management as a motivator for their organisation to achieve compliance and seek accreditation under BS 7799-2:2002. Interestingly, best practice was seen by our interviewees as desirable for two

reasons that are different, even though linked. The first reason is access to information and expertise. Some interviewees indicated that accreditation was helpful to their company in its efforts to achieve best practice in Information Security terms. Accreditation was seen as a way to access proven Information Security Management methods. This was the case for subjects 3, 7, 8, 9, 10, 12, 15 and 18. In the words of subject 18, the standard was adopted because it is his company's policy *"that recognized international standards and best practice are incorporated into defining policy and ways of working"*, and as pointed out by subject 10, *"In reality 7799 is purely best practice"*.

The second reason why best practice as embodied by ISO 17799 was seen as desirable by interviewees was in fact connected to the ability, conferred by accreditation, to justify encouraging employees to adhere to 'safe' practices. In the words of subject 2 describing the standard, *"employees can see it is best practice and efficient and it becomes a "standard" way of doing things"*. In a similar vein, other interviewees seemed to take the view that the 'Best Practice' argument could be used as a lever to convince reluctant stakeholders to adopt procedures that might otherwise be seen as cumbersome. For instance subject 6 explained: *"People now accept rules as best practice"*. A similar argument was given by subject 13. In her words: *"Workload has increased slightly due to the adoption of best practice security. However employees generally seem to understand this"*. We also came across evidence in the interviews that this lever was seen as useful to encourage greater attention from top-management to Information Security. As pointed out by subject 3, *"generally 7799 has improved awareness of the importance of security at a Corporate Governance level."*

Looking back at our theoretical model and more specifically the 'IEi' arrow, our interpretation of the interview data so far is therefore that best practice is conceptualised in two ways regarding BS 7799-2:2002 accreditation: as a goal that accreditation can help achieve, but also as a powerful argument to convince (internal) sceptics. Interestingly we also found a third set of views connecting best practice and BS 7799-2:2002 accreditation: that the accreditation process may not actually help. This is discussed next.

4.3.2 Is best practice really achievable through certification?

In looking at the 'IEb' arrow of our original model, we came across, very early in our interview process, mixed views about the value, in best practice terms, of the accreditation process. This was invariably linked to views that

more value could have been gained by organisations from the accreditation audit. Firstly, in some cases it appeared that doubts could be raised about the level of expertise and training of the auditors. In the words of subject 3 for instance, *"early audits were the blind leading the blind due to a lack of experience* [of the auditors]". A similar view was echoed by subject 5 as he explained: *"During the initial audits it was clear both auditor and auditee were very much in a learning process due to the recent introduction of the standard"*.

Whilst these two interviewees were the most pessimistic about the opportunities for the accreditation process to be a source of best practice insights, others also expressed unease with the process itself. The auditors' 'style' was quoted by subjects 2, 8, 14 and 16 as being too driven by procedural compliance checks, rather than focussed on providing value. The second aspect of why value from accreditation is not gained, in the form of access to best practice, is therefore that accreditation is sometimes construed as a checking process rather than an enabling one. Only in the eyes of one of our interviewees was the tension between the auditors' role as impartial assessors and their role as sources of knowledge of best practice resolved. This was the case of subject 15 who explained that the BS 7799-2:2002 auditors *"were able to make valid contributions"*.

4.4 The role of senior management

The ISO 17799 standard itself stipulates that management involvement is key. Part 1 states that *"Information security is a business responsibility shared by all members of the management team"* (ISO, 2000, para 4.1.1) , but Part 2 of the British Standard goes further by making evidence of management commitment a requirement. In looking at implementation drivers, it is interesting to go beyond evidence of management commitment at the time when the accreditation is sought, to look at the role of management in *initiating* or *driving* the accreditation process, or if the initiative for accreditation is not originating from top management, what drivers will lead to top management support.

When looking at management commitment to implementation in order to probe the 'SF' construct in our original model, the picture that emerged from our interviews is that all organisations witnessed strong commitment from their senior management *during* implementation. Terms used by our interviewees about their top management's attitudes ranged from *"fully supported"* (subject 6) to *"actively involved"* (subject 18) and *"extremely supportive"* (subject 16). It was clear that those responsible for initiating the accreditation process had managed to gain commitment from senior

managers in all the organisations we interviewed. But what led to their support? Here the evidence is more mixed, and our interpretation of the data is that there are two groups of circumstances leading to top management support.

The first set of circumstances occurred in companies where top management was convinced by evidence from the market that accreditation is necessary. We found this was the case in companies represented by subject 3, where top management *"frequently need to be persuaded of the benefits"*. In another organisation *"pressure from customers and the market needs also played an important part in pushing management to support the certification process"* (subject 5). In the case of subject 7, the *"CEO was converted as a result of the competitive advantage and customer security [that accreditation would confer]"*.

The second set of circumstances occurred in organisations where the awareness of technological matters at senior management level is high. This was the case in the companies represented by subjects 2, 10 and 15. Company 2 for instance has a very 'IT oriented' Managing Director who needed little convincing that accreditation was necessary. The company's web-site actually lists her areas of responsibilities as Operations, but also, Field Operations, and IT. Similarly, in the case of company 10 and 15, both respondents suggested that given the markets their companies operated in and their respective cultures, engaging top management and obtaining their support was relatively easy.

5. CONCLUSION

As argued in the introduction, there is a need to understand what motivates organisations to adopt ISO 17799 and seek accreditation under BS 7799-2:2002. This research has contributed to this understanding, firstly at a theoretical level, and secondly by investigating, in some depth, what has driven 18 UK companies to adopt the standard and seek accreditation. We will pick up on two salient findings from our research here. Firstly, it has shown that, in the organisations we interviewed, competitive advantage was often seen as a significant driver of adoption – whereas regulation and encouragement from Information Security bodies, governments and other trade associations very rarely featured in our interviewees' responses. This is contrary to the orthodoxy found amongst many advocates of the 7799 standards as a demonstrably robust control system. This is significant in that it suggests that the message from these third parties perhaps needs to be realigned to emphasise the competitive benefits of adoption and certification.

Here we can speculate that whilst the 'compliance' message may be of interest to auditors, it is likely that the primary initiators of BS 7799-2:2002 accreditation will belong to an Information Systems community of practice where compliance may not be considered as a significant business issue.

The second, paradoxical findings that seems to emerge is about the nature of the intent to adopt best practice through accreditation. Here, we found that the argument of best practice was often used as an internal lever to convince perhaps reluctant employees or senior management to change their behaviour and support changed Information Security practices. At first sight this could be a worrying management practice – and perhaps counter productive in the long term if changes in attitude as well as behaviour are not achieved. It would be beyond the scope of this paper to discuss the organisational politics implications of the practice we unearthed, but is worth asking whether it falls within Information Systems phenomena that and can be used to reduce emancipation by alienating workers (Angell, 1990, p. 173). The main drawback of such an approach, according to Angell is that that managers make the process of security too complex, uncertain and unimaginative. Risk Management actions are, according to Ciborra (2004), *"intertwined in social processes and networks of relationships"*. Many similar observations are grounded in the psychology of risk literature, and the argument that *"risk is what matters to people"* (Renn, 1998). This therefore suggests that accreditation under BS 7799-2:2002 can sometimes act as a pre-requisite to a change towards a culture of best practice, as much as a response to regulatory and competitive pressures to demonstrate that best practice has been achieved.

Finally, we should reflect on the limitations of the work presented here and potential avenues for further research. The fist limitation is largely unavoidable: because there are few organisations accredited worldwide, it is impossible to get a very large sample base for this kind of research. This is compounded by the fact that access to organisations in Information Security research is generally difficult (Kotulic and Clark, 2004). The second limitation is more conceptual. In looking at adoption drivers in those companies that are compliant with the standard and that have sought accreditation, we have left out those companies that have decided *against* accreditation, and instead have chosen partial adoption, or rejected the standard altogether. Whilst knowing why those that have adopted have done so, the picture this provides is by nature partial and can only to some extent help answer the puzzle of why there are so few companies accredited. An interesting line of further enquiry would therefore be to attempt to collect data about what factors influences the decisions of non-adopters of accreditation.

APPENDIX 1: INTERVIEW FRAMEWORK

Heading	Interviewee prompts
Organization Background	What is your: primary activity, target markets sectors, geographic coverage: What (qualified) information security human resources are available within your organisation? Do you outsource any Information Security tasks, if so which, and to what extent? What information security risks exist in the environment in which your business operates?
Adoption and Accreditation process	How wide is the current scope of certification within your organisation? How long did the accreditation process take? What effect did your organisation's size have upon implementation? What were the approximate costs sunk during the implementation process? Were external consultants appointed and how would you rate their effectiveness? What changes to your business processes were necessary during implementation?
Motivation and drivers	What were the primary motivations behind implementation? What effect did certification have upon communication - internal or external?
Benefits	What objectives or benefits were expected as a consequence of accreditation? Have these been achieved? What unforeseen benefits have accrued? How do you assess certification ROI?
Adoption Success Factors	What major barriers did you need to overcome during implementation? What do you consider to be the Critical Success Factors for certification? What lessons were learnt through the implementation process? What advice or guidance was available – i.e. from auditors or BSI?
Internal Stakeholders: Management	How influential was management to gaining accreditation? What management levels were involved and how?

Heading	Interviewee prompts
	How strong is their post implementation involvement?
Internal Stakeholders: Employees	How were employees encouraged to become part of the accreditation program? How critical was employee involvement to the accreditation process? How much training, and what methods were undertaken during accreditation? Has certification had an effect upon employee morale?
External Stakeholders: Governments and regulators	How influential were legal influences to the management's decision making process? What Government influences were apparent during the certification process? What other ISO standards are you certified to?
External Stakeholders: Customers	What are the customer expectations of information security? How do you promote certification as a source of CA in specific customers or markets? What impact has your accreditation had upon customers? Has Customer Satisfaction increased as a consequence of certification?
Other competitive position drivers	How have your competitors reacted to your gaining accreditation? How do you ensure the "security integrity" of third parties to which your systems are linked?
Best practice	How influential was 7799 in guiding process improvements? Do you consider your IT environment more secure as a consequence of implementation?

APPENDIX 2: INTERVIEWEES

Subject	Sector	Title or Department Represented	Type of Interview
1	Logistics	Head of Information Security & Governance	Face to face
2	Energy Metering Service Provider	Quality & Estates Manager	Face to face
3	Information Security Solutions Provider	Director	Telephone
4	Information Security Solutions Provider	Professional Services	Face to face

Subject	Sector	Title or Department Represented	Type of Interview
5	Outsourcing Partner	Quality Assurance Manager	Telephone
6	'big 4' professional services firm	Quality Manager	Face to face
7	Banking IT infrastructure provider	General Manager - Operations	Telephone
8	IT services	Senior Consultant	Telephone
9	Local Government	Head of Information Management	Face to face
10	Outsourcing Partner	Founder	Face to face
11	Insurance and Financial Services	Head of Information Assurance	Face to face
12	Energy	Global Information Security Manager	Telephone
13	Outsourcing Partner – IT services	Quality Manager	Telephone
14	Outsourcing Partner – IT services	Training & Quality Manager	Face to face
15	Information Security Solutions Provider	Technical Director	Face to face
16	Manufacturing	Director of Group Audit	Telephone
17	Publisher	Managing Director	Telephone
18	IT services	Chief Information Officer	Written response

REFERENCES

Anderson, S. W., Daly, J. D. & Johnson, M. F. (1999) Why firms seek ISO 9000 certification: Regulatory compliance or competitive advantage. *Production and Operations Management,* 8(1), 28-43.

Angell, I. O. (1990) Systems Thinking about Information Systems and Strategies. *Journal of Information Technology,* 5(3), 168-74.

Armstrong, J., Rhys-Jones, M. & Rathmell, A. (2002) Corporate Governance & Information Assurance - What Every Director Must Know. Information Assurance Advisory Council, Cambridge - UK.

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

Baskerville, R. & Siponen, M. (2002) An information security meta-policy for emergent organizations. *Logistics Information Management,* 15(5/6), 337-46.

Brooks, W. J., Warren, M. J. & Hutchinson, W. (2002) A security evaluation criteria. *Logistics Information Management,* 15(5/6), 377-84.

BSI (2002) BS 7799-2:2002 Information security management systems - Specification with guidance for use. British Standards Institution.

BSI (2005) Frequently Asked Questions for BS 7799-2:2005, British Standards Institution. http://www.bsi-global.com/ICT/Security/27001faq.xalter visited on 31/08/2005

Ciborra, C. (2004) Digital Technologies and the Duality of Risk. *Discussion Paper - Centre for Analysis of Risk and Regulation, London School of Economics,* (27).

Clemons, E. K. & Row, M. C. (1991) Sustaining IT advantage: The role of Structural Differences. *MIS Quarterly,* 15(3), 275-92.

Dehning, B. & Stratopoulos, T. (2003) Determinants of a sustainable competitive advantage due to an IT-enabled strategy. *The Journal of Strategic Information Systems,* 12(1), 7-28.

DTI (2004) Information Security Breaches Survey. Department of Trade and Industry / PriceWaterhouseCoopers, London.

Feeny, D. F. & Ives, B. (1990) In Search of Sustainability: Reaping Long-term advantage from Investments in Information Technology. *Journal of Management Information Systems,* 7(1), 27-46.

Fulford, H. & Doherty, N. F. (2003) The application of information security policies in large UK-based organizations: an exploratory investigation. *Information Management and Computer Security,* 11(3), 106-14.

Gossels, J. (2003) Making Sensible Investments in Security. *Financial Executive,* 19(9), 46.

Griffiths, G. H. & Finlay, P. N. (2004) IS-enabled sustainable competitive advantage in financial services, retailing and manufacturing. *Journal of Strategic Information Systems.,* 13, 29-59.

Groves, S. (2003) The unlikely heroes of cyber security. *Information Management Journal,* 37(3), 34-40.

Guler, I., Guillén, M. F. & Macpherson, J. M. (2002) Global Competition, Institutions, and the Diffusion of Organizational Practices: The International Spread of ISO 9000 Quality Certificates. *Administrative Science Quarterly,* 47, 207-32.

ISO (2000) ISO/IEC 17799:2000 Code of practice for information security management. ISO, Geneva.

ISO (2003) The ISO Survey of ISO 9001:2000 and ISO 14001 Certificates. International Standards Organisation.

Ives, B. & Learmonth, G. P. (1984) The Information System as a competitive weapon. *Communications of the ACM,* 27(12), 1193-201.

Kearvell-White, B. (1996) National (UK) Computer Security Survey 1996. *Information Management & Computer Security,* 4(3), 3-17.

Kenning, M. J. (2001) Security Management Standard - ISO 17799/BS 7799. *BT Technology Journal; London,* 19(3), 132.

Kotulic, A. G. & Clark, J. G. (2004) Why there aren't more information security research studies. *Information & Management,* 41(5), 597-607.

Lee, A. S. (1999) Researching MIS. IN CURRIE, W. & GALLIERS, R. (Eds.) *Rethinking management information systems: an interdisciplinary perspective.* Oxford, Oxford University Press.

Li, H., King, G., Ross, M. & Staples, G. (2000) BS7799: A Suitable Model for Information Security Management. *Americas Conference on Information Systems.*

Mata, F. J., Fuerst, W. L. & Barney, J. B. (1995) Information technology and sustained competitive advantage: A resource-based analysis. *MIS Quarterly,* 19(4), 487-505.

McAdams, A. C. (2004) Security And Risk Management: A Fundamental Business Issue. *Information Management Journal,* 38(4), 36-44.

Miles, M. B. & Huberman, A. M. (1994) *Qualitative data analysis: an expanded sourcebook,* Thousand Oaks, Calif.; London, Sage.

Pattinson, M. R. (2003) Compliance with an Information Security Management Standard: A New Approach. *Ninth Americas Conference on Information Systems,* Tampa.

Renn, O. (1998) Three decades of risk research: accomplishments and new challenges. *Journal of Risk Research,* 1(1), 49-71.

Turnbull, N. (1999) Internal Control: Guidance for Directors on the Combined Code: *The Turnbull Report.* The Institute of Chartered Accountants in England & Wales, London.

Velayudham, C., Shoemaker, D. & Drommi, A. (2004) A Standard Methodology for Embedding Security Functionality Within Formal Specifications of Requirements. *Americas Conference on Information Systems,* New York, August 2004.

Venkatesh, V., Morris, M. G., Davis, G. B. & Davis, F. D. (2003) User acceptance of information technology: Toward a unified view. *MIS Quarterly,* 27(3), 425-78.

von Solms, B. (2005) Information Security governance: COBIT or ISO 17799 or both? *Computers & Security,* 24, 99-104.

von Solms, B. & von Solms, R. (2001) Incremental Information Security Certification. *Computers & Security,* 20(4), 308-10.

von Solms, R. (1998) Information security management (3): the Code of Practice for Information Security Management (BS 7799). *Information Management & Computer Security,* 6(5), 224.

Waloff, I. (2002) Speech by at "7799 Goes Global" conference. *(text available at http://www.bsi-global.com/News/Releases/2002/September/n3f029de8c689a.xalter),* September 5

Walsham, G. (1993) *Interpreting information systems in organizations,* Chichester, Wiley.